ABSTRACT Due to the proliferation of ICT during the last few decades, there is an exponential increase in the usage of various smart applications such as smart farming, smart healthcare, supply-chain & logistics, business, tourism and hospitality, energy management etc. However, for all the aforementioned applications, security and privacy are major concerns keeping in view of the usage of the open channel, i.e., Internet for data transfer. Although many security solutions and standards have been proposed over the years to enhance the security levels of aforementioned smart applications, but the existing solutions are either based upon the centralized architecture (having single point of failure) or having high computation and communication costs. Moreover, most of the existing security solutions have focussed only on few aspects and fail to address scalability, robustness, data storage, network latency, auditability, immutability, and traceability. To handle the aforementioned issues, blockchain technology can be one of the solutions. Motivated from these facts, in this paper, we present a systematic review of various blockchain-based solutions and their applicability in various Industry 4.0-based applications. Our contributions in this paper are in four fold. Firstly, we explored the current state-of-the-art solutions in the blockchain technology for the smart applications. Then, we illustrated the reference architecture used for the blockchain applicability in various Industry 4.0 applications. Then, merits and demerits of the traditional security solutions are also discussed in comparison to their countermeasures. Finally, we provided a comparison of existing blockchain-based security solutions using various parameters to provide deep insights to the readers about its applicability in various applications.

INDEX TERMS Blockchain, consensus algorithms, cyber-physical systems, IoT, smart grid, supply chain management, intelligent transportation.

I. INTRODUCTION

With the wide popularity of Internet and related technologies, various Industry 4.0-based applications have been used across the globe in which sensors and actuators sense, compute and communicate the data for industry automation. As in Industry 4.0-based applications, data between different locations flows using an open channel, i.e., Internet, so threats to security and privacy has also increased manifold [1]. Such applications deal with data in large volumes and hence, so it is necessary to consider issues such as-data heterogeneity, data integrity, and data redundancy alongwith the security and privacy concerns. Moreover, different applications require datasets from different domains in different formats. Therefore, it is also needed to standardize the data format so that it can be used by different Industry 4.0-based applications.

The usage of smart phones and smart applications for personal, professional, and social activities is increasing exponentially across the globe. It results an increase in both the network data traffic (in GBs) and overall expenditure (in

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
Millions USD) as shown in Fig. 1 (a) and (b) as per the report mentioned in [2], [3]. According to this report, smart industries would spend $40B on IoT by 2020 in various sectors including transportation and manufacturing. However, due to the large number of data exchanges over the Internet, maintaining confidentiality, privacy, and integrity becomes a major issue in Industry 4.0 [4]. Moreover, according to the surveys conducted by different agencies [5], [6] nearly 60 millions people are affected by identity theft and 12 billion peoples records misused in 2018 and expected to increase to 33 billion by 2023 as shown in Fig. 2 (a). Fig. 2(b) shows the 10 recent security breaches incidents reported till July 2018, which are expected to increase in the years to come.

Security and privacy preservation are important concerns for Industry 4.0 applications [4], [7]. There may be chances of unauthorized data breaching or information leakage leading to the financial losses to Industry 4.0-based applications. In the absence of robust security architecture, the system along with data are prone to various types of attacks (such as DDoS, ARP spoofing attacks, data rate alteration, network congestion, manipulation, noise interference, phishing and config threats) which can harm the confidentiality and integrity of data and can affect the overall functioning of any system. For such types of attacks, prevention is better than any reactive defense mechanisms to assure confidentiality, integrity, and privacy within the legal compliance rules [8]. It has been found in the literature that with an increasing rate of automation in Industry 4.0., the probability of violating the security rules and launching new type of cyber-attacks is also increasing. Access control, authorization, confidentiality, availability, and integrity are the prime concerns in Industry 4.0.

To mitigate the aforementioned threats, current Industry solutions are using the centralized, client-server based architecture in which the centralized authority holds all the privileges. But, if the centralized authority is compromised then the entire system may crash. Conventional security mechanisms such as Data Encryption Standard (DES), and Advanced Encryption Standard (AES) and their variants are
also being used but they have high computation and communication overhead. However, a revolution in this area came with the introduction of the concept of “Bitcoins” [9]. For example, Authors of [10] illustrated that how blockchain technology can be used to deal with privacy & security issues in Industry 4.0 [11].

The blockchain technology has the potential to handle various security attacks as it can eliminate the need of the centralized authority to perform various operations. In the blockchain technology, a number of users participate in transaction verification and validation [12]–[17]. It uses a structural distributed database which stores data from all the nodes in an encrypted form validated using various checks such as Merkle hash tree (MHT) and Elliptical Curve Cryptography (ECC) [17]. As the database is distributed, so there is a risk of getting crashed or corrupted. Transactions are linked together with cryptographic keys and immutable ledgers which makes it difficult for attackers to manipulate or delete the recorded information. Data is always stored in an immutable manner using timestamps, public audit and consensus mechanisms [18], [19]. The use of these mechanisms makes security architecture a robust and assures data integrity and privacy [20].

A. SCOPE OF THIS SURVEY ARTICLE

The blockchain reduces the risk of single point of failure and network attacks using the distributed network nodes. Use of the decentralized platform reduces fraud by time stamping entries, and information of users is stored in immutable ledger across the network using the smart contact. Blockchain eliminates manual processes like reconciliation between multiple isolated ledger and administrative processes which helps to reduce the cost of the system. Due to the use of various cryptographic linked chains, the speed of transaction and level of security is enhanced manyfold. Several surveys are conducted by the researchers using the blockchain technology for Industry 4.0 which are summarized as follows [21].

Mettler [22] explored how blockchain technology revolutionized the healthcare along with various open challenges [23], [24]. Yli-Huumo et al. [25] reviewed the current scenario of the blockchain technology and its research gaps and challenges. They have also discussed the suitability of the blockchain for various smart applications. Ahram et al. [26] discussed the various components in blockchains such as decentralized techniques and immutability of ledger that makes it difficult to attack the system [27].

Weiss et al. [28] discussed about blockchain public healthcare applications. They have also explored how the blockchain technology eliminates the centralized authority during the verification process, its digital signatures [29] for safe data repository, its architecture, and also the challenges. Zhang et al. [30] evaluated the metrics of blockchain-based decentralized applications. In this paper, they considered the evolution metrics, security, and challenges which are important for various applications like healthcare, smart-agriculture, IoT, and tourism & hospitality. Krieger et al. [31] explored an advanced blockchain architecture for the electronic health systems. They focused on the regulatory compliance for the data privacy of blockchain, its architecture, limitations, and benefits [32]. Duan et al. [33] explored educational applications of the blockchain technology. In this paper, an automated evaluation software as a tool with blocks is proposed, which contains graduation marks along with the certificate. They also highlighted how blocks are recorded, Merkle hash tree, hash functions, digital signatures, and timestamp mechanisms during the verification of various transactions.

Radanović and Likić et al. [34] explored the opportunity of applying blockchain technology in the medical domain. Authors focused on the areas such as supply-chain of drugs, pharmaceuticals, and health insurance with associated challenges. They also discussed how the blockchain can be used in countries like USA and India for the land registration. Vujčić et al. [35] gave an overview of blockchain bitcoin and Ethereum cryptocurrency platforms. In this paper, the authors explained the architecture, security parameters, and challenges for implementation of blockchain in various applications.

Chen [36] discussed the tokenization of money that uses the blockchain. In this paper, the working of the token and their types such as token, initial coin offering, and its currency are discussed. Gatteschi et al. [37] explained whether the adoption of the blockchain in different industries can improve their productivity. Authors showed the blockchains has been used in various smart applications. Authors also described the functionality, architecture, techniques used, security parameters, and open research areas. Kumara and Mallickb et al. [38] explored the blockchain security, issues and challenges in IoT systems. They discussed various existing security and privacy issues related to IoT devices and the possible solutions by the adoption of blockchain technology [39]–[41]. Konstantinidis et al. [42] presented various blockchain-based smart business applications.

From the above-mentioned proposals, we found that most of the recent surveys on the blockchain technology have concentrated on various smart application areas in Industry 4.0 and its security parameters [43], [44]. The comparative analysis of pre-existing surveys on Blockchain with the proposed survey is given in Table 1.

B. RESEARCH CONTRIBUTIONS OF THIS PAPER

Following are the research contributions of this paper:

- A detailed taxonomy of blockchain-based Industry 4.0 applications is presented.
- A reference architecture having various modules and components for applicability of blockchain in Industry 4.0 is presented.
- The merits and demerits of the current security solutions which are applicable in Industry 4.0 are discussed.
- Finally, the Open issues and challenges in Industry 4.0 based smart applications are presented.
TABLE 1. Comparative analysis of pre-existing surveys on Blockchain with the proposed survey.

| Author            | Year | Objective                                                                 | Pros                                                                 | Cons                                                                 | 1 | 2   | 3 | 4 | 5 | 6 | 7 | 8 |
|-------------------|------|---------------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|---|-----|---|---|---|---|---|---|
| Motter et al. [5] | 2018 | To explore the innovation in healthcare with Blockchain technology       | Database ownership is available with healthcare specialties to counter  | Security compliance is missing                                    | X | X  | X | X | X | X | X | X |
| Yin-Hussain et al. | 2018 | To review the current research on Blockchain                             | Uses decentralized environment for transactions; Provides research     | Not mentioned about the future implementation with Blockchain        | X | X  | X | X | X | X | X | X |
| Abrahim et al.    | 2017 | To explore the innovation in blockchain                                  | Maintains precise health information patients with proper access      | Not discussed security and data access issues                       | X | X  | X | X | X | X | X | X |
| Wold et al. [5]   | 2017 | To implement a healthcare system with Blockchain technology              | Eliminates entity control and multi-party failure; Transactions are  | Mobile bandwidth and stable data usage are major constraints        | X | X  | X | X | X | X | X | X |
| Zhang et al. [5]  | 2017 | To evaluate the matrix of Blockchain technology with respect to healthcare| Consider critical metrics important for the Blockchain technology      | Public blockchain regulations are not mentioned; cost of implementation is high | X | X  | X | X | X | X | X | X |
| Liu et al. [5]    | 2017 | To explore the advanced blockchain architecture for e-health systems     | Distributed databases, peer-to-peer transmission, transparency, and    | Analysis of different application domains is not done               | X | X  | X | X | X | X | X | X |
| Duan et al. [5]   | 2017 | To explore the applications of Blockchain technology in education domain  | Security compliance is missing                                       | Public blockchain regulations are not mentioned; cost of implementation is high | X | X  | X | X | X | X | X | X |
| Radunova et al.   | 2018 | To explore the opportunities of Blockchain technology in the field of medicine | Cost-effective, optimized, secured, and personalized access to stored | Lack of scalability and data access control                        | X | X  | X | X | X | X | X | X |
| Kalani et al. [45] | 2018 | To describe how Blockchain is applied in various domains in the developed countries | Application-specific solution is presented; not applicable in other domains | X | X  | X | X | X | X | X | X |
| Pietrusiak et al. [5] | 2018 | To give an overview of the Blockchain, Bitcoin, and Ethereum             | Provides abstract layering of transactions                            | Mining difficulty after every 2016 blocks in Bitcoin; Unclear except cryptocurrency are not discussed | X | X  | X | X | X | X | X | X |
| Cerny et al. [45] | 2018 | To explore the tokenization of assets using Blockchain and Token          | Describes Initial Coin Offering (ICO) mechanisms                     | Not discussed the other applications area                          | X | X  | X | X | X | X | X | X |
| Gettink et al. [4] | 2016 | To decide whether to use Blockchain                                       | Highlights Blockchain innovations such as transparency, automation,    | Not discuss issues related to large-scale IoT implementations       | X | X  | X | X | X | X | X | X |
| Nikolaescu et al. | 2018 | To assess the security aspects of Blockchain                               | Describes important security parameters and issues for IoT domains   | X | X  | X | X | X | X | X | X |
| Kwon et al. [45]  | 2018 | To discuss Blockchain-based business applications                         | Illustrates blockchain applications sector-wise to Blockchain        | No architecture or implementation in proposed, results of the survey is not mentioned clearly | X | X  | X | X | X | X | X | X |

C. ORGANIZATION OF THE PAPER

The structure of the survey is as shown in Fig. 3. Table 2 lists all the acronyms used in the paper. Rest of the paper is organized as follows. The background and history of the blockchain technology is presented in Section 2. A reference architecture of blockchain is discussed in Section 3. In Section 4, blockchain deployment for various smart applications is discussed in detail. Then, Open issues and research challenges in smart applications are presented in Section 5. In Section 6, two case studies on smart farming and tourism and hospitality are presented to give more insights to the readers. Finally, in Section 7, the paper is concluded with future research directions.
II. BACKGROUND AND HISTORY OF BLOCKCHAIN

A. TRADITIONAL SECURITY SYSTEM AND BLOCKCHAIN

In the present era, most of the database systems use a centralized client-server based architecture. In this systems, a client (user) has the authority to modify the data stored in the centralized server. The control of the entire server database is with the centralized authority who can control and take decisions with respect to various access control policies defined on the data stored in the database. They also have the authority to authenticate users credentials before they access the database. To resolve the issues in the traditional centralized systems, blockchain can be an effective solution.

A blockchain is a chain of blocks which can be used to store and share data in a distributed, transparent and tamper resistant manner. Each block consists of data and is linked with other blocks using pointers. Such linkages ensure the integrity and tamper resistance in the blockchain. When a new data is added to the blockchain, link to the free end is created which extends the blockchain by one block or unit. As more data is added to the blockchain, it gets longer and chain grwos in size. If one of the blocks is modified in the chain, it breaks cryptographic links which disrupts the whole blockchain. It also allows the user to verify the integrity of the stored data.

The risk of the centralized control system can be eliminated with an implementation of decentralized systems. The database authority holds the centralized control on the security needed for all the users for the required access. The blockchain stores the data and builds the structural data storage which makes the network more secure. Due to this, the blockchain technology makes easy records or transactions with heterogeneous information in the databases.

B. BACKGROUND OF BLOCKCHAIN

The idea of blocks connection by cryptographic chains was introduced by Stuart Haber and Scott Stornetta in 1991. They designed a system, in which information or transaction stored with timestamps can not be modified or tampered. After that...
Bayer, Haber, and Stornetta proposed verification and validation of various transactions using the Merkle tree. In the Merkle tree, recorded data was gathered into a single block with an improved quality.

Satoshi Nakamoto created the initial blockchain network in 2008 [9]. He introduced the hash function method to create blocks in the chain. The major attempt was to improve the architecture and development of the blockchain in which there was no need of sign by the clients or the users. This implementation build the network for cryptocurrency recognized as bitcoin. The bitcoin network is publicly available ledger for all the transaction records. In his research work, blocks and chain were separate words which are combined together known as blockchain. They got the bitcoin network file size and the records of its transactions reached up to 20 GB by 2014, which went to 30 GB between the last quarter of 2014 to 2015. The bitcoin network was pushed from 50GB to 100 GB in January 2017.

The blockchain is used in the finance or cryptocurrency applications as it enhances the quality of various applications with respect to speed, security ease of use, and confidentiality. To explore the possibilities of applying blockchain technology in various industries, many companies have established their research centers for growth of this technology. For example, IBM has its research center in Singapore which was inaugurated in July 2016. In November 2016, the group of world economic forum discussed the development of the governance models for the blockchain technology. The global blockchain forum introduced the chamber of digital commerce in 2016 by Accenture’s trade group. Emma Macclarkin suggested the use of blockchain to enhance the trade which was executed by the European parliament’s trade in 2018.

How blockchain revolutionized: The revolution of blockchain technology from inception to till today is explained in detail as shown in Fig 4.

1) BLOCKCHAIN 1.0
The first generation of the technology was started with the bitcoin network in 2009, which is known as blockchain 1.0. In this generation, the creation of the first cryptocurrencies was introduced. The idea was all about payment and its functionalities to generate cryptocurrency.

2) BLOCKCHAIN 2.0
In the second level of the blockchain technology, smart contract and financial services for various applications were introduced in 2010. The development of blockchain with Ethereum and Hyperledger frameworks was proposed in this generation.

3) BLOCKCHAIN 3.0
In this generation of blockchains, the convergence towards the decentralized applications was introduced. Various research areas such as health, governance, IoT, supply-chain, business, and smart city were considered for building decentralized applications [46]. In this level, ethereum, hyperledger, and other platforms were used which having the ability to code smart contracts for a variety of decentralized applications [47], [48].

4) BLOCKCHAIN 4.0
This generation mainly focused on services such as public ledger and distributed databases in real-time. This level has seamless integration of Industry 4.0-based applications. It uses the smart contract which eliminates the need for paper-based contracts and regulates within the network by its consensus [49].

Blockchain Requirements:
- **Smart Contracts**: It is a protocol which allows the performance of transactions in absence of third party that makes transactions irreversible and traceable.
- **Tokenization**: It is one of the most important things that must to be included in the blockchain. It facilitates digital representation of the goods, services, and rights with the help of tokens. It allows the exchange of values and trust for different users without involving the central authority.
- **Data security**: Security compliance is a major and essential requirement of blockchain technology with a legal point of view.
- **Decentralised data storage**: It is a basic requirement of the distributed system.
- **Immutability**: All the records on the network should not be modified or tampered in the shared ledger. This enables the integrity of the stored data.
- **Consensus**: Transactions should only be updated when all the verified users in the network agree for the same.
- **Typed Blocks**: It is required for the smart contract and for high speed payment in business transactions. So, data formatting of the different types of blocks include its time, consensus algorithm [50], number of transaction per blocks, and its content data types.
- **Sharding**: It is required for the separation of content over subsets of nodes in a way, that not all the nodes need to carry all processing load or any burden.
- **Access rights management**: Encryption based private and public key cryptography and distributed databases with user identification is required to assign and manage access rights.
Standards used to manage permissioned blockchains:
Immutability of the blockchain network makes the data access in a specific order. The public certificates are available in public blockchain, but without having the private key, authorization cannot be provided to the users. So, all the data should be managed in order of data elements like user’s internet protocol (IP) address, name, its code, and extensible markup language. These all are published to the consortium with the communication process.

Standard data formatting: In the blockchain system, it is also needed to standardize the data formats with respect to Application Programming Interfaces (API). Each organization in the blockchain network needs to use the same data format or APIs to communicate in the same network.

Updatability: The need for data updation in the distributed ledger is most important for records. In a peer-to-peer network, data needs to be structured and systematically updated for each node that transacts within the network.

P2P encryption between blockchain nodes: Encryption is needed to secure the transactions between the end nodes that may link together in the blockchain protocol.

UX: One of the major factors in a system is the user interface design that provides an easy and convenient application environment to the users. The main difference between the blockchain-based and non-blockchain-based systems is the manner in which the user perceives it.

Development operation: The main step in the production of the system is the selection of platforms that requires less time and the setup complexity.

III. BLOCKCHAIN ARCHITECTURE AND ITS COMPONENTS

A. BASIC BLOCKCHAIN BASED ARCHITECTURE

In the basic architecture of the blockchain, each transaction needs to be verified which can not be altered as shown in Fig. 5.

1) ADDITION OF TRANSACTIONS IN THE BLOCK STRUCTURE

A blockchain transaction has various steps. First, a network node or user requests for a new transaction. After that, the transaction is recorded in the block format or structure. The block structure consists of the index, time-stamp, data, previous hash, and current block hash.

2) TRANSMISSION TO PEER NODES

A block of transactions is broadcasted to the peer nodes available in the network.

3) VALIDATION OF TRANSACTIONS

The blockchain network uses SHA-256 algorithm for creating a unique hash. Each block in the blockchain is linked with the hash of the previous block which makes an unbreakable network of transactions. If someone tries to append a transaction, then it must be validated by the network nodes or by smart contracts, and consensus. This immutable ledger cannot be modified, it can only be appended to the transaction of blocks, which results in a secured and reliable decentralized system. Various algorithms are used to validate transactions and user status.

4) BLOCK ADDED TO LEDGER

The new transactions are first verified by the other nodes and then they are added in a new block for the ledger or chain. The existing blockchain is extended by addition of a new block that is unalterable and undeletable for any other users.

B. REFERENCE ARCHITECTURE

The blockchain reference architecture consists of three different networks which combine together and run the whole blockchain application for the users. The three different networks are the public network, cloud network, and enterprise network as shown in Fig 6. Each has its own capabilities and functionalities for the smooth working of the decentralized applications.

1) PUBLIC NETWORK

In this network, the users, edge services, and peer cloud providers are connected or linked together.

a: USERS

In the public network, the users manage the distribution and creation of the blockchain decentralized application and execute the operations with the help of the blockchain network. Users have different roles as follows:

b: DEVELOPER

Developers make various types of applications for the client or users with different functionalities. They develop the smart
contract for the interaction with the users which helps to add transactions or records within the blockchain network. The developers can also build the inheritance applications for facilitating communication in the blockchain.

c: ADMINISTRATOR
The functionality of the administrator is to produce, maintain, and configure decentralized applications for the blockchain network.

d: OPERATOR
Operators have the control to monitor and manage the blockchain network and its applications.

e: AUDITOR
The blockchain auditors maintain or review the history of the transactions over the blockchain network for business and legal compliance point of view.

f: EDGE SERVICES
These services authorize the information that gets transferred via the internet to the cloud, enterprise applications, and client applications. They maintain systems such as domain name systems, content delivery networks, firewalls, and load balancers. Domain name systems are used to correct the Uniform Resource Locator (URL) of the web sites that are linked to the Transmission Control Protocol-Internet Protocol (TCP-IP) address for the system which is to be used for the resources. The content delivery network carries user applications, which gives the geolocation for the distributed systems which are installed to minimize the response time for the distributed users in the network. The firewall is responsible to maintain and give access control to the incoming and outgoing traffic in the network allowing or blocking the access. The load balancers are used for the distribution of the network traffic to maintain minimum response time, latency, and maximize throughput across the resources such as computers, processors, and storage systems. They are needed to balance the load in local and global systems.

2) INTERACTION OPTION
In the blockchain, there are various ways through which users can interact with the blockchain network, they are shown below as:

a: SOFTWARE DEVELOPMENT KIT
The SDK is useful for facilitating interaction between applications and their platforms. Blockchain application development lifecycle has a number of phases such as developing phase, debugging phase, testing phase, and production phase. The blockchain applications need to interact and communicate with the network when the software development cycle executes.

b: CLIENT SOFTWARE DEVELOPMENT KIT
It is a client-side programming library, which provides API methods to be used by the end user program to give access functionality within the blockchain network. The programs
are written in Java, Python, and other languages and the kit also supports development tools.

c: COMMAND LINE INTERFACE
Developers and administrator usually need activities such as monitoring, managing accounts of users, and importing & exporting some text commands formats. All these activities can be executed through the command line interface.

3) CLOUD NETWORK
The cloud network consists of a variety of running nodes, each with its own capability and functionality. The cloud network includes the blockchain applications, application programming interface, blockchain services, security services, and system integration.

a: BLOCKCHAIN APPLICATIONS
There are various types of applications such as web application, end-user applications and server-based applications. Users play different roles such as business users, administrators, auditors, and operators. The blockchain applications use the APIs for the post and get services of the resources like databases. A variety of applications such as healthcare, financial sector, insurance, energy domain, supply-chain, and IoT can be enabled with the blockchain to minimize the cost and time [51]–[56].

b: APPLICATION PROGRAMMING INTERFACE
An API is useful for the developers and users to reuse the data or information and its analytics with their services. It can be called by different cross-platform technologies. Blockchain technology provides various APIs for the application interfaces to use the components that can be handled in the business transactions.

c: BLOCKCHAIN SERVICES
For the performance and functional environment of the blockchain systems, there is a range of services such as:

d: MEMBERS
This service manages the user ids, credentials, and the history of users transactions in a confidential manner over the blockchain network. The permissioned network needs to validate the users of ongoing transactions and the users identification for the record of transaction and verification, so it requires membership in the network. In such networks, users have the access control to allow or block the transaction. In a non-permissioned network, it does not require the authorization by the user while submitting the transaction details.

e: CONSENSUS
Consensus is a protocol in the blockchain network, which must be followed by each node in the network. This protocol specifies time validity and rules that need to be followed by all the nodes or users in the network to perform various tasks or append transactions in the blockchain network. It also maintains a copy of the ledger in the network.

f: LEDGER
All the transactions are linked together with a cryptographic hash in the blocks to form a ledger.

g: SMART CONTRACT
In general, a smart contract is a chain of the codes, which executes in the blockchain network environment. This code chain communicates the conditions or rules for different parties to follow the terms between the nodes or users in the network. Smart contract can be developed in the blockchain platform with the help of the supported programming languages.

h: SECURE RUNTIME
In the secure runtime environment, blockchain transactions are added in the ledger with the secured container such as secure OS, and library of the programming language runtime used.

i: EVENT DISTRIBUTION
In the blockchain network, the publisher notifies the subscribers for a specific event. The notification is sent in a broadcast manner within the network. Subscribers who subscribe to a specific publisher or events receive the notification.

j: SYSTEM INTEGRATION
The blockchain services and the enterprise network are combined or integrated together via the application programming interface and enterprise service bus.

k: CONNECTIVITY
The connectivity between the cloud network and the enterprise network is established by the Virtual Private Network (VPN) or the gateway tunnel. It enables the secure connectivity and standard data format and filters within the blockchain network.

4) ENTERPRISE NETWORK
The enterprise network consists of the enterprise directory, its applications, and the database.

a: ENTERPRISE USER DIRECTORY
In the enterprise applications, data or information regarding user authentication, authorization, and personal data of users are recorded. The gateway and virtual private network (VPN) maintain secured services for the access control of the users.

b: ENTERPRISE APPLICATIONS
These applications are used for the enterprise that communicates with the blockchain network. They also communicate
with smart contracts in the network. Hence, smart contract collect and store the enterprise data in the network and share that information over the applications. They also make requests for availing the services in the blockchain network.

c: ENTERPRISE DATA
The enterprise application in the blockchain records and maintains the metadata of the system. It also maintains the feedback of the system that contains the entire history of the blockchain network. Transactional data contains all the records of the network which includes master repository, financial information, and business communication. All the data is available via data repository and distributed data storage. The second type of blockchain enterprise data is application data in which, data is collected and produced by enterprise applications and its operations. All the values are added for a better understanding of the application performance. The log data is recorded in log files for future inspection for the security, governance, or compliance.

IV. BLOCKCHAIN DEPLOYMENT IN SMART APPLICATIONS
The detailed taxonomy of blockchain deployment in real-time applications such as energy, healthcare, manufacturing, agriculture, business, digital content distribution, smart city, IoT [57], supply-chain & logistics, and tourism & hospitality [58] is shown in Fig. 7. Table 3 provides the detailed relative comparison of the State-of-the-art proposals/Tools used for blockchain-based security system. Parameters used for this comparison are objectives, techniques used, setup type, programming languages or simulators, pros, and cons of the existing tools/frameworks.

A. SUPPLY CHAIN AND LOGISTICS
Agricultural applications need critical management inputs, such as supply-chain management (SCM) which plays a prominent role in human lives. Traditional logistic systems used in food-supply and agriculture simply store the orders and delivered them to the destination. These conventional systems have a lacuna with respect to various features such as auditability, traceability, and transparency [59]. However, in the modern digital era, these features can improve safety and food quality, and hence, there is a huge demand of good quality of food by consumers [60]. Hence, most of the research & development (R&D) organizations adopt IoT technologies such as wireless sensor networks (WSN), and radio frequency identifications (RFID), which remotely observe the food supply-chain.

According to Caro et al. [61], most of the centralized cloud infrastructures are being used as current IoT solutions in SCM. These infrastructures usually have open issues like data integrity, lack of transparency, tampering and single point of failure. These issues can be handled in an efficient way by using blockchains. Decentralized trustful systems can be designed for the same by using the blockchain. A decentralized, blockchain-based solution named AgriBlockIoT, was proposed in [61] for Agri-Food SPM. It integrated various IoT sensor devices which produced and consumed data along the chain. The stored data can be accessed, and autonomous executable smart-contracts could be implemented through AgriBlockIoT, with the objective of achieving transparency, and inflexibility of the records in an environment, that uses modern devices such as mini-PC and gateways. The performance and efficiency of AgriblockIoT are quantified in terms of CPU load, network traffic, and latency. The performance can be improved by working on the constrained hardware architectures.

Perboli et al. [62] suggested that the blockchain improves the reliability, efficiency, and transparency of supply-chain, and speedup inbound processes. Though many IoT technologies are used for food safety and SCM, there are some issues which are not properly addressed. The major issue is to decide
TABLE 3. State-of-the-art proposals/Tools used for Blockchain-based Security system.

| Author(s) | Year | Objective | Technique Used | Security/Privacy | Coding | Opener | Price | Cost |
|-----------|------|-----------|----------------|-----------------|--------|--------|-------|------|
| U. Bodkhe et al. | 2019 | To implement a global and decentralized blockchain protocol for secure and efficient communication with low latency. | Distributed blockchain network | Not available | Not available | High | Not available | High |
| Weber et al. | 2019 | To improve the information sharing and traceability of supply chain transactions. | Blockchain-based smart contracts | Not available | Not available | High | Not available | High |
| Leng et al. | 2019 | To present an Agricultural Supply Chain (ASC) system based on the double chain architecture. | Distributed ledger technology | Not available | Not available | High | Not available | High |

whether the information or data shared among the members of other supply-chain is trustworthy or not. To overcome this issue, authors of [60] proposed a system called Hazard Analysis and Critical Control Points (HACCP), which provided real-time food tracing information to all SCM members and had features like reliability, openness, neutrality, security, and transparency.

Weber et al. [69] proposed a blockchain based decentralized solution to solve the problem of determining if the information or data shared among the members of the supply-chain is trustworthy in collaborative processes. They also discussed various notations and process models for business.

The prototype model was implemented using blockchain and validated through business processes [70]. To execute business transactions securely, a model called business process management (BPM) was proposed by Guerreiro [71]. This model used the blockchain technology and an Enterprise Operating System (EOS). The risk involved in the secured execution of business transactions was eliminated in the proposed model by increasing trust, authenticity, robustness, and traceability against fraud.

An Agricultural Supply Chain (ASC) system was presented in [68] by Leng et al. This system was completely dependent on the double chain architecture which accelerated...
TABLE 4. Supply chain management with blockchain technology.

| Author               | Year   | Objective                                                                 |
|----------------------|--------|---------------------------------------------------------------------------|
| Mao [72]             | 2018   | To adopt blockchain network in food-supply chain management               |
| Leng et al. [68]     | 2018   | To implement double chain architecture                                     |
| Chen et al. [61]     | 2018   | To adopt blockchain network in food-supply chain management               |
| Sinz [67]            | 2018   | To adopt blockchain network in food-supply chain management               |
| Kajjou et al. [64]   | 2018   | To adopt blockchain network in food-supply chain management               |

Table 4 provides the detailed relative comparison of the existing blockchain based approaches for supply-chain & logistics systems using the parameters such as transparency, reliability, security, architecture, consensus mechanism, traceability system, framework, pros, and cons of the existing approaches.

B. ENERGY DOMAIN

Energy is the actual base of our existence. It is essential to the lives of humans and all other living organisms on earth. Humans and all the living creatures on the earth cannot survive in the absence of energy. We use energy for a vari-

the efficiency of the blockchain in the ASC. The authors suggested solutions to provide adaptive rent-seeking and matching mechanisms for public service platform. These solutions ensured transparency, security and privacy of the enterprise information. Moreover, the use of public service platform and the efficiency of the system were also improved. The proposed system had drawbacks mainly in terms of performance and increased size of the blockchain.

Mao [72] proposed a credit evaluation system which was based on public blockchains. This system helped in the management and supervision especially for the food-supply chain to improve the effectiveness. In particular, the authors gathered the credit evaluation text from the traders by smart contracts on the blockchain, and then analyzed the text using a deep learning method named Long Short Term Memory (LSTM). Though the authors claimed the effectiveness of their method, they did not consider the overall system costs and benefits. Due to these issues, they can not provide a standard methodology to design, develop, and validate the overall blockchain solution. Later on, the authors in [62] concentrated on one of the most critical issues, i.e, the implementation of the blockchain in the supply-chain with the need of including all the different actors. Moreover, the sharing of information along the entire blockchain could lead to inertia in adopting the solution. For this reason, a correct implementation of the blockchain technology in the supply-chain must starts from an analysis of the needs and the objectives of the different actors involved. Keeping this objective in mind, the authors created a business model capable of highlighting the returns in terms of both economic and customer satisfaction.

Kshetri [65] presented an early evidence of linking the use of the blockchain in supply-chain activities to increase transparency and accountability. They also examined how the blockchain is likely to affect the key SPM objectives such as cost, quality, speed, dependability, risk reduction, sustainability, and flexibility.

A public blockchain of the agricultural supply-chain system based on the double chain architecture was proposed by Leng et al. [68]. In this system, the authors mainly focused on the dual chain structure and its storage mode, resource rent-seeking and matching mechanism, and consensus algorithm. The results exhibited that the double chain structure based agricultural supply-chain could take care of the openness and security of transaction information and the privacy of the enterprise information. It also had the ability to complete rent-seeking and matching of resources self-adaptively. Therefore, the proposed architecture greatly enhanced the credibility of the public service platform and the overall efficiency of the system.

Table 4 provides the detailed relative comparison of the existing blockchain based approaches for supply-chain & logistics systems using the parameters such as transparency, reliability, security, architecture, consensus mechanism, traceability system, framework, pros, and cons of the existing approaches.
TABLE 5. Energy applications with blockchain technology.

| Author | Year | Objectives | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Notes |
|--------|------|------------|---|---|---|---|---|---|---|-------|
| Kos et al. [73] | 2016 | To utilize automation of electric vehicle charging stations with blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Transparency, efficiency, real-time update in transactions, scalability |
| Swank et al. [74] | 2017 | To develop decentralized energy production and consumption using geos blockchain | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | Tracking of records, easy maintenance, optimization |
| Nene et al. [75] | 2018 | To manage energy requirement with micro grid network | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | Organized, trustable operations, eliminates intermediaries, privacy, social cohesion, inclusiveness, solidarity |
| Truly et al. [76] | 2019 | To reduce regulatory compliance for increasing the energy consumption | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | Enhanced trust, security, legal and policy tools |
| Nappa et al. [77] | 2020 | To maximize vast range of services in distributed energy system | X | X | X | X | ✓ | ✓ | ✓ | Monitoring, sharing and trading financial flows; emission of records |
| De Cistis et al. [78] | 2021 | To secure decentralized energy resource management using erasure blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Easy identification and authentication using smart contract |
| Kong et al. [79] | 2022 | To develop energy trading platform for homes in micro grid infrastructure | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Automation of renewable micro grid energy and its trading, implementation |
| Hinterberger et al. [80] | 2023 | To discuss potential impact of blockchain solution on energy markets | ✓ | X | X | ✓ | ✓ | ✓ | ✓ | Reduced costs and efforts, efficient processing |
| Ashley et al. [81] | 2024 | To establish trust for renewable energy credits over the system | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Secure and transparent distributed ledger, smart contracts |
| Plaza et al. [82] | 2025 | To implement distributed solar grid consumption and blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Smart meters, reduced cost, distributed consumption |
| Wang et al. [83] | 2026 | To explore contract based energy blockchain for securing electric vehicles charging with smart community | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Improved energy efficiency and sustainability, energy generation |

1. Distributed energy system 2. IoT 3. Micro grid network 4. Architecture 5. Smart meter 6. peer to peer trading 7. Renewable energy sources

Energy of purposes like food, Communication, transportation, heating/cooling, and lighting. All conventional transportation means such as trains, buses, automobiles, and airplanes work on energy, which is derived from electricity, and fossil fuels. Our food is grown with considerable energy expenditure, and its storage and transportation also consume energy. Our modes of communication, such as internet and telephones run on electricity. Sun is the major source of all energies available on the earth. It is very important to select the type of energy resources carefully, because it can lead to adverse effects on the environment such as global warming, and pollution.

Energy resources are classified into two categories: nonrenewable resources and renewable resources. The exponential use of non-renewable resources may lead to rare existence of these resources. So, it is very important to manage them with intense care and proper management. Proper usage of non-renewable resources has become mandatory due to their scarcity. The use of renewable energy sources such as solar power or wind can leverage energy efficiency to maintain the ecosystem [84]. Hence nowadays, most of the countries encourage their people to use renewable energy resources for the growth of their industries, agriculture, and transportation.

1) DISTRIBUTED ENERGY SYSTEM

Distributed Energy System (DES) is one of the important concepts in the energy domain. DES generates power on decentralized levels. It also enhances the overall throughput quality of the energy system by considering the parameters like energy production, economics, and environment. DES overcomes the many challenges of the centralized energy network systems and maximizes the use of renewable sources for a distributed generation of energy. With the use of IoT, Artificial Intelligence (AI) and Machine Learning (ML), DES has made it quite simple to monitor and maintain data and records. With its due popularity, DES has brought a significant improvement in the sector of electric utility which gives the ambit for the expansion of renewables empowered digital services.

Nowadays, there are many evolving technologies available which can simply convert energy into a digital. Using such technologies, we can keep a closer watch on a DES which is placed at a remote location. Moreover, the IoT plays a vital role in energy transitions and hence is adopted by DES. The presence of the blockchain and IoT facilitates a wide range of services enabled by the DES. In fact, the blockchain technology and IoT get the credit of giving a digital look to DES for energy transitions. The application of the blockchain in DES helps it to have a trustworthy data flow among emission traders, energy traders, energy producers, and operating staff. Digital DES offers a high level of security, and scope for decision making and processing based on the real conditions. The blockchain also helps to generate energy efficiently. There are numerous scenarios where energy sharing DES is more appropriate and better than the conventional DES. The Blockchain technology provides a decentralized energy trading platform for the imports and exports of energy, which can monitor electricity flows and aid to maintain them by time stamping [77].

DES is a truly intelligent system that provides a broad range of services in various stages such as the operating stage, development phase, energy trading stage, and energy metering phase. Authors of [77] did not highlight the issues like old grid infrastructure, reliability, energy loss, stability, environmental concerns, obsolete design, less efficiency in transmission, generation and distribution.

Truly [76] described how to improve environmentally sustainable development of the blockchain applications. Their study was based on the fiscal policy and regulatory approaches for the digital currencies [54]. This research led them towards the proposal and establishment of some
new policy tools and legal tools which are required for the consumption of energy with the usage of blockchain technologies. Authors [76] also came up with the fiscal policy for the same purpose and suggested the use of the blockchain technology.

2) MICROGRID
Small-scale power stations which have their own production as well as storage resources are known as microgrids. A microgrid always has definite boundaries. It can be perceived as a tiny cluster of electricity users who have a local source of electricity supply. The clusters are connected to a national grid which operates independently. If a microgrid is connected to the main grid, it is known as a hybrid microgrid. Decentralized Energy Resources (DER) such as diesel generators, PV Panels and a group of loads are integrated with Energy Storage Systems (ESS) like flywheels and batteries to form a microgrid and provide electricity [73].

Decentralized flexibility created by renewable energy sources can be easily reduced by approach, i.e., microgrids. Goranović et al. [85] suggested the two approaches for controlling electric grids, i.e., decentralized and centralized monitoring systems. In the centralized monitoring systems, an operator is accountable to execute the whole system. The use of centralized control devices needs expensive infrastructure. Centralized systems measure and process the data and then set proper proceeding in the circumstances. Multiple points can be made available in the system through which information is sent and received by the communication channels and centralized control devices. The major drawback in this mechanism is that the use of multiple points in the centralized system increases the probability of system failure. This limitation of the centralized system can be conquered by the decentralized system where each device independently controls itself. The decentralized system also improves the fault tolerance and communication speed of the system. The decentralized blockchain is precisely suitable to implement business processes in microgrids using smart contracts [86]. Authors of this paper also provided a few examples of the blockchain projects for microgrids with certain technical parameters. The type of the blockchain, consensus mechanism and availability of parts required in the hardware development or open source were the technical parameters considered by the authors for describing the example microgrid projects [85]. A brief summary of these projects is given below.

I) PowerLedger: It was a blockchain based market clearing & trading mechanism [87]. It included the use of private Ethereum with Proof-of-Work (PoW) and public eco-chain that employed proof-of-Stack (PoS). This was an open source project.

II) Share&Charge: It was a group of Electric Based Vehicle (EBV) charging stations [88] which used public Ethereum and consensus algorithm as a PoW. Owners can register his or her station to fix charging tariffs. Any charging station could be integrated and combined to Share&Charge network [73] through Share&Charge module.

III) NRGcoin: This framework was based on energy crypt-currency developed through a smart contract. It operated through gateways which simply calculated the flow of electricity and communicated through a smart contract.

IV) GrunStromJeton: It was an Ethereum based conceptual framework developed to verify the actual use of electricity. It used PoA as a consensus mechanism.

V) SolarCoin: It was developed to enhance the mass production of solar energy. Due to the lengthy setup process, customers usually do not go for solar installations. This project aimed at eliminating this problem by giving rewards to buyers. One solarCoin was given as a reward per produced MWh. It used PoA as a consensus mechanism and bitcoin as crypt-currency.

VI) GridSingularity: It was a decentralized data exchange framework specially designed for energy sector emphasizing on electricity, water, gas, and heat. In this platform, PoA and PoW were the consensus algorithms which used public Ethereum.

VII) Electron: It is a Company which works in the energy sector and provides Ethereum based better solutions. Apart from the above projects, people are currently working on numerous projects in the same domain. Table 5 provides the detailed relative comparison of the existing blockchain-based approaches in the energy domain using parameters such as the objective, transparency, reliability, security, architecture, consensus mechanism, traceability system, framework, pros, and cons of the existing approaches.

C. DIGITAL CONTENT DISTRIBUTION
Since the commercialization of the internet in 1994, delivery services of digital content has been increased exponentially. [89]. Delivery systems are mainly of two types: non-protected and protected delivery systems. Generally, digital content is protected using the conventional encryption mechanism. Different encryption mechanisms use different ways to generate, propagate, and maintain the keys and decrypt the encrypted content with keys. Traditional systems such as Conditional Access System and Digital Rights Management (DRM) are popular for protecting digital content, but face some major issues like network attacks, stealing of keys, and pirate attacking.

To overcome the drawbacks of the conventional centralized system, the authors of [89] proposed a decentralized digital content distribution system based on the blockchain. In this digital content system, the owner of the actual content could supervise and control the security as well as simplicity. The use of the mining techniques ensured that the addition of each type of transaction to the blockchain. PoW was used as the consensus mechanism to guarantee the security and privacy of the transactions stored in the blockchain. Due to some open issues such as pirate attacking, it was not possible to entirely control this mechanism.
Table 6 provides the detailed relative comparison of the existing blockchain-based approaches in the digital content distribution domain using parameters such as the objective, transparency, reliability, security, architecture, consensus mechanism, traceability system, framework, immutability of the blockchain, advantages, and drawbacks of the existing approaches.

| Author | Year | Objectives | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Peer | Case |
|--------|------|------------|---|---|---|---|---|---|---|-----|-----|
| Kishan | 2015 | To develop blockchain based digital content distribution system | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Access control mechanism, encrypted data in blockchain with no authority, permission based control system | Private attacking |
| Isman | 2015 | To achieve proof of majority for digital value by blockchain based smart contract | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Immutability of ledger; audit from distributed ledger | Lack of security, reliability, corruption |
| Fujit | 2015 | To achieve decentralized tampering by blockchain technology | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Hierarchical identity based encryption, unique identification for content distribution over distributed network | No Implementation |
| Key | 2017 | To ensure data distribution platform using blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Decentralized peer to peer consensus mechanisms for verifying transactions | Privacy management |
| Fing | 2018 | To develop a distributed and immutable blockchain framework | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Self-interlinking watermarking algorithm, detection of tampering and retrieval of original content | Revocation of metadata |
| Tanm | 2017 | To devise blockchain based information distribution for the IoT | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Robustness, resilience | Malicious gateways, privacy threats |
| Sun | 2017 | To create payment collection management system using extensible bitcoin | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Privacy of data, undetectable transactions, reliability, decentralized timestamped data | Counterfeiting, lengthy blockchain generation process, no technical extension |
| Wu | 2018 | To develop model for central bank digital currency | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Decentralization, transparency, flexibility | Privacy, supervision and transaction speed |
| Lai | 2018 | To support decentralization transaction method based on blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Decentralization, safety, effectiveness, reliability, flexibility | Lack of interoperability, limitation of scale and regulation, computing power |

1: Encryption system 2: Digital right management 3: peer to peer authentication 4: Content distribution 5: Architecture 6: Identity management 7: Conditional Access System

D. TOURISM AND HOSPITALITY INDUSTRY

Tourism is the process of spending time to outside station, i.e., away from our home for purposes such as business purpose, personal purpose, relaxation and pleasure. Serving travelers is the major functionality of the tourism industry. Nowadays, most of the people search and book their traveling tickets, food, and lodging online with the use of the internet. Therefore, the worldwide usage of the internet, the tourism and hospitality industry has witnessed rapid changes. In this digital world, many tourism companies like Expedia Group, BCD Travel, Uber, Ola, and AirBnb have replaced their traditional business models by Consumer-to-Consumer (C2C) models to achieve transparency and security in transactions. There is a huge demand for innovative platforms in the tourism industry, which can integrate technology, money, and knowledge.

TUI and many other companies have already started using the blockchain for implementing the functionalities like booking tickets and making payments. Many companies like Expedia, CheapAir, Webjet, and One Shot Hotels use bitcoins for the travel purpose, i.e., to book and reserve tickets. Digital currencies simply integrate with smart contracts which have enough potential to develop highly disruptive technologies for the tourism industry. Authors of [99] suggested three prepositions which helped to highlight some open issues in the tourism industry. These prepositions mainly focus on the customer’s point of view and market implementation’s point of view. The prepositions include: I) New Type of evaluation as well as review techniques which can build trustworthy systems for rating purpose. II) The extensive adoption of digital cryptocurrencies for C2C markets. III) Use of blockchain leads to increase of disintermediation in the tourism industry. In the case study part of our paper, we try to highlight the above issues in the tourism industry. The detailed explanation of the same is available in the case studies section.

E. SMART HEALTHCARE

Health is the most valuable asset of any nation. In traditional healthcare, all patient related data is stored in a centralized way and therefore, it is not advisable to give access of data to any untrusted third party. Moreover, the privacy and security of patient information must be maintained as it is vulnerable to a variety of attacks [121]. A centralized architecture cannot fulfill these requirements completely. Hence, smart healthcare is introduced to deal with the above mention issues in conventional healthcare systems. Smart healthcare focuses on monitoring and diagnosing patients’ health remotely through wireless communication channels. It collects the necessary information of various patients through heterogeneous wearable devices and sensors. Enormous data is collected for a large number of patients. It is a big issue to analyze and store this data in a secured manner. These data should also be shared securely among trusted parties such as hospitals, patients, doctors, and medical stores. Secure communication of these data is pivotal as it affects important decisions such as planning of new services in the hospital, recommending doctors, analyzing symptoms of different diseases or health issues, and improving the overall system to make it intelligent.

Table 7 provides a detailed relative comparison of the state-of-the-art healthcare security standards used for smart healthcare. These standards are compared using the parameters such as access management, security maturity, reduction in cost and complexity, and improvement in healthcare compliance. For the various medical research activities, deciding
treatments, and analyzing symptoms of diseases, patients’ data is required to be shared periodically. Traditional access control policies are not secured enough to share highly sensitive patient records from one party to another. Moreover, in most of the cases, patients do not share their medical history with the doctors. In case of a medical emergency, medical records of the patient are necessary, but the same is not available due to poor record maintenance. All the above-mentioned issues can be solved by smart healthcare using Electronic Health Records (EHR). Though smart healthcare is capable of solving the major issues in the healthcare industry, there are some challenges to be addressed. Access control policy for EHR, privacy, security, and availability, are open issues in smart healthcare. The blockchain technology can be used to get solutions to these issues. In fact, the blockchain has the potential to support smart healthcare through the distributed ledger among various users such as patients, doctors, medical stores, and insurance agencies.

Authors of [100] proposed a blockchain-based intelligent application commonly known as Healthcare Data Gateway (HDG). Patients can securely share and control their data through a secured data gateway. It processes and manages patients’ data without any concern about the third party. HDG consists of three layers namely Data Usage, Data Management, and Storage. Entities that use healthcare data such as physicians, companies, government, and researchers are associated with the data usage layer. In the data management layer, HDGs independently connected to each other. This layer also manages all types of metadata such as patients’ data, schemas, and indices information. The storage layer prevents the attacks on integrity and confidentiality by providing secure and scalable storage for the healthcare system.

Azaria et al. [101] developed a decentralized MedRec model which was a novel data management system for large scale EHR. In this proposal, confidentiality, authentication, and accountability of health records were maintained via a comprehensive log using blockchain-based MedRec model.

Authors of [102] developed a new architecture for the medical field especially for precision medicine and clinical trial. This architecture had four new components: I) Blockchain-based parallel and distributed computing component to examine parallel computing using data analytics, II) Trustworthy information sharing component to enable a trustworthy medical data system for collaborative research, III) Application data management component to maintain the integrity of data, and to integrate dissimilarity of medical data, IV) Verifiable unknown identity management component for maintaining identity privacy for IoT, person and devices as well as secured access to patient-centric medicine data.

Authors of [103] developed a reliable healthcare system on the basis of Pervasive Social Network (PSN) using different protocols. The first protocol was an extended version of IEEE 802.15.6 display authenticated association. It was used to establish secured links by means of unbalanced computational requirements for mobile devices and resource-restricted sensor nodes. Health data was shared between PSN nodes with the help of the second protocol which was based on the blockchain technique. The authors examined the proposed protocols and other factors for evaluating the performance. The proposed system demonstrated the possibility of using the blockchain technology, especially for PSN-based applications. Though the performance of the proposed system was not measured on a mass-scale healthcare system, i.e, PSN-based system, as stated by the authors, the performance of the proposed system could be improved in terms of transport and monitoring of the environment.

Authors of [104] discussed a viewpoint on the blockchain founded healthcare data management system. They also bestowed a framework for sharing, managing EMR, especially for the patients suffering from cancer. The proposed architecture included a user interface as well as the backend. The backend comprised of the components such as membership services, certification authority, clusters of nodes, load balancer, and distinct cloud storages for patients’ certificates and data. This work substantially reduced turnaround time for EMR sharing, increased the power of decision making for the sake of medical care, and also reduced the overall system cost. The proposed system also guaranteed the availability, security, privacy, and access control across the EMR data.

Xia et al. [105] developed a trustworthy blockchain-based system called “MeDShare” especially to handle the
TABLE 8. State-of-the-art blockchain based approaches to secure healthcare 4.0.

| Author            | Year | Objectives                                                                 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|-------------------|------|-----------------------------------------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Yu et al. [104]   | 2019 | To discover healthcare knowledge on blockchain with privacy and danger control | ✓ |   |   |   |   |   |   |   | X |   |   |   |   |   |   |   |   |   |   |
| Azaria et al. [105] | 2017 | To access medical data and permission management using blockchain          |   | X | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Shar et al. [106] | 2017 | To implement the design over blockchain for clinical trial and precision medicine |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X |   |   |   |   |   |   |   |   |   |   |
| Zhang et al. [107] | 2017 | To secure a network for extensive social network based healthcare          |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Dabiri et al. [108] | 2017 | To empower eHealth                                                        |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Xia et al. [109]  | 2017 | To create trustless medical data sharing among cloud service providers with blockchain |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Rifi et al. [106] | 2017 | To explore blockchain technology for eHealth data access                  |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Li et al. [110]   | 2017 | To align blockchain technology for data sharing and collaboration in mobile health image |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Magyar et al. [111] | 2017 | To resolve the privacy and availability issues for EHR data using blockchain |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Al-kahtani et al. [112] | 2017 | To explore the feasibility of blockchain in healthcare                      |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Jiang et al. [113] | 2018 | To implement the blockchain system for health data exchange               |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Thereskul et al. [111] | 2018 | To design a system for smooth healthcare data sharing                      |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Zhang et al. [114] | 2018 | To support flexible queries with access control to EHRs                     |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Li et al. [115]   | 2018 | To explore data protection system for health data                          |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Fan et al. [116]  | 2018 | To strengthen efficient and secure health data sharing with blockchain network |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Wang et al. [117] | 2018 | To ensure EHR system with cloud and attribute based cryptography and blockchain |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Radanovic et al. | 2018 | To explore the opportunities for blockchain technology in medical network   |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Kass et al. [118] | 2018 | To explore the future of blockchain based heterogeneous medicare information in cloud |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Urigga et al. [119] | 2018 | To develop healthcare system with smart contracts for secure automated remote patient monitoring |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Ozer et al. [120] | 2018 | To secure MAR scheme with multiple authorities for blockchain in EHRs        |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Vaida et al. [121] | 2018 | To explore continuous patient monitoring with patient-centric agents        |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |
| Sun et al. [122]  | 2018 | To explore decentralization based blockchain for healthcare                 |   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |   |   |   |   |   |   |

| Framework | Algorithm |
|-----------|-----------|
| Control and privacy | Access control |
| Privacy | Security |
| Identity | Data provenance |
| Integrity | Accountability |
| Traceability | Data provenance |

challenges of maintaining voluminous medical information on a cloud using big data for data provenance. Activities such as sharing and transition of information were recorded and stored in a tamper-proof manner. The authors also compared the performance of “MedShare” with the existing methods of data sharing and came up with the conclusion that auditing and data provenance could be achieved by cloud service providers through the MedShare. Risk factors of data privacy were also minimized through the proposed system, but issues such as scalability, data interoperability and key management were not highlighted in the paper. Rifi et al. [106] discussed the important problems such as scalability and interoperability, and highlighted the advantages of including the blockchain technology for medical data exchange to achieve the best performance.

Liang et al. [107] developed a user-driven health information sharing solution to handle the issues of privacy and identity management. To address these issues, they suggested the use of the channel formation scheme and membership service of the blockchain. The authors also proposed a mobile-controlled system based on hyperledger fabric with the use of permissioned blockchains. The proposed work majorly focused on the validation of the network nodes, and the preservation of healthcare-related data.

A new blockchain-based information model was proposed by Magyar et al. [108]. This model basically integrated complex Electronic Healthcare Data (EHD). The implementation of a decentralized and purely expendable network was possible due to the use of cryptographic tools and the blockchain. The model was developed by considering the basic beliefs
of the HIPAA regulation existing in America. The proposed work ensured information availability and resolved the issue of data privacy at the same time, although the authors did not provide any algorithm or method to handle the EHD related issues such as integrity, security, portable user-owned data, and interoperability.

Jiang et al. [110] focused on the fact that everyday huge number of healthcare-related data are produced by individuals and hospitals. This data is very beneficial in the medical industry for various purposes. It is quite challenging and important to store this data securely. It is must to have mechanisms to maintain confidentiality, privacy and integrity of data. By keeping these requirements in mind, the authors developed a BLOckchain-based model for Healthcare Information Exchange(BlocHIE), which resolved the above-listed issues. In this mechanism, they considered two types of healthcare-related data - personal healthcare related data and electronic medical records. They performed analysis of various ways and requirements to share and store the healthcare related data. The framework was based on two blockchains which were loosely-coupled and one was an EMR-chain and the other was a data-chain. Different methods and techniques of chain verification, as well as storage, were integrated to ensure authentication and privacy. The authors also developed two transaction packaging algorithms such as TP&FAIR and FAIR-FIRST for PHRD-Chain and EMRChain respectively, which increased the fairness, efficiency, and system throughput among the users. These two packaging algorithms were evaluated in terms of throughput and fairness using the BlocHIE mechanism. As claimed by the authors, the FAIR-FIRST algorithm increased the fairness and the TP&FAIR algorithm increased the throughput.

Nowadays the blockchain is being used worldwide in the medical field to maintain and store the healthcare related data securely. Theodouli et al. [111] said that this data could be used for further innovation and research in the healthcare industry. By considering the needs of the healthcare industry, the authors of [111] proposed a design architecture for a system which can easily secure permission management and data sharing for the healthcare with the help of the blockchain features. The proposed infrastructure consisted of three layers: Web/cloud platform layer, Cloud middleware layer, and Blockchain network layer. As shown in the paper, this model could help to enhance security and integrity to a good extent. This model was also used in the KONFIDO project to verify the parameters such as interoperability and data exchange. According to the authors, and the proposed model gave additional benefit with respect to workflow automation, patient pseudonymity, accountability, auditing, and data integrity.

Fig 8, gives an idea about the use of blockchain technology in smart healthcare. Table 8 provides a detailed relative comparison of the existing blockchain-based approaches for smart healthcare. Parameters used for this comparison are the objective, security, architecture, simulation tool or framework, hardware, and physical design, benefits and drawbacks of the existing approaches.

F. SMARTCITY

In smart city implementations, heterogeneous sensors are used by various smart devices and users to collect the required data. These data are processed and used in traffic management, transportation systems, waste management, schools, libraries, water supply networks, community services, and power plants to improve the performance. There is a gradual increase in the number of people living in city areas. Due to increased use of the Internet, big data [129], and IoT, the concept of a smart city has become very popular. To strengthen the development of the smart cities, we need effective mechanisms to solve the existing problems related to energy, transportation, governance, and environment. Some open issues such as deficient security in IoT, difficulty in maintenance and upgradation of equipment, maintaining the trust among the internet users, optimizing the cost of running data centers, damage resistance, privacy, and security need to be addressed to deploy smart city projects effectively and efficiently. According to the authors of [128], the blockchain technology is the potential of solving all these problems and hence, it is best suited for developing smart city solutions.

As we know, the consumption of energy increases due to urban development. The purpose of the internet is to develop an intelligent energy system. Authors in [128] mainly focused on how the blockchain could help to solve the problems in the internet, big data, and IoT [15], [16]. In this research, issues such as user’s creditability, the creditability of the data in the central database, data privacy protection, and privacy protection of data were addressed. In the proposed work, the blockchain identified valid IoT nodes and denied the system access by malicious nodes. It also maintained data privacy in IoT and improved storage and computing abilities with the help of decentralized databases. As shown in the paper, the proposed work effectively prevented various attacks on the network infrastructure with improved recovery mechanism in big data [130].

Various architectural issues in the network infrastructure of the smart city were discussed by Sharma and Park [126]. Due to the exponential rise in information volume as well as the increase in the count of connected IoT devices, different issues such as bandwidth, security, latency, and scalability emerge in the existing smart city frameworks. To address these issues, authors in [126] proposed a hybrid architecture.
for a smart city. It was divided into two partitions: edge and core network through the hybrid architecture scheme. Moreover, this architecture was developed by considering all the strengths of the distributed as well as centralized architectures. In this paper, the authors also suggested the PoW scheme to strengthen privacy and security. They simulated the proposed model by evaluating feasibility and performance based on different performance metrics such as latency, and throughput. Authors also came up with a software-defined networking (SDN) and blockchain-based hybrid network architecture, although they did not focus on important parameters like how to deploy edge nodes, how to enable the caching technique at edge nodes etc. Due to this research gap, there is a tremendous scope of work in this domain in the near future.

Biswas and Muthukkumarasamy [122] proposed a four-layer security based framework which was developed using the decentralized blockchain technology. It was integrated with smart devices that provided a secure and trustworthy communication model for a smart city. The proposed framework comprised of four layers: the physical layer, communication layer, database layer, and interface layer. In the physical layer, multiple standards were defined for smart devices using which data collected could be shared and integrated. The blockchain protocols were used to integrate with the communication layer to provide privacy and security of the transmitted data. The authors also suggested that the extensive use of the private ledger could lead to the improvement in performance, efficiency, and security for various real-time applications such as smart parking of vehicles, smart cleaning, smart home, and traffic control system in a smart city [131]. Scalability achieved by this framework was also up to the mark. As shown in Fig. 9, the proposed model had good features like fault tolerance, reliability, capability, and faster execution of the operation. Due to the use of the blockchain, various smart devices were able to communicate in a distributed environment. The major gap found in this paper is that the proposed model not missed to focus on some of the important issues like scalability and interoperability of the heterogeneous platforms.

Rivera et al. [123] defined a smart city as the use of information technology (IT) to make the life of citizens more better and comfortable [125]. A smart city is a digital world which interconnects various areas such as government offices, schools, healthcare, colleges, and the economy. Nowadays, the unique identity of users is the biggest concern in business and smart city environments. Many researchers and developers have attempted to develop a reliable technology which can accurately determine the users’ identities. These attempts have used various attributes such as name, address, health status, hobbies, and credit record of the users. The digital identity is significantly important as it plays a vital role in security measures for interconnected devices in a smart city. The authors of [125] failed to highlight some of the important issues like smart energy, architecture, and SDN based security in the development of a smart city.

In [124], Liao et al. focused on some important issues of smart cities like interoperability and transparency of various services. Due to the advancement in technology, fair and transparent services are demanded by the citizens in a smart city. Lottery game is an important segment in a smart city application, but it has a deficiency in terms of fairness and transparency. Therefore, the authors of [124] came up with an optimal solution to improve the transparency and fairness of a lottery system. They designed a blockchain-based transparent lottery system for a smart city. The authors proposed a three-layered blockchain-based lottery system known as FairLotto which used four lightweight protocols. Closing time, lottery purchase, initialization, and verifying winning numbers were the four different lottery stages in the proposed system. Equal possibility of winning the prize for each and every participant was guaranteed by this four-layered architecture. FairLotto effectively ensured transparency and did not store any financial transactions in the blockchain. Due to this, the transactional privacy was preserved and fairness and transparency were achieved in the lottery system. However, there was a lack of connectivity and service integration in the lottery system. Moreover, the authors also implemented Fairlotto system in Ethereum, but the results of the numerical analysis on the performance were not provided. These two were the major research gaps in the proposed work.

Table 9 provides a detailed relative comparison of the existing blockchain-based approaches for smart city applications. We use parameters such as the objective, digital identity, security, architecture, smart energy, smart parking and automation, smart traffic, green environment, advantages, and drawbacks of the existing approaches for making this comparison.

**G. BUSINESS**

The Blockchain is a decentralized technique used for the secured exchange of cryptocurrency and financial transactions. Each user maintains its distributed ledger which is useful for validating a new transaction. Bitcoin is a medium of digital cryptocurrency that provides transactions in a secured and distributed environment. The group of all executed
bitcoin transactions performed in the past is called a distributed ledger. After every successful transaction, an authentic user has to make changes in the distributed ledger which is distributed over the network and shared by all users in the network. As hash functions are used in the formation of the blockchain, data integrity, confidentiality, and privacy are maintained across all the transactions.

Singh and Singh [73] discussed the importance of blockchain in business, banking, and financial applications. It has enough potential to reorganize the business market industry. Use of block-chain reduces the risks, cost, probability of cyber attacks in financial organizations, and precise auditing of organizations can be achieved. Authors simply discussed the use of blockchain in the business application is highly desirable and convenient, due to its characteristics. They did not suggest any basic architecture for a business application to overcome the problems of blockchain like interoperability and scalability.

Nguyen [132] discussed that sustainable development in finance can be achieved through the inclusion of the secured blockchain. This technology could bring various benefits for the existing banking system as well as society. It could increase the speed and efficiency of execution, optimize the transaction time and networks of record keeping, reduce the cost of financial transactions, and improve the probable chances of accessing the financial market. Nowadays, still there are no complete legal rules and regulations for cryptocurrencies and bitcoins. Hence, the use of the blockchain is a big challenge in the payment industry.

Rimba et al. [133] provided a comparison of cloud services and blockchains for Business Process Execution (BPE). Based on the experimental results, the authors showed that the cost of Ethereum based process execution is higher as compared to the cost for business process execution on Amazon SWF, but authors ignored to formulate a method which could estimate the execution cost depending on the model as well as data collected in the past. Moreover, this paper did not describe how to minimize latency and execution cost.

Lundbak and Huth [134] discussed that consensus and trust could be achieved in a distributed network through the blockchain. Thus, many private and governmental sectors, central banks, insurance and finance agencies, academic institutions, and especially some startups in Europe focus on the implementation of the blockchain in their routine operations. Improper implementation of the blockchain may lead the industrial standards and agendas to non-secured operations. The authors of [134] devised an oligarchic approach to authenticate and secure business processes and data. Their approach shared the business data without exposing the sensitive information and resolved numerous issues of game-theoretic mining but it was not able to prevent uncertain behavior such as cheating.

The authors of [135] described an algorithm to ensure data confidentiality in an untrustworthy environment. This algorithm translated the Business Process Execution Language (BPEL) into a highly confidential smart contract, but this algorithm did not meet the basic security pillars such as data integrity, correctness, and authenticity. The implementation of the blockchain may help to resolve the above-mentioned issues.

Johng et al. [136] presented a framework to improve the trust in business processes using the blockchain. This framework mainly focused on issues like transparency and immutability. It also improved the trust among different stakeholders. Though the framework was not capable of resolving issues like traceability, the authors tried to build a process meta-model for supply-chain through the same mechanism.

An end-to-end model for Real Time Gross Settlement (RTGS) through hyperledger fabric blockchain platform was designed by the authors of [137]. The proposed system made the payment service more secure and efficient. It used a timestamp algorithm which resolved the problem of gridlock and the risk of privacy. This framework was not generic for diverse payment services. A more generic platform can be developed through the blockchain technology [138].

Mendling et al. [139] discussed the execution of business processes beyond organizational boundaries through the blockchain without the inclusion of any trusted third party, although the authors did not explain how to resolve the existing issues such as latency, bandwidth, throughput, and size in the proposed work.

Table 10 provides a detailed relative comparison of the existing blockchain-based approaches for the business

| Table 9. Smart city development with blockchain technology. |
|-------------------------------------------------------------|
| **Author**       | **Year** | **Objectives** | **Quality** | **Reliability** | **Interoperability** | **Scalability** | **Implementation** | **Security** | **Integrity** |
|------------------|----------|----------------|-------------|----------------|---------------------|----------------|--------------------|--------------|--------------|
| Burga et al.     | 2016     | To create smart city with blockchain technology | ✓            | ✓              | ✓                   | ✓              | ✓                  | ✓            | ✓            |
| Rhee et al.      | 2017     | To explore how digital identity can help smart cities with blockchain | ✓            | ✓              | ✓                   | ✓              | ✓                  | ✓            | ✓            |
| Luo et al.       | 2017     | To design a library system for smart cities with the help of blockchain network | ✓            | ✓              | ✓                   | ✓              | ✓                  | ✓            | ✓            |
| Lazarova et al.  | 2017     | To combine 30% and blockchain in smart city development | ✓            | ✓              | ✓                   | ✓              | ✓                  | ✓            | ✓            |
| Shanmugam et al.| 2018     | To develop a hybrid network architecture for the smart city | ✓            | ✓              | ✓                   | ✓              | ✓                  | ✓            | ✓            |
| Bulat et al.     | 2019     | To analyze the transformational effect of blockchain and IoT in smart cities | ✓            | ✓              | ✓                   | ✓              | ✓                  | ✓            | ✓            |
| Staling et al.   | 2019     | To express applications of blockchain in smart city infrastructures | ✓            | ✓              | ✓                   | ✓              | ✓                  | ✓            | ✓            |

1. IoT 2. Software defined network 3. Security 4. Digital identity 5. Architecture 6. Smart energy 7. Smart parking & automation 8. Smart traffic 9. Green environment
TABLE 10. Business in blockchain technology.

| Author | Year | Objective | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Pros | Cons |
|--------|------|-----------|---|---|---|---|---|---|---|------|------|
| Nguyen et al. [134] | 2016 | To develop sustainable financial technology with blockchain with business model | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ | Faster, efficient, time-optimized solution, reduced cost, access management | Incompleteness of legal regulations |
| Singh et al. [135] | 2016 | To explore future of finance in business and cyber security with blockchain technology | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ | Encrypted ledger, tamper-proof, decentralized registry | Lack of interoperability, scalability |
| Rumba et al. [136] | 2017 | To execute business process model with blockchain | ✓ | ✓ | ✓ | ✓ | X | ✓ | Cross-organizational, computational cost model | High latency, cost |
| Lin and Chien [137] | 2017 | To control logistic business to benefit blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Smart-theoretic mining incentives, immutability, anonymity, non-repudiation | Trustworthiness |
| Mondal et al. [138] | 2018 | To review sustainable business process execution on blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Trust, transparency, and accountability over business processes | Previous engagement on confidentiality and privacy |
| Joing et al. [139] | 2018 | To increase transparency of business process in Blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Distributed database, traceability, immutable ledger | Lack of trust, transparancy |
| Wang et al. [139] | 2018 | To develop secure healthcare system on business blockchain platform | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Distributed trust, confidentiality, gridlock resolution and reconciliation | Distributed system lack of security and recovery |
| MINDLENG et al. [141] | 2018 | To manage the business process management in Blockchain technology | ✓ | ✓ | X | ✓ | ✓ | ✓ | No single point of failure | Throughput, Latency, Size and bandwidth |
| Oak et al. [142] | 2018 | To create smart collaboration mechanism in business using Blockchain | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Smart contracts, collaborations, social networking, Consensus, Authorization, Secure Release, Non Repudiation | Increased latency, Increased Traffic, Complexity |
| Konstatiniotakis et al. [143] | 2018 | To review business applications of blockchain technology | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Smart collaboration, decentralization | Complexity |

1: Business process service 2: Trust management 3: Security 4: Architecture 5: Consensus transaction mechanism 6: cost model 7: Monetary policy

H. INTERNET OF THINGS

In the Internet of Things (IoT), various devices are connected through the internet to share useful information via servers for performing specific tasks or actions in the external environment such as measuring temperature or humidity and moving of shaft. Delivering the right information to the right people at the right time is possible through the use of IoT. Various sensors continuously sense the data and these collected data can be used for effective decision making. Things connected to the internet are expected to cross 50 billion in the near future, which is basically an approach of how these various devices should be designed and integrated with each other, so as to deliver a service delivery network, which can serve the needs in the future. The architecture of IoT is basically the backbone of any application and thus, it should be crafted carefully considering the needs of the evolution of functionality, scalability, availability, and maintainability. From this IoT architecture model, it is very clear to know that security is an essential factor in all IoT layers as shown in Fig. 10.

Nowadays, most of the IoT devices are not fully secured and can be easily hacked. These devices have restricted network capacity, limited computation power, and small storage capacity. Due to these characteristics, such devices are vulnerable to a variety of attacks as compared to computer systems. Samaniego and Deters [141] observed that the issues of network latency occurred due to cloud-centric IoT systems. To overcome these problems, they developed a software-defined IoT management construct known as Virtual Resources (VR). Tamper-proof, decentralized blockchains have the potential to solve security issues in any IoT Implementation. To use the blockchain as a service for the IoT, hosting environment is one of the challenges.

Edge devices have limited computational resources as well as bandwidth, thus making fog or cloud as the potential hosts.

The authors of [142] surveyed and categorized some important IoT related security challenges and requirements. The same were tabulated and mapped against the existing state-of-the-art solutions. The authors suggested the integration of the blockchain as a key solver for such challenges and also outlined the research issues which must be addressed in future, that could provide scalable, reliable, and efficient security solutions for the IoT.

FIGURE 10. IoT architecture model.
Singh et al. [143] observed that the current security technologies do not have the potential to secure IoT applications from various cyber-attacks in the business domain. They also suggested three different patterns of the blockchain-based security model for the IoT. There are various distributed ledger protocols suitable for the IoT implementation such as hyperledger fabric, Ethereum, and Internet of Things Application (IOTA) [144]. In this paper, the performance of these protocols was compared for the development of IoT applications. The authors also presented three different architectures for the same. The architectures differ in the position of key storage and Ethereum blockchain which enhanced the security and reduced the network traffic. The problem with these architectures was that they were not capable of monitoring the IoT devices' transactions automatically.

Huh et al. [145] developed a new way to manage a few numbers of IoT devices with the use of Ethereum and computing platform. They used three Raspberry Pis, and smartphones and proposed three smart contracts which used public keys and signatures to track meter values and save the values of light bulbs and air conditioners. Malicious attacks on smart contracts could be detected and ignored by the computing systems of light bulbs and air conditioners. However, the proposed work failed to resolve issues such as Denial of Service (DoS) and synchronization. Moreover, the proposed mechanism considered a small number of IoT devices and thus was unable to implement a full-fledged IoT system for multiple devices.

Liao et al. [146] presented various design issues and an architectural approach for the blockchain-based IoT services. Design decisions could be carried out by developers with the help of this architecture. Unfortunately, the proposed work failed to show the adverse effects on architectural attributes like robustness, efficiency, and security.

Reyna et al. [147] analyzed the major challenges of IoT Integration such as scalability and storage capacity, data privacy and anonymity, and consensus mechanisms. They identified the potential benefits of the blockchain for the IoT and also suggested different topologies for the integration. Some key points to enhance the performance and feasibility of IoT applications with the help of the blockchain was also discussed in the paper.

Table 11 provides the detailed relative comparison of the existing blockchain-based approaches for the IoT. This comparison has been done using parameters such as reliability, encryption, security management, edge computing, architecture, consensus mechanism, threat model, framework implementation, advantages, and disadvantages of the existing approaches.

I. MANUFACTURING

The process of manufacturing includes several elements such as operations management, asset management, intelligent manufacturing, planning, the interaction of humans and machines, performance optimization, performance monitoring, and end-to-end operational visibility.

Li et al. [157] stated that the IoT has converted the conventional manufacturing processes into a smart manufacturing process. The IoT enabled manufacturing is far smarter and efficient than cloud manufacturing, as it speeds up the flow of production especially in the manufacturing plant, management of inventories & warehouses, and observation of development cycles by using IoT devices. Due to this, most of the manufacturing companies have invested crores of funds in the implementation of the IoT applications. The use of the IoT in the field of manufacturing and logistics will rise to 40 Billion by 2020 [162]. Due to the characteristics of the IoT such as greater energy efficiency, predictive maintenance, higher product quality, reduced downtime, speed, and more informed decisions, it has various applications in the manufacturing plants [163]. As we know, energy is one of the largest expenses for manufacturing Industry, energy efficiency must be achieved which can be done through IoT based smart manufacturing.

The authors of [159] proposed a trusted FabRec prototype, which linked physical devices and various computing nodes through a decentralized platform. In this prototype, transparency was ensured through audit trails. In the decentralized network, the authors developed smart contracts for the autonomous interaction of nodes in the absence of human involvement. The proposed architecture used a proof of concept linked with the nodes and physical devices and enabled smart manufacturing. Cloud-based manufacturing basically use the centralized networks which have problems such as security, flexibility, availability, and efficiency.

To resolve such issues, the authors of [157] discussed and developed a blockchain-based distributed network architecture known as BVmfg. This architecture had a total five layers which improved the trust between the service providers and users for secured service sharing. The authors evaluated the performance of BCmfg a case study in which for fifteen end users and five service providers, scalability, and security were improved. Later, the authors revised their prototype and developed a shop floor and machine level data sharing prototype [160]. Authors used a public blockchain for shop level and a private blockchain for service providers through which important data is collected and gathered. The new prototype was level 2 Point-to-point (P2P) network implemented through the blockchain. It handled cloud manufacturing challenges like security and centralization effectively.

The authors of [158] proposed a blockchain and private cloud based manufacturing four-layer knowledge sharing system for Injection Mould Redesign (IMR). This work provided the rules and standards for the secured implementation of the system in a trusted environment. It also provided a knowledge sharing mechanism for the owners through which their data, as well as assets, could be shared securely among them. The system used the k- nearest neighbor retrieval method which improved the efficiency of the search process. The proposed model was limited to only some applications and not fully developed for many applications. The authors of [161] investigated various industrial requirements
such as scalability and adaptability of the network with the implementation using OMNeT++ network simulator. Their approach was efficient up to the first fourteen participating lines and no uncertainty was identified.

Table 12 provides the detailed relative comparison of the existing blockchain-based approaches for manufacturing using the parameters such as scalability, architecture, security, simulation/framework, smart contract, pros, and cons of the existing approaches.

### J. AGRICULTURE

In recent times, various issues related to food safety have been observed. Higher use of fertilizers and pesticides on agricultural products is the major concern in food safety. Pesticides and fertilizers residues on various agricultural products have caused world-wide concern [165]. Due to this, there is a huge demand for safe agricultural products in the market. To fulfill this demand, we need secured solutions for handling the perfect tracing and management of the production, wholesale, logistics to retail, production standards, certifications, and business reputation [166].

Hua et al. [164] proposed a blockchain-based agricultural tracking system, which was basically a decentralized system in order to solve the trust crisis in the domain of supply-chain. This blockchain-based agriculture platform recorded the information about the production, storage, transportation, processing, distribution and supply-chain of agricultural products for the third parties like government, insurance...
companies, customers, and banks. The platform recorded all the agriculture product related information on the blockchain structures, as it could involve different users such as companies, agencies, banks, or government to work together. By considering the requirements, the authors developed an agricultural traceability system for the same. This system considered the fertilizers, pesticides, companies, seeds, agricultural operations, time, and residue testing. According to the authors, it was a very tedious task to build a platform having a uniform structure, which considered all the complex information and eliminated the possibility of the redundancy in data. Hence, the authors designed two related structures especially for the basic planting information as well as for provenance records. Planting information included the source production information in terms of identity, species name, planting-time, company-name, greenhouse number, and geographical location. Provenance records include the details about the agricultural operations in terms of identity, date & time, person, digital-signature, location, operation-type, inputs & memo, and company. The agriculture tracking platform consisted of three components- data node, clients and registration center. The issues in the agriculture system such as creditability of data and integration the subsystems were easily handled by this open data-sharing platform. Due to this, any participant could view the data uploaded by any participating companies, which was also one of the major advantages of this platform.

According to Tian et al. [63], food safety is the major concern, especially in China. As China is an agricultural country, the annual demand for vegetables and fruits is approximately 730 million tons [167]. Due to the huge demand of the market, traditional agri-food logistics are not capable of handling this situation. There are some open challenges in traditional agri-food logistic systems such as deficiency of funds and modern equipment, shortfall of a monitorable traceability system, moderate level of information, and unordered regulatory systems. Therefore, there are massive and frequent breakdown events of food safety in China. To overcome the limitations of the traditional agri-food logistic systems, the authors of [63] proposed a blockchain and RFID-based agri-food supply chain traceability system. This system significantly improved the quality and safety of food, and also reduced the probability of different losses in the conventional logistics process. The building process of the system included various stages such as production link, processing link, warehouse management link, distribution of cold chain link and sales link. The authors compared and analyzed the proposed traceability system with the traditional traceability systems using various parameters. The authors also discussed the advantages of using the blockchain and RFID technology in the proposed system. As stated by the authors, the major advantage was that the traceability system totally removed the necessity of the trusted centralized agencies and provided a data sharing decentralized platform through which all the users could carry out their respective operations with openness, neutrality, transparency, security, and reliability.

Lin et al. [167] developed a blockchain-based traceability system, especially for food supply-chain. It stored the data of every node in the food supply-chain and combined all the information using blockchains. The authors proposed a conceptual framework for agri-food traceability system using Ethereum and blockchain as shown in Fig. 11. In this figure, a user can register with the help of the cryptographic keys and can get the information of the products stored on BigchainDB. As per the authors, this RFID and blockchain-based model had a few limitations such as it did not have any mechanism to ensure whether the raw data collected from sensors was correct, whether the data scanned by the RFID tags and
barcodes to scan food tracking is correct, i.e., anyone can tamper the sensor’s data and the absence of the blockchain methods to detect the same.

Table 13 provides a detailed relative comparison of the existing blockchain-based approaches for the agriculture domain. The parameters used for this comparison are transparency, reliability, security, architecture, consensus mechanism, traceability system, framework, advantages, and disadvantages of the existing approaches.

V. OPEN ISSUES AND CHALLENGES

In this section, we highlight the open issues and challenges in some application domains such as healthcare, IoT, energy, business, smart city, agriculture, energy, and supply-chain & logistics. Fig. 12 gives a detailed taxonomy of the open issues in the blockchain applications.

A. BLOCKCHAIN DESIGN AND IMPLEMENTATION CHALLENGES

The future of the blockchain can be decided by its safety, robustness, smart contract, database technology, security tokens, and changing regulatory environment. However, to achieve the goals, the design and implementation of the blockchain need to provide extreme reliability, safety, and scalability which rely on major technologies such as shared ledger, consensus, provenance, immutability, and smart contract. In this section, we outline the design and implementation issues faced by the traditional systems and the possible solutions by the blockchain technology, as shown in Fig. 13.

1) CENTRALIZATION

One of the major hurdles in the traditional system is its centralized mechanism. Such systems are larger, more complex for organizations in particular. If the centralized system is getting attacked or compromised, all the data can lead to a different direction. In this more network delay and higher computing power required, so the cost is more for the server. The central authority having all privileges in the system that clears the transactions made by the users. It can be eliminated or replaced with the decentralized system, in that verification is done by the consensus of the different users in the network.

2) SCALABILITY

Nowadays, we store all the transactions in the decentralized blockchain network to validate them. As a result of this, the blockchain becomes heavy and slow. There is a restriction on the size of each block and time interval required to create a new block. The blockchain can process only 7 to 8 transactions in one second, but in real-time scenarios, millions of transactions execute and hence it is impossible to implement a blockchain for a real-time scenario which imposes a challenge of scalability.

3) ESTABLISHING TRUST

In today’s era, how to establish the trust is the major problem for everyone because any third party creates major issues with the ongoing situation or breaches the data and increases the redundancy which makes more difficult to trust anyone. In such scenarios, the blockchain can be used to prevent hampering and establishing the trust as it uses the cryptographic hash for building the blocks and immutable nature of the ledger.

4) SECURITY

Security of important data is the major concern in every organization. The security challenges include monitoring the cloud configuration, impact of attacks, vulnerability of mobile carriers, unauthorized access, and modification of data by intruders. The blockchain technology records the transactions using blocks which are linked together with the help of the cryptographic keys and immutable ledger and
TABLE 14. Design and implementation challenges of existing system and possible solutions by blockchain.

| Aspect          | Challenges                                                                 | Implications                                                                 | Possible solutions with blockchain                                      |
|-----------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Centralization  | Fragmented systems, data storage problem                                     | Network delay, Needs high computing power                                     | Decentralized access, improved transparency, low computing power          |
| Establishing    | Manufacturer-specific safety standards                                       | Increased redundancy, Platform dependency                                     | Immutable nature of ledger to prevent tampering                           |
| Trust           |                                                                              |                                                                              |                                                                           |
| Security        | Unauthorized access, data modification                                       | Data loss; Centralized server; single point of failure; data breaches         | Decentralised database; Immutable ledger of records                        |
| Cost            | Needs middleware, intermediaries and centralized system                     | High cost and time, high fraud risk; product duplicity                        | Decentralized database; payment processing with cryptocurrency            |
| Transparency    | Company-specific policies, standards, regulations, and tracking systems      | Poor customer-business connection; less visibility                            | Distributed ledger with consensus mechanism for verified transactions    |

Table 15 provides the detailed relative comparison of the design and implementation challenges associated with the traditional systems and the possible solutions by using the blockchain technology.

thus, makes it very difficult for attackers to modify or delete information or transactions.

5) COST
Use of different agencies, intermediaries mostly includes various frauds, commission charges, and duplication of product. The blockchain eliminates the need of a third party and therefore, the transactions can be completed resulting in fewer fees [168]. Smart contracts, a component of the blockchain technology are self-executing and stored on the blockchains. Due to the decentralized nature of the system, no one can control these contracts and therefore each involved party can trust their validity. Because of the high level of automation in this technology, the companies who have adopted the blockchain technology, have experienced huge cost savings.

6) TRANSPARENCY
Different companies have their own policies, regulations, and tracking systems. This leads to a poor connection and less visibility among the customers and business. The distributed nature of the blockchain transactions make them public and verifiable by every user in the network with transparency [169].

Table 14 provides the detailed relative comparison of the design and implementation challenges associated with the traditional systems and the possible solutions by using the blockchain technology.

B. OPEN CHALLENGES IN HEALTHCARE
Table 15 provides a detailed relative comparison of the design and implementation challenges in the healthcare domain and the possible solutions using blockchains.

1) MASTER PATIENT INDICES
Every year the volume of the healthcare related data increases and often when dealing with the healthcare data, records get mismatched or duplicated. Also, different electronic health records systems have their own data format and data set to enter and execute the data, which raises a need for having a standardized data format. Due to the use of blockchain technology, the data are cryptographically hashed in the ledger. The user could look for the recorded transactions which can have multiple records or the keys, but with the use of the blockchain technology, all information is linked with single patient Ids.

2) PATIENT DATA MANAGEMENT
The Health Insurance Portability and Accountability Act is known as (HIPAA) controls the patients’ data privacy and makes the data PHI secured, but the patients need to give their medical data to the third parties such as pharmacists, imposing the need of protecting the data. With the use of the blockchain, a hash for each patient’s health information in blocks which contains the patient ids is created. Using the blockchain network API, the disease-related data can be viewed with respect to the affected patient without...
revealing the patient’s personal information. In the same manner, a patient can have the privilege to decide who can view or access his data with a specific third party [170].

3) DATA PROVENANCE AND INTEGRITY
Patients’ health information, electronic health records, data collected from IoT, and monitoring systems are maintained by the medical facilities. Here, the main target is to secure the information and its sharing techniques, authorize healthcare facilities and its entities to confirm the correct information and ensure the proper services. The blockchain is more useful in such scenarios because of its ability to provide data integrity. The approach of the blockchain is to share and distribute data publicly with the secured transactions. The technique used by this technology is PoW with time stamping.

4) CLINICAL TRIALS
Researchers working in various domains always want their confidential information to be stored privately and securely so that no unauthorized person can breach or modify or steal their data. In the blockchain technology, data modification is impossible with the SHA256 algorithm that creates the unique hash values which are linked together into a chain. The healthcare industry needs to maintain and share the information related to clinical trials securely which can only be shared with authorized parties such as research sponsors or regulatory committees. With the blockchains, the data can be managed or traced with consent within multiple sites, protocols, and systems. Patients having proper access privileges can also access this information regarding their health issues and related research.

5) DRUG TRACEABILITY
Currently, the main hurdle in pharmacology is the drug counterfeiting. By the survey of the health researchers, it has been observed that about 10 to 30 percentage of the drugs in the developing countries are duplicate. The adverse effect of this is the loss of business and improper usage of fake drugs which can lead to severe damages to a person’s health. The use of the blockchain network across the drug facilities can detect fraud from the drug dealer. All the operations from the manufacturers to the suppliers are contained in the blockchain network that enables to trace the whole route of drugs.

6) DATA ENRICHMENT
Storing unstructured data can lead to variability, time consumption in the search process, the lack of reliability. Data enrichment is an operation for adding values to increase quality. Health records must be structured, secured, accurate, time-stamped, and easy to read. Following steps are required to be executed to organize the data before adding it to the blockchain: Replacing the patient’s identity with the public hash key, making it compliance-ready, adding meta information and structuring it for computation. Organized data enables all healthcare providers to access the data efficiently.

C. OPEN CHALLENGES IN INTERNET OF THINGS
Table 16 provides the detailed relative comparison of the design and implementation challenges in the IoT and possible solutions by using blockchains.

1) ARCHITECTURE
IoT ecosystems depend upon the centralized network in which all the devices are connected in a client-server model through the brokered communication. It uses the cloud server to authenticate and identify devices. It needs higher processing time, computation power and bandwidth. The blockchain decentralized architecture creates a P2P network through which messaging, file sharing and device coordination becomes easier.

2) SENSORS’ MAINTAINING ISSUES
With the increase in the number of devices used in IoT each year, it becomes a very problematic and challenging task for the manufacturers or service providers to maintain these devices on a daily basis. Moreover, this is a time consuming and high maintenance cost task. The use of blockchain technology in this domain can reduce the cost as well as time.

3) CENTRALIZED DATABASES
A centralized database has a restricted computing power and storage capacity. There is always a large number of nodes to connect to the server which is a time-consuming task. It is also difficult to find faulty nodes in this structure. Most of the IoT devices connect with the centralized database and cloud network which increases the cost and computational requirements. In the distributed blockchain technology, nodes have minimum connectivity and still, the network remains reliable and safe. With distributed computing, the utilization of available computing power is increased for billions of transactions irrespective of the location of the devices. This makes the IoT more reliable and cost-effective.

4) DATA PRIVACY AND SECURITY ISSUES
If the users’ data are stored in a centralized database then privacy & security becomes the major concern. Nowadays, to earn profit, various companies store, use and sell user’s data to third parties without the consent of the users. Such actions compromise the privacy of users’ data. The blockchain technology uses a distributed database structure which stores data in the encrypted form and thus reduces the risk of data stealing and breach of privacy.

5) DEVICE LEGAL IDENTIFICATIN
In the current era, sensor devices used in the IoT applications are small in size and have limited computing and storage capacity. Hence, such devices are vulnerable to physical attacks such as impersonation or spoofing. The blockchain technology uses smart contracts and consensus mechanism which boost the proper identity verification of the IoT nodes.
TABLE 16. Open challenges in IoT.

| Aspect                        | Challenges                                                                 | Implications                                                                 | Possible solutions with blockchain                                                                 |
|------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Architecture                 | Brokered, centralized client-server model connected through cloud servers    | Increased time and computational requirements                                | P2P-peer messaging; Distributed file sharing; Autonomous device coordination                         |
| Sensors maintenance issues   | Maintenance issues with large number of IoT devices                         | Increased time, cost and maintenance                                          | Point-to-point, end-to-end decentralized blockchain system                                           |
| Centralized databases         | Centralized networking                                                     | Need for more storage devices and computing power                             | Distributed, point-to-point computing of transactions                                              |
| Data privacy and security     | Easy tempering of centralized database                                      | Data stealing                                                                 | Decentralized and distributed data at every node                                                   |
| Device legal identification   | High risk of counterfeiting                                                 | Difficult to sense devices due to various security measures                   | Consensus mechanism                                                                                |

and eliminates the unauthorized access of the active devices by unknown users.

D. OPEN CHALLENGES IN BUSINESS

1) DATA PRIVACY

In today’s era, data privacy is one of the key challenges in the business domain, where many systems encounter data breaches, leak of personal information, unauthorized monitoring and eavesdropping, breach of access control rights, data stealing and leaking. With the distributed blockchain technology, data are stored in an immutable manner having secured time-stamping, public audit and consensus, making the system robust against privacy issues.

2) BACKUP AND DISASTER RECOVERY

Storage and backup of data are very important in any business application. For storing and maintaining large a volume of data, more computing power is needed which results in the increase of the overall cost. Moreover, if data is maintained on a centralized system, the risk of a single point of failure also increases. The blockchain mechanism uses decentralized systems for the distributed handling of data. A clustered hierarchy is used for data storage and backup that eliminates the probability of losing the data.

3) SMART CONTRACTS

The process of contracting includes bidding, validation, and approval for enabling the next steps. Execution of a traditional contract may require human intervention which makes the involvement of a third party as a service. The same is required even during disputes and leads to take higher time for resources consumption, and the high cost of the contract. Using blockchains, smart automation is created without human intervention, which eliminates the involvement of third party transactions and unnecessary time delays.

4) LETTER OF CREDIT (LC) PAYMENT

An international letter of credit payment requires a purchaser and dealer and they use paper-based letter of credits to make transactions. In this scenario, each party needs to send the necessary documents via post or courier services. Due to requirement, time and cost involved in the process are much higher and not convenient for the exporters. If used in this domain, the blockchain technology has the potential to eliminate the time delay by providing cost-effective faster services. The blockchain makes the transactions transparent and integrated with the electronic bill of the ledger.

Table 17 provides a detailed relative comparison of the design and implementation challenges for business applications and possible solutions by using blockchains.

E. OPEN CHALLENGES IN SMART CITY

Table 18 provides a detailed relative comparison of the design and implementation challenges in the smart city domain and the possible solutions with the blockchain technology.

1) DIGITAL IDENTITY

In the current era, online services need users or clients to provide personal identification information before availing the services. All these data are stored without the knowledge of the owners and can be accessed by third parties. When the decentralized blockchain technology is used to implement online services, digital ids are created for all the users. These ids along with digital watermarking techniques are used while executing user transactions. This is how users’ data can be stored, maintained and controlled in the permissioned network having access rights only with the individual users.

2) TRANSPORTATION MANAGEMENT

The transportation business is very popular these days to provide routine services to a large number of customers. Providing necessary services to the customers is quite costly. The involvement of third parties in providing services may lead to the breach of privacy of users’ personal data as well as an increase in the cost of availing services. A decentralized blockchain network can handle all these issues effectively and efficiently by enabling a P2P platform for transportation services.

3) EDUCATION

In today’s world, education institutes either private or public, do not provide the exact records to the government. That is why the government cannot check or help for literacy targets. With the inclusion of blockchain technology, educational records can be made available via an automated consent mechanism. This solution makes the information redundant and the same can be integrated with the government population registry so that it can handle all the literacy targets in country’s population.
TABLE 17. Open challenges in business.

| Aspect       | Challenges                                                                 | Implications                      | Possible solutions with blockchain                                      |
|--------------|----------------------------------------------------------------------------|-----------------------------------|---------------------------------------------------------------------------|
| Data Privacy | Leaking of personal information, data breaches                              | Data breaches and stealing         | Immutable data storage, public audit, secure time-stamping                |
| Backup and   | Single point of failure with centralized database                           | Data loss, high resource requirements | Decentralized system, combined computing power of nodes                    |
| Disaster     | Needs human intervention, involvement of third party                        | More time and resource consumption, high cost | Smart Automation without human intervention and involvement of third party |
| Recovery     | Communication difficulties due to third party services                       | Difficulty in dealing or communicat- | Processing all transactions without involving third parties               |
| Smart contracts |                                                                                      |ing directly, increased cost        |                                                                            |
| Intermedi-   | Letter of credit (LC) payment                                                | Increases time and cost            | Integration with electronic ledger bills, transparent liquidity          |
| ary          |                                                                                      |                                   |                                                                            |

TABLE 18. Open challenges in smart city.

| Aspect                  | Challenges                                                      | Implications                        | Possible solutions with blockchain                                      |
|-------------------------|-----------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------|
| Digital Identity        | Leaking of personal identification information, high storage requirement; single point of failure due to central authority | Data modification or data breaches | No need for personal information with the use of blockchain and immutable ledger |
| Transportation Management | Need for business entity for service                              | Extra burden on customers           | Peer-to-peer transportation                                               |
| Education               | Inaccessibility of records by Government                         | Unachieved literacy targets         | Automated consent mechanism, redundant attestations, integration with population registry |
| Land use                | Tenure issues; intermediary approval problems                    | High cost and time                  | Immutable 360-degree view of assets                                      |

TABLE 19. Open challenges in Agriculture.

| Aspect           | Challenges                                                                 | Implications                        | Possible solutions with blockchain                                      |
|------------------|-----------------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------|
| Outdated record-keeping | Fragmentation and lack of standardization                                   | Difficult to gather and analyze data | A trusted shared system of record-keeping and transaction settling         |
| Traceability     | Difficult to trace and trust the origin and quality of food                  | Difficult to find original and genuine food | Sensor-based tracking of food in the blockchain system                      |
| Transparency     | All farmers cannot enter into large market                                  | Increased cost due to limited access | Connecting farmers with the market to build trust                          |

4) LAND USE

Traditional registration of land or property is a very time consuming and costly process. The blockchain technology can eliminate the hurdles associated with this conventional process by creating a digital process of automated property registration. This solution increases the transparency and trust within the system and improves the economy. The newer development of smart cities combines the blockchain based technology for a number of processes such as land and property registry, getting approvals, generating inspection reports and recording the certificates.

F. OPEN CHALLENGES IN AGRICULTURE

Table 19 provides the detailed relative comparison of the design and implementation challenges in the agriculture domain and the possible solutions using blockchains.

1) OUTDATED RECORD-KEEPING

In agriculture, all the information regarding foods, farmers, seller-buyer information are very outdated and not available to all the users. So, its very difficult to process the data and conduct market analysis. With the usage of blockchain network all the participants have the access of all record and transactions in trustworthy and secure manner.

2) TRACEABILITY / TRANSPARENCY

The second open challenge in agriculture is traceability, which focus on the origin of the foods and its quality. But, its very difficult to find original and genuine products or foods in supply chain. Blockchain based sensor tracking system is a viable possible solution to eliminate the aforementioned issue.

3) TRANSACTION COST AND MARKET ACCESS

Some times small scale farmers are not getting the whole market access in agriculture. Thus, the farmers compromised with higher cost with limited access to the market. With the help of distributed ledger technology of blockchain network, all the data are available and easily access to the every market on the network, which helps the all the farmers to connects with market and also to built trust.

G. OPEN CHALLENGES IN ENERGY

Table 20 provides the detailed relative comparison of the design and implementation challenges in the energy domain and the possible solutions based on the blockchains.

1) ENERGY AND ENVIRONMENT

In today’s scenario, we don’t have a smart grid like infrastructure, and the use of the normal infrastructures makes the third party intermediary problems such as VAT frauds, security issues, high cost, and carbon emission which can lead the environment to a very worse condition. With the use of blockchain technology, the development of the smart grid energy infrastructure is possible through which each customer can get emission allowance criteria for the safety of the environment. All kind of tracking and monitoring of
energy makes it easier to build and sustain a healthy and green environment on the earth.

2) INEQUALITY
In the current scenario, retailers don’t have the grid infrastructure to monitor the electric meters and put extra burden on the customers to cover the cost of the middlemen and earn high profits. The blockchain technology helps to eliminate the middlemen energy retailers so that the consumers can trade the energy and also buy it, directly from the smart grid. It has been observed that the consumers can reduce the energy bill by 38%.

3) PEER-TO-PEER TRADING
Energy trading has involved intermediaries or brokers so far. They charge their fees for every trading process and act as a link between energy generators and consumers. Energy trading takes place at the power exchanges and over the counters. The blockchain P2P network created in the smart grid infrastructure helps directly exchange the energy to one another without involving brokers and paying them unnecessary costs. The overall process becomes cost-effective and easy for customers.

4) ENERGY METERS
Currently, the use on energy meters creates dependency on middlemen monitoring. It also increases the amount of billing and makes the overall process tedious. Smart meters can be used for quick implementation of the process and monitor the correct energy usage. This eliminates the dependency of meter monitoring by middlemen at a great extent. The users can avail the required load and power with the use of blockchain-based microgrids energy.

H. OPEN CHALLENGES IN SUPPLY-CHAIN & LOGISTICS
1) COUNTERFEITING
In today’s world, every industry has issues of counterfeiting of products and drugs. This creates issues like poor customer satisfaction with quality, unverifiable products or fake products. All these make the overall trust and reputation of companies or manufactures to go down. The blockchain technology lessens the distance between customers and companies and makes the processes more transparent. It stores tamper proof tracking history of the products which makes it difficult to counterfeit the products.

2) AUTHENTICITY
In today’s world, users rely on the documents to check products’ or services’ validity and originality. But such documents can easily be tempered. The blockchain technology provides a secure way to maintain the information about the supply chain to avoid any kind of modification or breaching of data. This technology enables the clients and suppliers to trace the origin as well as movements of the products. With the use of RFID tags attached to the vehicles, it becomes possible to trace the products along with timestamps.

3) PROVENANCE TRACKING
Every industry and company has dependencies on the supply chains. It is very difficult to track every record in transit even in multinational companies. The need for transparency leads to the increased cost and clients’ relational issues which can weaken the brand or company value. A blockchain-based supply chain can maintain all the necessary records and their tracking details easily with the help of the embedded sensors. This kind of precise tracking can help to identify any fraud that occurs anywhere in the supply-chain.

4) INEFFICIENCY
Although contemporary supply-chains can handle the complexities of manufacturing processes, they are still extremely slow, expensive, and inefficient. When each supplier and manufacturer have their own infrastructure, tracking products in real time is difficult in a fragmented system. Product delivery delays are usually caused by the lack of access to up-to-date data. This can be mitigated using the blockchain technology, which increases the supply-chain efficiency while speeding up the time to market. Table 21 provides the detailed relative comparison of the design and implementation challenges in the supply chain and logistics and the possible solutions based on the blockchain.

VI. CASE STUDIES
In order to demonstrate the use of blockchains, we have tried to implement the blockchain technology for two different applications: smart farming and tourism & hospitality. The blockchain is one of the greatest inventions of this decade and it has taken the whole world by a storm. Nowadays, the blockchain has become a popular technol-
ogy due to its properties such as decentralization, improved security, replication, irreversibility, time-stamping and cryptography. In this paper, we have discussed the use of the blockchain technology for a variety of applications such as smart farming, smart healthcare, supply chain & logistics, energy sector, IoT, smart city, business, manufacturing, agriculture, and tourism & hospitality. We have also discussed various open issues and challenges associated with different applications.

### A. SMART FARMING

In this case study, we provide insights into the current issues associated with smart farming and how they can be resolved by implementing the blockchain mechanism. Here, we present blockchain-based smart farming and mentioned role & functionality of different users in smart farming.

In smart farming, various issues related to food safety, food integrity, transaction cost, and food traceability need to be considered. Extensive use of fertilizers and pesticides on agricultural products is the major concern in food safety. Pesticides and fertilizers residues on various agricultural products have drawn the attention of many countries. [165]. This has leveraged the demand for safe agricultural products in the market. To handle this demand, we need a perfect tracing and management system for ensuring food safety during each process of production and supply [166].

All these issues in smart farming can be handled with the help of the proposed architecture shown in Fig. 14. This architecture, different stakeholders such as farmers, crop insurance agencies, feed manufacturers, food producers, food manufacturers, retailers, and consumers are considered. Farmers have various functionalities such as farm management through the analysis of soil/crop health, crop-livestock management through agricultural robots, financial services management based on the entities like transaction costs, the safety of crops by sensors and insurance agencies. Feed manufacturers take the raw data from the oil-seed-crusher and mineral suppliers. They provide inputs to the food processor, through which the food is manufactured, and then sent to the customer across the chain of the food distributors & retailers. To maintain the food safety, transparency & food traceability and minimum transaction cost, our proposed blockchain-based architecture uses a distributed network which establishes and maintains all the transactions in a secured manner.

### B. TOURISM & HOSPITALITY

In this case study, we highlight the current issues in the tourism industry and show how they can be resolved by implementing the blockchain mechanism. We present a case study that follows the process model shown in Fig. 15. Recently, many tourism companies like Expedia Group, BCD Travel, Uber, Ola, and AirBnb have replaced their conventional business models by C2C models to achieve transparency and security in transactions. There is a huge demand for innovative platforms in the tourism industry to integrate technology, money, and knowledge. There are many companies like TUI which has already started using blockchains for ticket booking transactions. Many companies like Expedia, CheapAir, Webjet, and One Shot Hotels have started using bitcoins for their transactions. Digital currencies simply integrate with the smart contracts which have enough potential to develop highly disruptive technologies for the
tourism industry. Generally, customers take the help of online reviews of different tourism products to make a decision. They think that all the reviews of real travelers are honest and true, but actually, most of the tourism & hospitality industry players, (i.e. Hotels, Travel agencies, or restaurants) use centralized platforms to store and maintain these reviews. Through such centralized storage platforms, user reviews can be manipulated and modified very easily by different agencies for their own profit.

There is a frequent involvement in the exchange of money in the tourism industry across the country to another party where they do not have any past business relationship. For such exchanges, customers generally take the help of the trusted third parties. Every time, a trusted third party tries to maintain a secured exchange of money. For providing this service, the trusted third party takes a commission. The need of involving third parties in the transactions can be avoided by the inclusion of cryptocurrencies in the blockchain technology for the exchange of money. We can create a new platform for C2C transactions in markets for tourism products. So, in our case study, we have suggested the use of a blockchain-based decentralized online customer review system to resolve the above issues. All the current issues in the tourism industry could be resolved with the help of our proposed architecture. In this architecture, users, travel agencies and hotels are the different categories of tourism industry users. Here, we use the blockchain decentralized network and cryptocurrencies through which the users can book tickets. Thus, the trusted third parties and commission charges by them can be avoided. All the transactions are maintained through blocks with unique identities which eliminates the creation of duplicate or fake online reviews.

**VII. CONCLUSION**

In this paper, we provide insights to the readers about the importance of the blockchain technology for various smart applications, where security remains paramount. This survey is divided into five parts. The first part discusses the traditional security systems, background, and history of the blockchains. The second part describes the basic architecture of the blockchain technology, including the verification of each transaction in the distributed network which makes a permanent, verified and unalterable nature of ledger for the information or data. Moreover, the blockchain reference architecture which consists of three different networks such as public network, cloud network and enterprise network. The Third part of our paper focuses on the real-time deployment of the blockchain for various applications such as smart healthcare, smart farming, supply-chain & logistics, business, tourism& hospitality, energy, agriculture, digital content distribution, smart city, IoT, and manufacturing which are also considered in the survey part of the paper. The fourth part emphasizes on the open issues and challenges in Industry 4.0-based smart applications and suggests some blockchain based solutions for those applications. Finally, to demonstrate the suitability of the blockchain technology for smart applications, the last part of our paper illustrates case studies on two application domains: smart farming, and tourism & hospitality. We plan to explore the feasibility of developing a blockchain-based infrastructure for precision agriculture in future.

**REFERENCES**

[1] G. Gambhire, T. Gujar, and S. Pathak, “Business potential and impact of industry 4.0 in manufacturing organizations,” in Proc. 4th Int. Conf. Comput. Commun. Control Autom. (ICCUBA), Aug. 2018, pp. 1–6.
[2] International Tourist Arrivals Reach 1.4 Billion Two Years Ahead of Forecasts. Accessed: Apr. 7, 2019. [Online]. Available: https://www.visit.org/sites/louisianas/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/#2faabe643ecc
[3] International Tourist Arrivals Reach 1.4 Billion Two Years Ahead of Forecasts. Accessed: Apr. 7, 2019. [Online]. Available: https://www.forbes.com/sites/louisianas/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/#2faabe643ecc
[4] P. Fraga-Lamas and T. M. Fernandez-Carames, “A review on blockchain technologies for an advanced and cyber-resilient automotive industry,” IEEE Access, vol. 7, pp. 17578–17598, 2019.
[5] International Tourist Arrivals Reach 1 Billion Two Years Ahead of Forecasts. Accessed: Apr. 7, 2019. [Online]. Available: https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/
[6] International Tourist Arrivals Reach 1 Billion Two Years Ahead of Forecasts. Accessed: Apr. 7, 2019. [Online]. Available: https://www.businesswire.com/news/home/2018080800533/en/Jan-Jun-Research-Cybersecurity-Breaches-Result-146-Billion
[7] I. Mahkdoom, M. Aboholas, H. Abbas, and W. Ni, “Blockchain’s adoption in IoT: The challenges, and a way forward,” J. Netw. Comput. Appl., vol. 125, pp. 251–279, Jan. 2019.
[8] U. Bodkhe, J. Chaklasiya, P. Shah, S. Tanwar, and M. Vora, “Markov model for password attack prevention,” in Proc. 1st Int. Conf. Comput., Cyber-Secure (IC4S), P. Singh et al., Eds. Chandigarh, India: Springer, 2020, pp. 831–843.
[9] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Tech. Bitcoin.Org., 2008.
[10] P. Noizat, “Blockchain electronic vote,” in Handbook of Digital Currency, D. L. K. Chuen et al., Eds. San Diego, CA, USA: Academic, 2015, ch. 22, pp. 453–461.
[11] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, “A survey on privacy protection in blockchain system,” J. Netw. Comput. Appl., vol. 126, pp. 45–58, Jan. 2019.
[12] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueuta, H. Chen, and B. M. Boshikoska, “Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions,” Comput. Ind., vol. 109, pp. 83–99, Aug. 2019.
[13] V. J. Morkunass, J. Paschen, and E. Boon, “How blockchain technologies impact your business model,” Bus. Horizons, vol. 62, no. 3, pp. 295–306, May 2019.
[14] Y. Lu, “The blockchain: State-of-the-art and research challenges,” J. Ind. Inf. Integr., vol. 15, pp. 80–90, Sep. 2019.
[15] H. F. Attam and G. B. Will, “Technical aspects of blockchain and IoT,” Adv. Comput., vol. 115, pp. 1–39, Mar. 2019, doi: 10.1016/bসd.2018.10.006.
[16] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, “Survey on blockchain for Internet of Things,” Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.
[17] M. Muramal, Q. Qu, and B. Nasrul, “Renovating blockchain with distributed databases: An open source system,” Future Gener. Comput. Syst., vol. 90, pp. 105–117, Jan. 2019.
[18] D. Mingxiaio, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A survey on consensus algorithm of blockchain,” in Proc. IEEE Int. Conf. Syst. Man, Cybern. (SMC), Oct. 2019, pp. 2567–2572.
[19] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. C. Hong, “A survey on decentralized consensus mechanisms for cyber physical systems,” IEEE Access, vol. 8, pp. 54371–54401, 2020.
[20] S. Hirsh, S. Alman, V. Lemieux, and E. T. Meyer, “Blockchain: One physical systems,” Future Gener. Comput. Syst., vol. 125, pp. 251–279, Jan. 2019.
[21] M. H. Onik, M. H. Miraz, and C.-S. Kim, “A recruitment and human resource management technique using blockchain technology for industry 4.0,” in Proc. Smart Cities Symp., Apr. 2018, pp. 1–6.
[22] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Sep. 2016, pp. 1–3.

[23] M. W. L. Moreira, J. J. P. C. Rodrigues, V. Korotaeva, J. Al-Muhtadi, and N. Kumar, “A comprehensive review on smart decision support systems for health care,” IEEE Syst. J., vol. 13, no. 3, pp. 3536–3545, Sep. 2019.

[24] M. M. H. Onik, S. Aich, J. Yang, C.-S. Kim, and H.-C. Kim, “Blockchain in healthcare: Challenges and solutions,” in Big Data Analytics for Intelligent Healthcare Management, N. Dey, H. Das, B. Naik, and H. S. Behera, Eds. New York, NY, USA: Academic, 2019, pp. 197–226.

[25] J. Yi-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is current research on blockchain technology?—A systematic review,” PLoS ONE, vol. 11, no. 10, 2016, Art. no. e0163477.

[26] T. Abram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” in Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON), Jun. 2017, pp. 137–141.

[27] S. Kim and J. Kim, “POSTER: Mining with proof-of-profitability in blockchain,” in Proc. Asia Conf. Comput. Commun. Secur. (ASIACCS), New York, NY, USA, 2018, pp. 841–843.

[28] M. Weiss, A. Botha, M. Herselman, and G. Loots, “Blockchain as an enabler for public mHealth solutions in South Africa,” in Proc. Int. Afri. Week Conf. (Afri-Africa), May 2017, pp. 1–8.

[29] T. Abram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” in Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON), Jun. 2017, pp. 137–141.

[30] P. Zhang, M. A. Walker, J. White, and G. Lenz, “Metrics for assessing blockchain-based healthcare decentralized apps,” in Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Oct. 2017, pp. 1–4.

[31] W. Liu, S. S. Zhu, T. Mundie, and U. Krieger, “Advanced block-chain architecture for e-health systems,” in Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Oct. 2017, pp. 1–6.

[32] Y. Yu, R. Liang, and J. Xu, “A scalable and extensible blockchain architecture,” in Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW), Nov. 2018, pp. 161–163.

[33] B. Duan, Y. Zhong, and D. Liu, “Education application of blockchain technology: Learning outcome and meta-diploma,” in Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS), Dec. 2017, pp. 814–817.

[34] I. Radanovic and R. Ljicic, “Opportunities for use of blockchain technology in medicine,” Appl. Health Econ. Health Policy, vol. 16, no. 5, pp. 583–590, Oct. 2018.

[35] D. Vujicic, D. Jagodic, and S. Randic, “Blockchain technology, bitcoin, and etherium: A brief overview,” in Proc. 17th Int. Symp. Infotech-Jahorina (INFOTEH), Mar. 2018, pp. 1–6.

[36] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, “Blind signatures based secured E-Healthcare system,” in Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS), Jul. 2018, pp. 1–5.

[37] Y. Zhao, K. Peng, B. Xu, Y. Liu, W. Xiong, and Y. Han, “Applied engineering programs of energy blockchain in US,” Energy Procedia, vol. 158, pp. 2787–2793, Feb. 2019.

[38] J. Hinckeldeyn and K. Jochen, “Short paper: Developing a smart storage container for a blockchain-based supply chain application,” in Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT), Jun. 2018, pp. 97–100.

[39] U. Bodkhe and S. Tanwar, “Secure data dissemination techniques for IoT applications: Research challenges and opportunities,” Softw. Pract. Exper., pp. 1–23, Feb. 2020, doi: 10.1002/spe.2811.

[40] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, “Blind signatures based secured E-Healthcare system,” in Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS), Beijing, China, Aug. 2019, pp. 1–5.

[41] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, and M. S. Obaidat, “Bloom: Blockchain enabled smart tourism and hospitality management,” in Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS), Beijing, China, Aug. 2019, pp. 1–5.

[42] M. M. Queiroz and S. F. Wamba, “Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA,” Int. J. Inf. Manage., vol. 46, pp. 70–82, Jun. 2019.

[43] F. Tian, “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things,” in Proc. Int. Conf. Service Syst. Service Manage., Jun. 2017, pp. 1–6.

[44] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, “Blockchain-based traceability in agri-food supply chain management: A practical implementation,” in Proc. Vertical Topic Summit ‘Tuscany-Agritourism’ (IOT Tuscany), May 2018, pp. 1–4.

[45] G. Perboli, S. Musso, and M. Rosano, “Blockchain in logistics and supply chain: A lean approach for designing real-world use cases,” IEEE Access, vol. 6, pp. 62018–62028, 2018.

[46] F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” in Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM), Jun. 2016, pp. 1–6.

[47] D. Tso, B. Zhang, Y. Yang, C. Cheng, and H. Mu, “Blockchain application in food supply information security,” in Proc. IEEE Int. Conf. Ind. Eng. Manage. (IEEM), Dec. 2017, pp. 1357–1361.

[48] N. Kshetri, “I Blockchain’s roles in meeting key supply chain management objectives,” Int. J. Inf. Manage., vol. 39, pp. 80–89, Apr. 2018.

[49] K. Kuhi, K. Kaare, and O. Koppel, “Ensuring performance measurement integrity in logistics using blockchain,” in Proc. IEEE Int. Conf. Serv. Oper. Logistics, Informat. (SOLI), Jul. 2018, pp. 256–261.

[50] H. Min, “Blockchain technology for enhancing supply chain resilience,” Bus. Horizons, vol. 62, no. 1, pp. 35–45, Jan. 2019.
K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. van Nieuwenhuyse, “Research on agricultural supply chain system with double chain architecture based on blockchain technology,” Future Gener. Comput. Syst., vol. 86, pp. 641–649, Sep. 2018.

I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, “Untrusted business process monitoring and execution using blockchain,” in Proc. Int. Conf. Bus. Process Manage., 2016, pp. 329–347.

S. Krishnamurty, “Blockchain for business,” Wilmott, vol. 2018, no. 96, pp. 18–19, 2018.

S. Guerreiro, S. H. J. van Kervel, and E. Babkin, “Towards devising on blockchain for multiple stakeholders in the food supply chain,” Int. J. Environ. Res. Public Health, vol. 15, no. 8, p. 1627, 2018.

S. Singh and N. Singh, “Blockchain: Future of financial and cyber security,” in Proc. 2nd Int. Conf. Contemp. Comput. Informat. (ICSCI), Dec. 2016, pp. 463–467.

F. Imbuuli, M. Siatwe, R. de Beaufort, and R. Plana, “The green blockchain: Managing decentralized energy production and consumption,” in Proc. IEEE Int. Conf. Environ. Electr. IEEE Ind. Commer. Power Syst. Eur. (EEEIC/ICPS Europe), Jun. 2017, pp. 1–5.

S. Noor, W. Yang, M. Guo, K. H. Van Dam, and X. Wang, “Energy demand side management within micro-grid networks enhanced by blockchain,” Appl. Energy, vol. 228, pp. 1385–1396, Oct. 2018.

J. Truby, “Decentralizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies,” Energy Res. Soc. Sci., vol. 44, pp. 399–410, Oct. 2018.

N. M. Kumar, “Blockchain: Enabling wide range of services in distributed energy system,” Beni-Suef Univ. J. Basic Appl. Sci., vol. 7, no. 4, pp. 701–704, Dec. 2018.

G. DeCusatis and K. Lotay, “Secure, decentralized energy resource management using the ethereum blockchain,” in Proc. 17th IEEE Int. Conf. Trust. Secure. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Syst. (TBSP), Aug. 2018, pp. 1907–1913.

E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, “A blockchain-based energy trading platform for smart homes in a microgrid,” in Proc. 3rd Int. Conf. Comput. Commun. Syst. (ICCCS), Apr. 2018, pp. 472–476.

M. Hinterstocker, C. Dufter, S. von Roon, A. Bogensperger, and A. Zeiselmaier, “Potential impact of blockchain solutions on energy markets,” in Proc. 15th Int. Conf. Eur. Energy Market (EEM), Jun. 2018, pp. 1–5.

M. J. Ashley and M. S. Johnson, “Establishing a secure, transparent, and autonomous blockchain of custody for renewable energy credits and carbon credits,” IEEE Eng. Manag. Rev., vol. 46, no. 4, pp. 100–102, Dec. 2018.

C. Plaza, J. Gil, F. de Chezelles, and K. A. Strang, “Distributed solar self-consumption and blockchain solar energy exchanges on the public grid within an energy community,” in Proc. IEEE Int. Conf. Environ. Electr. IEEE Ind. Commercial Power Syst. Eur. (EEEIC/ICPS Europe), Jun. 2018, pp. 1–4.

Y. Wang, Z. Su, Q. Xu, and N. Zhang, “Contract based energy blockchain for secure electric vehicles charging in smart community,” in Proc. IEEE 16th Intl Conf Dependable, Autonomic Secure Comput., 16th Int. Conf Pervasive Intell. Comput., 4th Int. Conf Big Data Intell. Comput. Cyber Sci. Technol. Cong. (DASC/PICom/DataCom/CyberSciTech), Aug. 2018, pp. 323–327.

N. Mohamed, J. Al-Jaroodi, and S. Lazaroa-Molar, “Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories,” IEEE Access, vol. 7, pp. 18008–18020, 2019.

A. Goranovic, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, “Blockchain applications in microgrids an overview of current projects and concepts,” in Proc. IECEN–33rd Annul. Conf. IEEE Ind. Electron. Soc., Oct. 2017, pp. 6153–6158.

A. Meeuw, S. Schopfer, and F. Wortmann, “Experimental bandwidth benchmarking for P2P markets in blockchain managed microgrids,” Energy Procedia, vol. 159, pp. 370–375, Feb. 2019.

N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu, X. Du, and M. Guizani, “When energy trading meets blockchain in electrical power system: The state of the art,” Appl. Sci., vol. 9, no. 8, p. 1561, 2019.

M. Roop, T. Schenkelberg, and D. Sümmermann, “Faqs-easily charge your electric car with reliable charging station providers,” EVBox, Amsterdam, The Netherlands, Tech. Rep., 2017.
Q. K. Nguyen, “Blockchain—A financial technology for future sustainable development,” in Proc. 3rd Int. Conf. Green Technol. Sustain. Develop. (GTSD), Nov. 2016, pp. 51–54.
UMESH BODKHE is currently pursuing the Ph.D. degree with Nirma University, Ahmedabad, India. He is also working as an Assistant Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University. His current research interests include network security and blockchain technology. He is a Life-time Member of ISTE.

SUDEEP TANWAR (Member, IEEE) received the B.Tech. degree from Kurukshetra University, India, in 2002, the M.Tech. degree (Hons.) from Guru Gobind Singh Indraprastha University, Delhi, India, in 2009, and the Ph.D. degree with specialization in wireless sensor network, in 2016. He is currently an Associate Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India. He is also a Visiting Professor with Jan Wyzkowski University, Polkowice, Poland, and the University of Pitești, Pitești, Romania. He has authored or coauthored more than 130 technical research articles published in leading journals and conferences from the IEEE, Elsevier, Springer, and Wiley. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING (TNSE), the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (TVT), the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, Computer Communications, Applied Soft Computing, the Journal of Network and Computer Application, Pervasive and Mobile Computing, the International Journal of Communication Systems, Telecommunication Systems, Computers and Electrical Engineering, and the IEEE SYSTEMS JOURNAL. He has also published six edited/authored books with International/National Publishers, such as IET and Springer. His current interests include wireless sensor networks, fog computing, smart grid, the IoT, and blockchain technology. He has guided many students leading to M.E./M.Tech., and guiding students leading to Ph.D. He was invited as a Guest Editor/Editorial Board Member of many international journals, invited for keynote Speaker in many international conferences held in Asia and invited as the Program Chair, the Publications Chair, the Publicity Chair, and the Session Chair in many international conferences held in North America, Europe, Asia, and Africa. He has been awarded best research paper awards from the IEEE GLOBECOM 2018, the IEEE ICC 2019, and Springer ICRIC-2019. He is an Associate Editor of IICS, Wiley and Security and Privacy Journal, Wiley.

KARAN PAREKH is currently pursuing the master’s degree with Nirma University, Ahmedabad, India. His research interests include blockchain technology, big data analytics, and computer security.

PIMAL KHANPARA received the B.E. degree in Information technology from Dharmsinh Desai University, Nadiad, the M.Tech. degree in computer science and engineering from Nirma University, and the Ph.D. degree in survivable mobile ad hoc networks from Gujarat Technological University, in 2018. She has been an Assistant Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, since 2012. Her research interests are wireless network communication, network security, and computer architecture. She has been actively contributing to the domain of ad hoc networks through research articles and projects.
SUDHANSHU TYAGI (Senior Member, IEEE) received the Ph.D. degree from Mewar University, Chittorgarh, Rajasthan, India, in 2016. He is currently working as an Assistant Professor with the Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Deemed University, Patiala, India. He has published 40 research articles in peer-reviewed international journal and conferences. His research area includes lifetime enhancement of homogeneous and/or heterogeneous WSNs. He is a member of IAENG.

NEERAJ KUMAR (Senior Member, IEEE) received the Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra (J&K), India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is currently a Visiting Professor with Coventry University, Coventry, U.K. He has published more than 300 technical research articles in leading journals and conferences from the IEEE, Elsevier, Springer, and John Wiley. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS (TIE), the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (TDSC), the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS (ITITS), the IEEE TRANSACTIONS ON CLOUD COMPUTING (TCC), the IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING (TKDE), the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (TVT), the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS (TCE), the IEEE NETWORK, the IEEE COMMUNICATIONS, the IEEE WIRELESS COMMUNICATIONS (WC), the IEEE INTERNET OF THINGS JOURNAL (IoTJ), the IEEE SYSTEMS JOURNAL (SJ), FGCS, JNCA, and ComCom. He has guided many Ph.D. and M.E./M.Tech. His research is supported by fundings from Tata Consultancy Service, Council of Scientific and Industrial Research (CSIR), and Department of Science and Technology. He has awarded best research paper awards from the IEEE ICC 2018 and the IEEE SYSTEMS JOURNAL 2018. He is also leading the research group Sustainable Practices for the Internet of Energy and Security (SPINES), where group members are working on the latest cutting edge technologies. He is a TPC Member and a Reviewer of many international conferences across the globe.

MAMOUN ALAZAB (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University of Australia. He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Australia. He is also a Cyber Security Researcher and a Practitioner with industry and academic experience. His research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention. He has more than 150 research articles in many international journals and conferences, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, the IEEE TRANSACTIONS ON BIG DATA, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, Computers & Security, and Future Generation Computing Systems. He delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police (AFP), Westpac, and the Attorney Generals Department. He is the Founding Chair of the IEEE Northern Territory (NT) Subsection.