IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 6, 2019, accepted November 19, 2019, date of publication November 29, 2019,
date of current version December 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2956748

Blockchain Applications for Industry 4.0 and Industrial IoT: A Review

TEJASVI ALLADI[1], VINAY CHAMOLA[1], REZA M. PARIZI[2], (Senior Member, IEEE), AND KIM-KWANG RAYMOND CHOO[3], (Senior Member, IEEE)

[1]Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani 333031, India
[2]College of Computing and Software Engineering, Kennesaw State University, Marietta, GA 30060, USA
[3]Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, USA

Corresponding author: Kim-Kwang Raymond Choo (raymond.choo@fulbrightmail.org)

This work was supported in part by the National Science Foundation under Award Number 1925723.

ABSTRACT The potential of blockchain has been extensively discussed in the literature and media mainly in finance and payment industry. One relatively recent trend is at the enterprise-level, where blockchain serves as the infrastructure for internet security and immutability. Emerging application domains include Industry 4.0 and Industrial Internet of Things (IIoT). Therefore, in this paper, we comprehensively review existing blockchain applications in Industry 4.0 and IIoT settings. Specifically, we present the current research trends in each of the related industrial sectors, as well as successful commercial implementations of blockchain in these relevant sectors. We also discuss industry-specific challenges for the implementation of blockchain in each sector. Further, we present currently open issues in the adoption of the blockchain technology in Industry 4.0 and discuss newer application areas. We hope that our findings pave the way for empowering and facilitating research in this domain, and assist decision-makers in their blockchain adoption and investment in Industry 4.0 and IIoT space.

INDEX TERMS Internet of Things, industry 4.0, industrial IoT, blockchain, smart contracts.

I. INTRODUCTION

Bitcoin and Etherum (a popular smart contract supported platform) are, perhaps, the two most widely recognized implementations of blockchain. The latter is a cryptographically linked and continuously growing list of immutable data records. Within the blockchain, a (public) ledger is used for recording the data, as well as the information of each transaction. Information about each completed transaction is stored in a distributed ledger, shared across all the participating nodes of the blockchain network. As discussed in the literature, blockchain is capable of efficiently recording transactions between two or more involved parties on a distributed peer to peer (P2P) network, with the stored data co-owned by all members of the network, and permanently unmodifiable [1]. In other words, blockchain provides an immutable, trusted and secure platform for multiple entities (both individuals and organizations) to exchange data/assets, collaborate and perform transactions.

Since there is no central controlling authority in the blockchain architecture, before a block can be accepted for inclusion into the ledger, the participating nodes have to reach a consensus by running a predefined consensus algorithm used in the blockchain's protocol. Commonly used consensus algorithms are Proof-of-Work (PoW) [11], Proof-of-Stake (PoS) [12], Delegated Proof-of-Stake (DPoS) [13], and Practical-Byzantine-Fault-Tolerance (PBFT) [14]. Other algorithms are used by some of the works reviewed in this article, such as Proof-of-Authority/ Proof-of-Authenticity (PoA), Proof-of-Concept (PoC), Proof-of-Existence (PoE), Proof-of-Object (PoO), Proof-of-Graph (PoG), and Proof-of-Data (PoD).

Although a key application of blockchain is to store financial data with a secure exchange, there have been attempts to explore and extend the applications of blockchain beyond payments and to other domains and settings such as healthcare, supply chain, manufacturing, and education [15]. Broadly speaking, Blockchain 1.0 is generally associated with cryptocurrency and payment (e.g. Bitcoin), and Blockchain 2.0 is associated with automated digital finance using smart contracts [16], [17]. The more recent Blockchain 3.0 trend is focused on addressing the needs of the digital society, such as smart cities and Industry 4.0 [18]. Industry 4.0, the fourth industrial revolution, is largely fueled

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Yu.

TABLE 1. Related literature reviews / surveys on blockchain for Internet of Things (IoT).

Year	Authors	Focus
2016	Christidis et al. [2]	Blockchains and smart contracts for IoT
2018	Fernández-Caramés et al. [3]	Challenges and recommendations for developing blockchain-based IoT applications
2018	Ferrag et al. [4]	Blockchain based security and privacy solutions for IoT
2018	Salman et al. [5]	Blockchain solutions to achieve distributed network security
2018	Shen et al. [6]	Review of blockchain use cases for cities
2019	Fraga et al. [7]	Review of blockchain in automotive industry
2019	Lu et al. [8]	Review of blockchain in oil and gas industry
2019	Yang et al. [9]	Integration of blockchain and edge computing technologies
2019	Xie et al. [10]	Blockchain applicability to smart cities

by the Internet of Things (IoT) and other related technologies. The German government is, perhaps, one of the first to define Industry 4.0 in 2011 [19], which is now widely accepted by both industry and academia. Industrial IoT (IIoT) is a similar concept but has a more specific/narrow focus (and one can think of IIoT as a subset of IoT), and Industry 4.0 is generally associated with a smart factory setup. The transition from traditional industry to smart industry or Industrial IoT is, in part, facilitated by the interconnectivity and digitalization of our society and the prevalence of IoT devices.

The interest of blockchain in Industry 4.0 applications, such as those involving IIoT, is evident [20]. For example, there have been attempts to utilize blockchain in IIoT security [21]–[23] and in facilitating data collection and storage techniques [24]–[26]. We also observed a number of published surveys and reviews on blockchain applications in IoT, smart cities and industry. For example, the authors of [3], [4], [27], [28] reviewed the applications of blockchain for IoT, and discussed the benefits and limitations of using blockchain in such applications. A small number of surveys and reviews focused on the application of blockchain in specific industries [6]–[8], [10], [29]–[33], or applications relating to edge computing [9] and distributed network security services [5], and so on.

In Table 1, we summarize a number of existing literature reviews and surveys. We also observe that there is no existing review or survey that focuses on the use of blockchain in Industry 4.0 and IIoT applications. Hence, this motivates this research. Specifically, we will survey the extant literature and discuss the various benefits and challenges associated with the adoption of blockchain in Industry 4.0 and IIoT.

The organization of the rest of this paper is as follows. Section II gives a brief overview of Industry 4.0 and IIoT. In Sections III to VIII, we present the current research trends in each of the related industrial sectors, as well as successful commercial implementations of blockchain in these relevant sectors. Along with these, industry-specific challenges are also discussed. Section IX summarizes the reviewed literature. In Section X, we discuss open challenges in the adoption of blockchain in Industry 4.0 and IIoT. We also discuss newer application areas with limited research in blockchain. And finally, Section XI gives the concluding remarks.

II. BACKGROUND MATERIALS

A. INDUSTRY 4.0

In 2011, at the Hanover event, Germany introduced Industry 4.0 or ''Industrie 4.0'' for 2020 [34]. Initiatives under Industry 4.0 would lead to distributed, highly automated and dynamic production networks with ten key technological enablers driving them. These enablers are the Internet, IIoT, blockchain, big data, edge and cloud computing, robotics, human-machine interaction, artificial intelligence, and open source software. The automation of the industrial systems is going to be achieved through interconnected cyber-physical systems (CPS) in Industry 4.0; thus, allowing the industrial infrastructure and production processes to transform into an autonomous and dynamic system [35]. The entities in this highly integrated network must communicate and behave as smart devices to autonomously work with each other and to achieve the common goal [36]. Information and communication technologies (ICT) are anticipated to play key roles in sustainable industrialization to support global economic, social, and environmental sustainability [37].

According to [38], Industry 4.0 has three central paradigms. The first paradigm is the smart product that takes control of the resources and orchestrates the manufacturing process to its end. The second paradigm is the smart machine that is a cyber-physical system, where conventional manufacturing processes transition into distributed, adaptable, flexible, and self-organizing production lines. The third paradigm is the augmented operator, which adds flexibility and capability of a human operator in the industrial system. Technologies will then be leveraged to support the human operator, acknowledging its centrality when faced with a variety of jobs like specification, monitoring, and verification of the production processes. It aims at augmenting workers' capability and providing a cooperative work environment, reshaping their role in production cycles through human-machine interfaces enabling collaboration among the entire manufacturing ecosystem.

The Internet is the most critical technology of Industry 4.0 as a majority of the other technology drivers of Industry 4.0 are dependent on it. For example, the real-time sharing of information between various entities through a digital communication network or leveraging computing power and data storage capability of warehouse-scale computers remotely is enabled through the Internet. Smartness in a system is achieved through the integration of objects, products, and operators and providing context awareness via the Internet.

B. IIoT

IIoT, a typical cyber-physical system, is defined as ''machines, computers, and people enabling intelligent industrial operations, using advanced data analytics for transformational business outcomes'' [39]. IIoT enables the integration of wireless sensor networks, communication protocols and internet infrastructure with the processes enabling intelligent industrial operations for monitoring, analysis and management [40]. This inter-network of anything in the production system context helps in automation of industrial production and improves intelligence, efficiency, and safety.

The physical layer, communication layer, and application layer form the three layers of the IIoT architecture. The physical layer consists of physical devices like sensors, actuators, manufacturing equipment, smart terminals and data centers. The communication layer uses network technologies, such as actuator and wireless sensor networks (WSNs), 5G, and machine-to-machine (M2M) communication, for the integration of various devices in the physical layer for industrial manufacturing and automation. The above layers form a CPS (Industrial-CPS in the context of IIoT) to support the industrial and production application layer using the above technologies for the development of smart factories, smart supply chains, etc. The control, networking and computing infrastructures of the cyber systems enable the networking and intelligent operation of the production systems.

III. HEALTHCARE INDUSTRY

In the healthcare sector, critical patient data can be shared in an effective manner using blockchain, which can potentially enhance the delivery of healthcare services, for example by reducing the potential for mismatched patients and reducing errors in patient care [41]. Interoperability is also shown to be enhanced using blockchain [42]. The latter can potentially provide the relevant stakeholders (e.g. medical doctors and healthcare providers involved in a patient's case) access to the patient's health records authentically and securely. Also, blockchain-enabled IoT has been implemented to facilitate the monitoring and management of diseases. Some of its examples include wearable devices (for tracking vital signs and providing feedback), smart pills, and improved quality control. They also allow for tracking clinical drugs during their investigation, by checking their effectiveness as well as their side effects, without the risk of modified results [43].

Following are major research initiatives of blockchain in the healthcare industry:

A. PATIENT DATA MANAGEMENT

One of the primary challenges faced in maintaining the patient records is that the patients leave their health-related data scattered across various healthcare providers. The design of Electronic health record (EHR) was never meant to manage lifetime medical records, spread across various organizational setups. Further, the challenges in interoperability existing between various hospitals and service providers create additional barriers for the successful sharing of data. This lack of coordinated data management and data exchange implies that these health records are not integrated, but are rather fragmented. Blockchain aids in providing a structure for data sharing along with the security of these data [44]. In this way, healthcare providers can gather data from the patients which may include their date of birth, name, prescriptions followed and previous procedures performed, etc. This data is then saved on the cloud computing systems and in the organization's existing databases. A cryptographic hash of the data from each data source is computed and sent along with the patient's public ID to be stored in the blockchain. Smart contracts are useful in this case to manage access to patient data. Through an Application Programming Interface (API), healthcare stakeholders can query the blockchain and locate this data without revealing the patient's identity. The patient can share his/her complete medical history (with or without recognizable data) with any stakeholder if required [45].

Another work proposed by researchers in this area [45] achieves data provenance and trustless data sharing among all the parties involved. They propose a system called ''MeDShare'' that employs a blockchain network along with side-blocks and smart contracts. Side-blocks contain smart contract reports and help in maintaining the accuracy of the logs and efficiency of block fetching. Authors in [42] propose two algorithms based on a blockchain system for protecting the privacy of shared data in healthcare. The first approach uses a public key cryptography technique in which every node is assumed to have a public-private key pair. The second approach uses bilinear key pairing based on elliptical curve cryptography (ECC) to achieve privacy and distributed key management. A blockchain-based secure system for pervasive social networks (PSN) is proposed in [46]. Instead of using direct health data, the addresses of mobile devices and sensor nodes is stored in the blockchain. And the authorized PSN nodes can now access the health data from these sensors in a secure manner. An illustration of blockchain for patient data management is shown in Fig. 1.

B. DRUG TRACEABILITY

A major issue currently faced by the pharmaceutical industry is drug counterfeiting, with around 10-30% of the drugs sold in the developing world being fake. The counterfeit drug market amounts to a total of $200 billion annually; however, the online purchases of these drugs account for $75 billion of the total industry [47]. The major issue with these counterfeit drugs is not the fact that these drugs are not original but

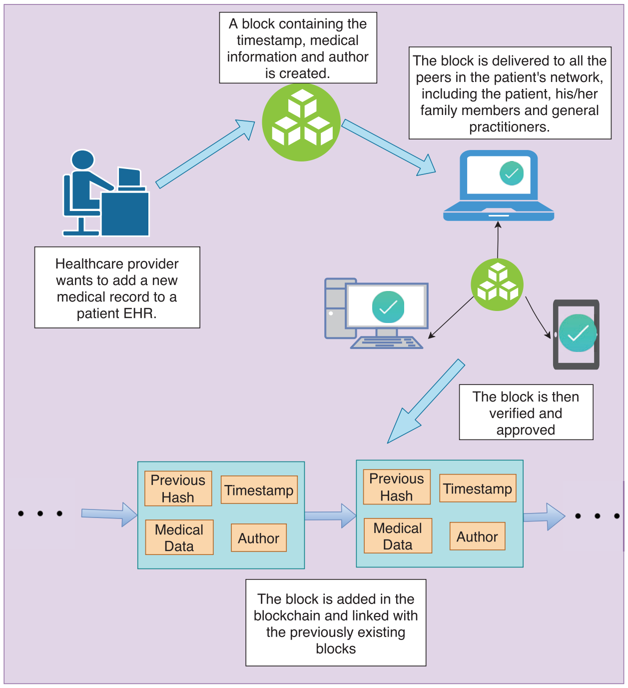

FIGURE 1. **Blockchain based Patient data management.**

rather that they can work in a very different way from the initially expected drug. This can prove to be hazardous for patients taking such counterfeit medicines, as it cannot treat the disease it was supposed to handle. Two major issues of drug traceability can be handled using blockchain technologies. Firstly, pharmaceutical companies can monitor their drugs in this supply chain, easily detecting any fake drugs in the chain. Secondly, the stakeholders, primarily the labs, are authorized to undertake action using their experience in instances of any issue by tracking the exact drug location. Tamper-resistance offered by the blockchain technology is useful in achieving traceability of drugs [48]. Every transaction going into the block of a blockchain is timestamped and immutable, which makes it convenient in tracking any product and ensuring that this information is not altered. For ensuring the traceability and authenticity of the drugs, the companies that are registering a product on the blockchain need to be trustworthy. Hence, only private blockchains that are under the control of a central entity are logical in ensuring that these counterfeit drugs are not registered. Therefore, access to the company's "drug blockchain" is proof that the drug manufactured by the company is genuine and not a fake product. The pharmaceutical companies have their say on which actors of the supply chain can act as miners. It can be retailers, manufacturers, or distributors, which is decided by the company. Each person has different rights depending on his location in the supply chain: labs can register any new drug whereas wholesalers can only verify the transactions. Once a drug is manufactured, a hash is produced which will contain all the relevant data regarding the product. Each time the drug is moved from one entity to another (e.g., from the manufacturer to the distributor), data gets saved in the blockchain technology, making it easier to track the drug. Authors in [49] show the benefit of using blockchain and smart contracts in the pharma supply chain. Doing away with manual intervention, the blockchain proposed by *Modum.io AG* in this paper uses smart contracts to assess and monitor the temperature and humidity levels read by the IoT sensors during the drug transportation process.

C. COMMERCIAL IMPLEMENTATIONS

We discuss popular commercial blockchain implementations in healthcare:

i. MedRec: MedRec [50] is a popular instantiation of health care blockchain architecture for storing EHRs efficiently and effectively. The patient, the health care provider as well as any third-party insurer/payer involved in the medical case could add data to the patient's health care record. The EHR in this implementation also has an integrated blockchain Patient Health Record (PHR) capability that enables the patient and the various providers in developing a longitudinal health care record comprising of a lifetime of health care cases for each patient.

ii. Medicalchain: Medicalchain [51] is a decentralized platform which is being used in the UK to maintain the patient data. It utilizes blockchain technology to create EHRs, focused on the needs of the user while keeping a single accurate edition of the data of the user. Medicalchain empowers its users to provide hospitals and healthcare providers access to their health data. The interactions with this data are then recorded securely and transparently on Medicalchain's distributed ledger (which is made up of a dual blockchain structure). One of the blockchains is built using Hyperledger Fabric and is responsible for managing access control to all the health records. The other blockchain is based on Ethereum, powered by an ERC20 token and forms the basis for services provided by the Medicalchain platform.

D. CHALLENGES

Anybody (EU countries mainly) using a healthcare blockchain will have to comply with the legal GDPR obligation of the European Union regarding the protection of the personal data [52]. Under this regulation, patients will soon have a right to get their healthcare-related data erased whenever they want, which goes contrary to the principles of a blockchain. Another challenge is regarding the size and type of patient data itself to be stored on the blockchain. Storage of medical scanning/imaging and other such high quality and large size data is another practical issue for a feasible, scalable and useful implementation of blockchain for healthcare. Storing only the hash of the medical data in the block may not help while retrieving the data at the healthcare provider's end since hashing is not a reversible function.

IV. SUPPLY CHAIN/LOGISTICS

With blockchain innovation, exchanges and transactions are reported in a permanent decentralized ledger [53]. These transactions are monitored transparently and securely. This can reduce human slip-ups and time delays and help to check the authenticity of the items by tracing their origin. Aspects of blockchain such as data accessibility and immutability greatly increase the transparency, reliability, and efficiency of the entire supply chain industry [54]. Important blockchain application areas in the supply chain industry are discussed below:

A. FOOD TRACEBILITY

Between 2013 and 2016, there was an outbreak of listeria infection in several states in the US due to the consumption of contaminated food products. By the time the source of contamination was identified, a significant amount of time had already passed, with more people infected by the bacteria. By the time the Food and Drug Administration (FDA) and the Center for Disease Control and Prevention (CDC) realized the extent of the infection it was early 2016 and the supplier in cooperation with these agencies finally recalled some of the contaminated food products. This recall was later expanded to include well over 300 products marketed under various brands. A tracking mechanism for the finished products from its source of origin and at various points in the supply chain could have averted this incident. Blockchain can efficiently address the traceability issue in food supply chains. Due to the lack of mechanisms for identifying and isolating contaminated food products, incidents such as listeria discussed above can cost a lot to the food and beverage companies. As per estimates, food recalls by companies in the US cost well over $3 billion per annum. Using blockchain's ability of product tracking, a statistical survey can be carried out to analyze various details such as the number of consumers falling ill, the food products they purchased and the retail/wholesale outlets which sold these products. These details can further help to trace the origin of the contamination, with possible details like the source of contamination, type of contamination and the intensity and impact of contamination.

Authors in [55] propose an Electronic Product Code Information Services (EPCIS) based blockchain management system for food traceability and show its superiority over the existing systems. The system model consists of an on-chain and an off-chain module. The blockchain is mainly used to store traceability information on-chain while most other food-related data is stored off-chain using EPC codes, thus alleviating the problem of data explosion. An RFID based end-to-end blockchain architecture for food traceability is proposed by researchers in [56] targetting food supply chains. They employ a new consensus algorithm called PoO, which exploits the primary difference between supply chain and cryptocurrency, to ensure immunity against cyber attacks and avoiding unnecessary transactions to be added to the blockchain, and thus making blockchain use cost-efficient.

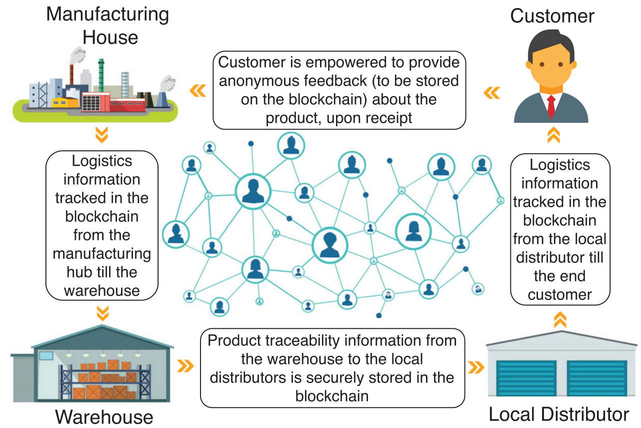

FIGURE 2. Blockchain for supply chain/logistics industry.

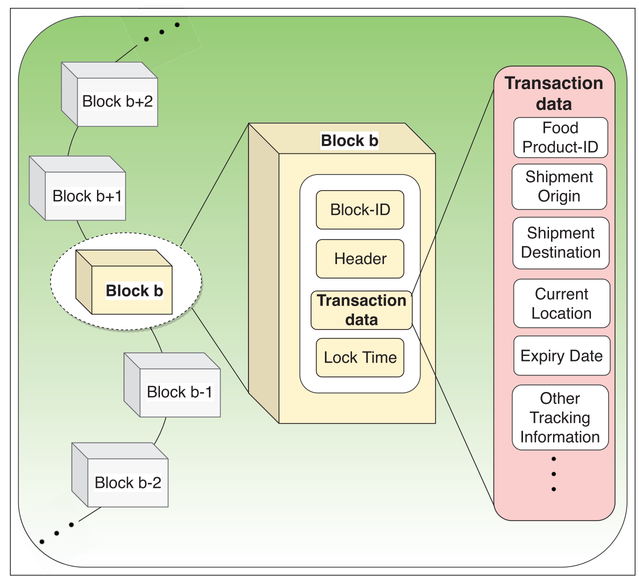

FIGURE 3. A sample block structure for food product traceability in the supply chain industry.

Blockchain flow for food product traceability in the supply chain/logistics industry is shown in Fig. 2, and a sample block structure of the blockchain containing essential details of the individual block is shown in Fig. 3.

B. SOLVING LOGISTICS INEFFICIENCIES

Every day, transporters, shippers, brokers, merchants, and other logistics experts must explore plenty of choices and "what if" situations when sending a truckload of products across the nation, all while recording each progression of the journey with extensive and thorough paperwork. Despite technological advances, logistics management is still in the need of improvement. Blockchain innovation is especially adroit at improving these complex and fragmented procedures by recording exchanges, tracking resources and making a transparent and effective framework for dealing with all archives engaged with the logistics procedure [57].

C. PRODUCT MANAGEMENT

Blockchain technology can contribute to supply chain product management in multiple ways by providing product transparency, traceability, and security. Authors in [58] propose a product ownership management system (POMS) which empowers the customer to reject counterfeit products which might have cloned genuine RFID tags also. They implement two smart contracts in this system, one for managing the manufacturers' information and the other for managing the products' information and together they verify the possession of products. A blockchain-based product traceability system using drones is proposed in [59] for Industry 4.0. This solution is shown to be five times faster than a human operator for inventory collection and management in a supply chain warehouse unit. The drone acts as a blockchain client for block creation and the blockchain is stored offline on a local storage network in the warehouse unit's server.

D. COMMERCIAL IMPLEMENTATIONS

There are several active commercial projects which are utilizing blockchain technology in the domain of supply chain management. Major active projects are listed below:

1) IBM Blockchain-TradeLens: IBM Blockchain provides solutions that cover all aspects of supply chain management, with a specific focus on logistics. Transparency and traceability are the most critical aspects of logistics, and IBM Blockchain can streamline business exchanges, transactions and trading associations with secure, worldwide business systems and networks. With the solutions like TradeLens – the new, open blockchain-fueled platform built to support worldwide trade – major logistics players are profiting by a common and shared ledger that is validated promptly with each system member [60]. The outcomes are streamlined stock administration, greater collaboration, improved resource usage and much more.
2) OriginTrail: OriginTrail [61] has been on a mission to bring transparency to complex international supply chains since 2013. It is a platform, which is already in use in the food industry, that lets its users know the whereabouts of their food products.
3) Blockverify: It is a blockchain-based anti-counterfeit solution presenting transparency in the supply chains. It is effectively being utilized in diamonds, pharmaceuticals, and a couple of electronic industries [62].

E. CHALLENGES

One of the important issues to be addressed while applying a blockchain solution for supply chains is that of supplier's/manufacturer's privacy. Any participating entity in the supply chain with access to the shared blockchain may be a potential competitor of the supplier/manufacturer and can gain unwarranted information from the blockchain. Another potential challenge is the cost of integration and adoption of the blockchain technology into the current infrastructure of legacy industries.

V. POWER INDUSTRY

The power industry has been undergoing major transformations over the past several years, with utilities embracing newer technologies and newer sources of power generation. With a deluge of smart and IoT enabled devices (ranging from smartphones to smart meters to electric vehicles) having variable power demands, and with mushrooming of many types of power generation schemes, the power grids are becoming very complex to handle. Blockchain as a tool can accelerate this global energy transformation by lowering the transaction costs and in operating the grid in a more efficient manner [63]. By enabling smart contracts between the different components and devices of the smart grid, they allow for optimized grid operations. Blockchain likewise enables buyers to move towards becoming *prosumers* (who consumes as well as produces) by empowering them to monetize their abundant power by safely recording information and sending and getting installments automatically, through smart contracts based on a platform such as Ethereum [64], [65]. Important research areas in blockchain applications for the power industry are discussed here:

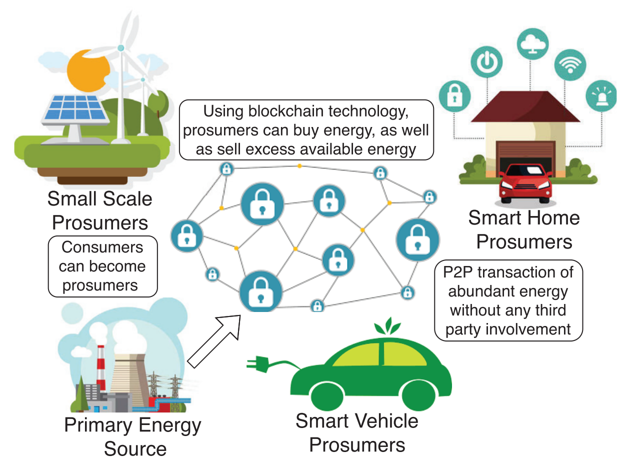

FIGURE 4. P2P energy trading using blockchain.

A. PEER TO PEER (P2P) ELECTRICITY TRADING

As per a recent GTM Research report [66], P2P grid networks are the focus of around 60% of blockchain-based projects in the power sector currently. These P2P networks are meant for facilitating energy trade between the individual entities of the network, by doing away with the involvement of a third party central authority. This concept would allow individuals who can produce renewable energy at home to sell their excess energy, and the individuals with a deficit could buy energy based on a mutually agreed-upon contract. Authors in [67] use a Blockchain platform to facilitate a secure P2P system for energy trade in IIoT. Another work [68] exploits Blockchain to develop an electricity trading system between Plug-in hybrid vehicles (PHEVs). Fig. 4 depicts a blockchain connected P2P energy trading system. While the traditional grid network lacks security and transparency regarding the energy transactions due to the presence of the third party entities, a blockchain-based smart grid provides for security and identity privacy of the parties involved.

B. SECURITY AND PRIVACY TECHNIQUES

Apart from giving consumers more efficiency and control over the energy sources, the property of immutability of blockchains makes them beneficial for security and privacy applications in the power industry. In April 2018, the Chilean National Energy Commission (CNE) announced that it had launched a blockchain project for the energy sector, the first of its kind from the nation's government. The proposed project will employ the Ethereum blockchain to record, store and track the energy data which may include fuel cost, market price, energy law compliance, etc. The prime impetus for this migration to blockchain-based approach is to lower the financial cost of unintentional errors such as clerical mistakes and corruption. In another work, a bloom filter based blockchain scheme for privacy preservation and efficient data aggregation in smart grids is proposed by authors in [69]. Researchers in [70] provide a blockchain-based transaction security framework for a decentralized smart grid environment.

C. COMMERCIAL IMPLEMENTATIONS

Here we discuss a couple of active commercial projects of blockchain implementation in the power sector:

1) PowerLedger: PowerLedger provides a market trading platform based on blockchain technology, enabling the owners of renewable energy sources to sell their energy surplus at a pre-determined price within the microgrids or over the distribution network [71], [72]. Distribution system operators receive revenue for the energy traded over the distribution network.
2) Bankymoon: Bankymoon provides blockchain-enabled smart prepaid energy meters, targetting schools and communities around the world in need of affordable power supply. With the facility of transferring and reloading the smart meters with Bitcoins, it not only benefits the customers, but the power suppliers also get on-time payment [73], [74].

D. CHALLENGES

As per the Bitcoin energy consumption report, 30 billion kWh electricity was consumed for carrying out 30 million transactions, accounting for 0.13% of energy consumption worldwide [75]. For the energy sector, the number of transactions can be safely multiplied 1000 times. This, in turn, can show that energy consumption for such blockchain-based transactions will be prohibitively high. Thus, the scalability of currently available blockchain solutions for the power sector is a high challenge.

VI. AGRICULTURE INDUSTRY

The agricultural industry depends on various external factors (such as climate, quality of reap, etc) and complex supply chains that could be made increasingly transparent by implementing blockchain technology. Using blockchain the journey of yield from the farm to the supermarket could be made accessible to all who need to see it – giving consumers a sense of security and control [76], [77]. It additionally permits small producers, with fewer assets, to access similar data as more affluent farms – making the market a more transparent space. A blockchain connected agricultural industry is depicted in Figure 5.

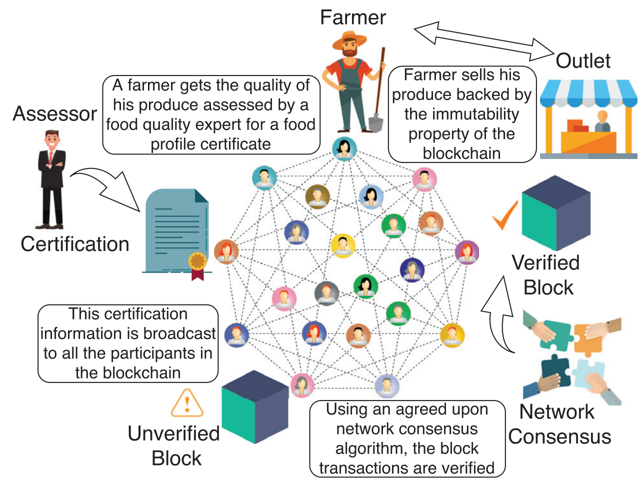

FIGURE 5. Blockchain connected agriculture sector.

Recent research in applying blockchain to the agricultural industry is discussed here:

A. AGRI-FOOD TRACEABILITY

Researchers in [78] propose and develop a blockchain-based decentralized solution called *AgriBlockIoT* for food traceability in the agricultural supply chain. This solution seamlessly integrates digital data produced by the IoT sensors along with the blockchain. Being a platform-agnostic solution, it has been shown to work on both Ethereum and Hyperledger platforms. Another work [79] discusses a case study for tracking quality assurance using Hyperledger blockchain technology. Using standard quality assurance procedures, grain quality profiles are generated and shared across the chain transparently.

B. COMMERCIAL IMPLEMENTATIONS

Some commercial implementations of blockchain in the agriculture industry are listed below:

i. iGrow is a commercial center that associates landowners, farmers, investors, and harvest purchasers to make a complete supply chain for organic food [80]. In the first stage, the iGrow team identifies crops with stable demand, prices and growing characteristics. In the second stage, the team finds arable land and the farmers to work on it. In the third stage, iGrow raises capital for seeds from urban people that want to have a connection with their neighboring countryside: this way they can see their investments grow. Finally, the platform connects all of these actors with the ultimate buyers, so everyone has a share of revenue and the consumers get their healthy crops. Agriculture Blockchain by iGrow has created a better network by connecting all the farmers on the same platform with the real-time market.

ii. Avenews-GT provides a platform for commercial trade of agricultural produce where dedicated farmers, agricultural cooperatives can conduct the entire trade process in a secure and transparent ecosystem. The blockchain records trade interactions and sharing of trade-related data among the partners involved in a transparent and trusted manner.

C. CHALLENGES

Since the data going into the blockchain is supposed to be open and transparent, it could be a challenge to convince and encourage small scale customers to adopt the blockchain technology. Most blockchain-based solutions currently on data collected through IoT sensors. Thus in addition to paying for the subscription of this technology, the involved parties also have to pay for the enablement of IoT, further leading to higher costs. Unless return on investments is high, the complexities involved in the blockchain technology will be a deterrent to the introduction of blockchain-based solutions in the agricultural industry.

VII. MANUFACTURING INDUSTRY

In the manufacturing industry, manufacturers have to publish technical manuals of their products which have to be distributed in the repair and maintenance departments. These technical records have to be released and timely updated, which is a very tedious process and involves tonnes of paperwork. By using blockchain technology, the technical publication can rest on this framework and is accessible to the users of blockchain without worrying about the version changes or losing the latest publication. Blockchain has significantly enhanced the working efficiency in the manufacturing industry by uploading the data on the shared ledger. For example, in the automobile manufacturing industry, tracking of the spare parts becomes vital, because the availability of the parts, in real-time, is not known. Blockchain technology helps resolve this issue by updating the relevant information of the spare parts on the shared ledger which is available to all the entities involved, for instance, car manufacturer, warehouse distributors, etc as shown in the Fig. 6.

Recent research in applying blockchain to the manufacturing industry is discussed below:

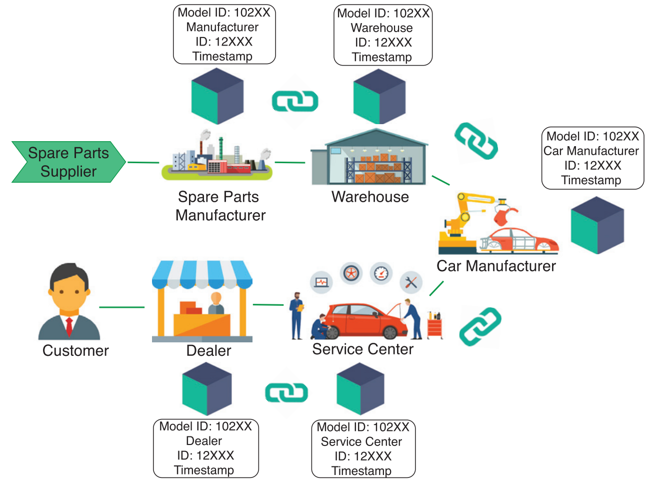

FIGURE 6. Tracing of spare parts using blockchain in automobile industry.

A. SECURITY AND PRIVACY TECHNIQUES

The manufacturing sector has begun a new boom period with the assimilation of Industrial IoT (IIoT) techniques. But this has not come without its share of security and privacy concerns. Authors in [81] propose a solution based on blockchain for securing data interactions in a smart factory setup. They use a private blockchain architecture inspired by Bitcoin, which comprises of an intranet for data collection and storage and an extranet for data utilization. While the equipment data is still stored on the cloud, only the interaction data goes onto the block, thus making it a lightweight and secure solution. Another work proposes a credit-based consensus security mechanism for the factories [21]. In this work, the authors use a directed acyclic graph (DAG) based blockchain, which they show to be more practical for realistic applications in power-constrained IoT devices. Their approach adopts an asynchronous credit-based proof-of-work consensus mechanism instead of synchronous consensus which is generally used in a chain-structured regular blockchain. This mechanism works by increasing the power consumption and computational complexity for malicious nodes while decreasing the same for honest nodes in the blockchain network.

B. OTHERS

Blockchains are being researched in many other areas of manufacturing as well. Researchers in [82] proposed and simulated a distributed blockchain-based framework on Ethereum to build a sustainable automotive industrial ecosystem. Another work [83] discusses *FabRec*, a decentralized methodology used to deal with manufacturing information generated by different manufacturing entities utilizing blockchain innovation. The decentralized information is made available to all the nodes in this peer-to-peer network. Verified manufacturers in any part of the world can be provided access to this blockchain network. This system was demonstrated on Ethereum platform using the PoA consensus algorithm.

C. CHALLENGES

Each manufacturer may be part of multiple blockchains, thus the need for a setup to manage all these chains. For a seamless integration of these blockchains, these different blockchain implementations have to be standardized and interoperable. Since different organizations are creating proprietary blockchains, interoperability would be a huge challenge to consider.

VIII. E-COMMERCE AND RETAIL INDUSTRY

E-commerce and retail business also may reap the benefits of advances in blockchain technology soon. This is yet another industry which researchers have started exploring for checking the applicability of blockchain technology. Figure 7 depicts one scenario of applying blockchain in the retail industry.

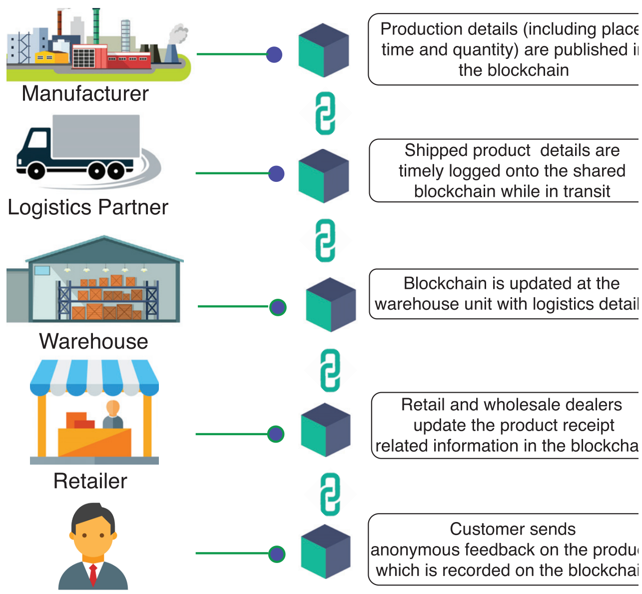

FIGURE 7. **Tracking product using blockchain in retail industry.**

A. SECURITY AND PRIVACY

E-commerce based on IoT is the new emerging business model with requirements of transactions to be secure, autonomous and lightweight. Authors in [84] propose a lightweight blockchain platform for E-commerce transaction management using the consensus mechanism called Practical Byzantine Fault Tolerance (PBFT). This 3-layered blockchain network is shown not only to be highly scalable and efficient but also secure against cyber attacks. For better performance in terms of reduced overhead, they implement this blockchain using C++ instead of using a standard blockchain framework like Ethereum. Blockchain technology offers transparency and traceability that can potentially help to eliminate difficulties faced in the retail business and provide trust, value, and incentive to the customers [85]. Blockchain brings with it the ability to have an audit trail to track a retail product right from its place of origin. Researchers in [86] propose a reputation system for retail business, that provides privacy to the consumer's feedback. They developed this system based on the Ethereum platform using the PoS consensus algorithm. The token generation for rating the retailers happens off-chain and thus reduces the overall computational overhead also.

B. CHALLENGES

As per the India Brand Equity Foundation (IBEF) report, more than 1 million e-commerce transactions were happening every day in India alone [87] as of January 2018, what to talk of the scenario world over. With very few e-commerce players sharing a major chunk of these transactions, it calls for these select companies to invest heavily in blockchain technology. The other minor players might just skip this technology, owing to high investment and maintenance costs. Also due to the cut-throat competition in this industry, inherent data transparency of blockchain may be another deterrent for the quick adoption of this technology.

IX. SUMMARY OF WORKS

In Table 2, we present a summary of all industry-specific case studies reviewed in this study giving details of the blockchain technology employed in each industry. For each case study, the problem addressed and the solution proposed are discussed. Technical details of blockchain such as consensus algorithm used, the blockchain platform used, transaction data which goes into each block, and the status of smart contracts usage have also been discussed.

X. OPEN ISSUES AND NEWER APPLICATION AREAS

In this section, we discuss some of the pressing open issues in the adoption of blockchain in the IIoT scenario and discuss newer application areas in Industry 4.0 and IIoT where blockchain is being experimented for identifying possible solutions.

A. OPEN ISSUES

1) SCALABILITY

Scalability issues in the existing blockchain technologies are a major deterrent in wide acceptance and deployment of blockchains (e.g. VISA can process around 2000 transactions per second [94], whereas Bitcoin can process only up to 7 transactions in one second [95]). In current blockchain implementations, each fully participating node is required to hold a blockchain copy. In contrast to traditional databases, this leads to huge storage overhead. Specifically in the IIoT scenario, with the growing number of sensor nodes and the amount of data generated, the problem is compounded. Although recent lightweight platforms like Ethereum have been developed [96], blockchain deployments remain out of scope for resource and storage constrained IoT devices.

2) SECURITY AND PRIVACY

IoT networks are already prone to various security attacks like replay attacks [97] and eavesdropping attacks [98]. Along with these security risks, blockchains bring their own set of security vulnerabilities. Some of the known security vulnerabilities in blockchain technology are smart contract program vulnerabilities [99], message hijack [100], etc. Privacy leakage is another concern in blockchains, as shown

TABLE 2. Summary of works.

Ref.	Problem addressed	Solution Proposal	Consensus Algorithm	Smart Contract Used?	Platform	Transaction data
			Healthcare Industry			
[90]	Decentralized Record Management System	Distributed Ledger Protocol	PoA	Used	Ethereum	Medical Records
[53]	Securing Health Records	Dual blockchain structure	PoC	Used	Ethereum and Hyperledger Fabric	Patient Record, Medical Record and Practitioner's Public Profile
[45]	Minimizing risk to data privacy	Smart contract with side-blocks	DNA*	Used	Private Blockchain	Data owner identity, requestor identity, sensitivity of data
[42]	Healthcare with smart medicine	Public key cryptography and bilinear pairing technology	PoA	Used	Private Blockchain	Medical records of user
[48]	Sharing health data in pervasive social network	Blockchain for sensor address storing with IEEE 802.15.6 protocol	PoA	Not Used	Private Blockchain	addresses, contributor's signature of health data, standard profile
[51]	Data integrity for pharma supply chains	IoT with smart contracts	PoC/ PoE	Used	Ethereum	Temperature, humidity data, serial number
[91]	In-home therapy management without third party	Blockchain Tor-based distributed transactions	DPoA	Used	Permissioned Ethereum and Private Hyperledger	Patient information and treatment profile, healthcare provider details
			Supply Chain Industry			
[58]	Reducing operational cost for food traceability	RFID based architecture with blockchain	PoO	Used	Private Blockchain	Sensor data, sensor type, location, manufacturer
[57]	Alleviating data explosion	on-chain and off-chain data storage	PoA	Used	Ethereum	Process support data, e.g. company ID, address index, traceability information
[61]	Traceability of products	UAV-based inventory information tracking	PoD	Used	Private blockchain	Inventory data of products
[62]	Tangible and intangible asset tracking	Hyperledger Fabric	PoC	Used	Hyperledger Fabric	Cargo details, shipping milestones

TABLE 2. *(Continued.)* Summary of works.

Ref.	Problem addressed	Solution Proposed	Consensus Algorithm	Smart Contracts Used?	Platform	Transaction data
[63]	Data exchange between companies with safety and integrity	Blockchain with industry standards for data exchange (GS1, IoT, etc)	PoC	Used	Ethereum	Trade transactions, physical or digital activity in the supply chain of assets
[64]	To tackle counterfeiting and forgeries in supply chain	Private blockchain with a private key per product	DNA*	DNA*	Bitcoin with a private blockchain	Product ID, consumer ID, retail location
Power Industry						
[69]	Optimal loan pricing in credit-based payment	Game theory	PoA	Not Used	Private blockchain	Transaction related energy coins
[72]	Security and privacy of decentralized grid transactions	Multisignature and encrypted transactions through anonymous message communication channels	PoA	Used	Bitcoin	Tuples of encrypted transaction data
[70]	Localized electricity transaction security and privacy	Consortium blockchain based P2P trading model	PoA	Not Used	Consortium Blockchain	Energy trading information like data type, pseudonyms for privacy, Energy coins for asset tracking
[71]	Privacy preserving and efficient data aggregation	Bloom filter and block chain, Pseudonyms	PoA	Not Used	Private blockchain	Electricity Consumption Data
[24]	Seamless connection of heterogenous vehicular context	Combined EV cloud computing and EV edge computing	PoA and PoS	Not used	Distributed consortium blockchain	Data coin
Manufacturing Industry						
[83]	To enhance security and privacy in manufacturing	Bitcoin inspired IIoT architecture	PoA	Not used	Private blockchain	Request address, request content, response from the management hub
[21]	Single point failure and malicious attack on IIoT systems	Directed acyclic graph (DAG) structured blockchain	Credit-based consensus mechanism	Not used	Consortium blockchain	Sensor readings

TABLE 2. *(Continued.)* Summary of works.

Ref.	Problem addressed	Solution Proposed	Consensus Algorithm	Smart Contracts Used?	Platform	Transaction data
[84]	Building a sustainable platform for the automotive ecosystem	Blockchain-based distributed framework	PoC	Used	Ethereum	Speed, mileage, driving behaviors, damaged parts
[85]	Sharing information in a trustless network	Decentralized P2P blockchain framework	PoA	Used	Ethereum	Machine type, type of event recorded
Agriculture Industry						
[80]	Trust and reliability in agri-food supply chain	IoT with blockchain	DNA*	Used	Ethereum, Hyperledger Sawtooth	Sensor data at each stage of the supply chain
[81]	Tracking grain quality in agri-food supply chain	Permissioned blockchain	PoC	Used	Hyperledger Fabric	Certified grain quality data
Education Industry						
[92]	Need for a credit platform for global higher education	European Credit Transfer and Accumulation System (ECTS)	Distributed PoS	Not used	Consortium blockchain	Educational institution's ID, anonymous student details, course ID, number of credits for a course
[93]	Technology for recording learning outcome of learners	Electronic Learning Contract (ELC), global support system	PoAc	Used	Private blockchain	Course name/ID, course weightage, maximum course credits and course credits obtained
Drone (UAV) Industry						
[94]	Security (confidentiality and integrity) in semi-autonomous UAVnets	Dynamic partitioning of UAV groups	PoG	Used	Private blockchain	Details of participating UAVs, sensor data, flight control algorithm, route information with coordinates
[95]	Detection of compromised UAVs	Private key cryptography with a pre-registered UAV list	PoA	Used	Hyperledger Indy	Details of the surveillance UAVs

*DNA = Data Not Available

in [101] (e.g. there is a risk of potential privacy breach with transaction data being stored on the blockchain [102]).

3) ENERGY AND COST EFFICIENCY

Consensus algorithms like PoW executed in the process of mining blockchains are known to consume a lot of electricity and are thus computationally quite expensive [103]–[105]. As the size of blockchain grows over time, more powerful miners have to be deployed for running these algorithms. Some energy-efficient consensus protocols such as PoS [106], DPoS [107], Proof of Trust [108] have been proposed in recent times. Instead of storing the whole blockchain data, these protocols store only the most recent transaction data on the blockchain. Nevertheless, energy and resource-constrained IIoT devices are still overwhelmed by huge amounts of industrial data generated. Thus, the design of more efficient consensus algorithms is still an open challenge.

4) RESOURCE CONSTRAINTS

Current blockchain implementations require stable network connections. IIoT devices do not always guarantee stable network connections, thus the implementation of blockchain technology is a challenge in this scenario. Also, blockchains incur high network overhead which further is a challenge for integration into IIoT [109]. Degree of decentralization possible in current implementations of blockchain integrated IoT networks is also limited, due to resource limitations of IoT devices and networks [102].

5) REGULATIONS

Since blockchain works in a decentralized way without reliance on a third party central authority, industrial standards and government regulations must be enforced [110]. With many new blockchain platforms being proposed, the need for timely enforcement of industry standards for block data formats and interfacing formats has increased even more.

B. NEWER APPLICATION AREAS

1) DRONE INDUSTRY

The newest industry where blockchains are being tried and tested is the drone industry. Drones or Unmanned Aerial Vehicles (UAVs) as are called now being deployed on a large scale for civilian purposes, diverging from their traditional use in military applications. Security of UAVnet (UAV networks) is an important research area, with many research works in this area. Not many research works exist currently in the literature discussing blockchain applicability for UAVs. In [92] researchers propose integrating blockchain technology with UAVnet, where each UAV in the network will function as a blockchain node. This approach is supposed to protect the network from hacking attacks where the attacker tries to intercept the control and communications commands to take control of the individual nodes in the network. Another work [93] proposes using an asymmetric key encryption technique for detecting compromised UAVs in a surveillance application. They use the *ABS-SecurityUAV* simulator for validating their technique, and show that 90% of the UAVs were able to reach the right consensus, and detect the compromised UAV. Thus, a compromised UAV sending incorrect information (in the form of fake alerts of detecting an intruder) will not be able to add data blocks in this blockchain, since the other UAVs in the network also participate in the consensus algorithm.

2) EDUCATIONAL INDUSTRY

As the power of web-based distance learning increases, so does the need for an independent and transparent way of verifying educational records and transcripts of students. A blockchain-based platform could serve as a notary for educational records, creating a way for educational institutions and employers to access secure transcripts and records. It could also enable the collaboration of universities and other academic institutions [111]. The increasingly dynamic nature of employment implies that more qualifications are required as career paths deviate across disciplines and organizations. Often qualifications are necessary just to apply for a role, and with the rise in demand, educational dishonesty is also increasing. However, blockchain can become the backbone of educational proof, giving employers the data required to determine whether a candidate's resume is accurate [112]. In the US, MIT is already implementing blockchain technology. They built an app, called Blockcerts Wallet, which enables graduates to securely share a tamper-proof and verifiable digital version of their degrees with prospective employers. It is simple to understand and use: a digital token represents the qualifications and credentials can be added to the app, providing both a digital degree and instant verification of authenticity. The portal uses the digital ledger to locate the transaction ID, verifying the keys, and confirming that nothing has been altered since the record was added. As each certificate is logged as a transaction on the blockchain network, it prevents tampering or fraud [113], [114].

3) MUSIC INDUSTRY

A smart contract ensures the authenticity of a copyrighted product. These contracts define and automate the relationships and interactions between the stakeholders of a product. They also aid in ensuring that the product a customer is buying is authentic and not just a perfect copy. A potential use case of smart contracts in the music industry is the music rights management. With the rise of the Internet and mushrooming of several online music streaming services, the music industry has been undergoing a major change in the last 10-15 years. Songwriters, artists, publishers, streaming service providers and many others involved in this industry have been affected by this change. The method of royalty determination in the music business has always been a complicated task, but with the Internet rise, this process has become even more complex. Blockchain technology can help to make the royalty payment process transparent by maintaining an accurate and comprehensive decentralized database for storing information (in the form of a public ledger) of music rights ownership. It would do away with the intermediation of the industry, allowing artists to create and capture more value from their products [115]. In addition to this, as determined by the smart contracts the royalty split for each work could be added to the ledger thus guaranteeing a fair royalty share to the original stakeholders of the copyrighted product [116].

4) TAXI INDUSTRY

Current ride-sharing services such as *Uber* work with a centralized model, running algorithms from their dispatch centers to control their fleet of cabs. Blockchain could provide a decentralized and distributed approach to the existing model, with cab riders and drivers creating a more customer-driven consumer place [117]. Drivers can also collaborate to operate on a larger scale, allowing for building trust and better coverage. They can also create a recurring list of clients whom they can rely upon for regular income and the customers will have a driver that they can trust. The California-based startup *Chasyr* is trying the same with its platform. A new P2P ride-sharing startup based on Ethereum blockchain called *Arcade City* is giving a stiff competition to the existing ride-sharing services with the motivation of eliminating the middleman involved and in saving the driver rights [118], [119]. Unlike the negative experiences of the current services based on a centralized model, the drivers can experience complete autonomy. The drivers in this service are free to converse with the customers, fix their charges, choose the payment method of their choice and collaborate with other drivers.

XI. CONCLUSION

The use of blockchain technology in IoT-enabled industries (Industry 4.0 and Industrial IoT) is expected to grow and benefit a broad range of industrial sectors. Tamper-proof and resilient techniques of record-keeping are said to be the game changers offered by this technology. As seen in multiple case studies reviewed in this paper, there have been significant investments in blockchain. In spite of scalability issues, the traditional method of centralized data sharing has been considered safer compared to a decentralized approach, and has been in practice in the industry for so long now. This is set to change now with blockchain promising solutions for addressing both security and integrity issues. In this paper, we surveyed the latest research work conducted on blockchain applicability in multiple IIoT-specific industries. We also looked into various commercial implementations of blockchain in the Industry 4.0 and IIoT to provide an Abstract measure of adoption in practice. And we further discussed the challenges faced by each of these industries for implementing blockchain. While many blockchain projects have emerged in the last few years, research in the blockchain is in its infancy. For blockchain to be fully utilizable and customizable, industry-oriented research should be further directed to address many of these challenges including personal data protection, scalability of block data, data secrecy and privacy of the participating organization, blockchain integration and adoption cost, and governmental regulations.

REFERENCES

[1] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.

[2] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[3] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[4] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2018.

[5] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, Jan. 2018.

[6] C. Shen and F. Pena-Mora, "Blockchain for cities—A systematic literature review," *IEEE Access*, vol. 6, pp. 76787–76819, 2018.

[7] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.

[8] H. Lu, K. Huang, and M. Azimi, "Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks," *IEEE Access*, vol. 7, pp. 41426–41444, 2019.

[9] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[10] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[12] D. Larimer, "Transactions as proof-of-stake," Apr. 2018. [Online]. Available: https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf

[13] D. Larimer, "Delegated proof-of-stake (DPOS)," Bitshare White Paper, 2014. [Online]. Available: https://www.bitshares.foundation/papers/BitSharesBlockchain.pdf

[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[15] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, Feb. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864818301536, doi: 10.1016/j.dcan.2019.01.005.

[16] R. M. Parizi, Amritraj, and A. Dehghantanha, "Smart contract programming languages on blockchains: An empirical evaluation of usability and security," in *Proc. Int. Conf. Blockchain (ICBC)*, in Lecture Notes in Computer Science, vol. 10974, S. Chen, H. Wang, and L. J. Zhang, Eds. Cham, Switzerland: Springer, 2018, pp. 75–91.

[17] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains," in *Proc. 28th Annu. Int. Conf. Comput. Sci. Softw. Eng. (CASCON)*, 2018, pp. 103–113.

[18] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia Comput. Sci.*, vol. 123, pp. 116–121, Aug. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050918300206, doi: 10.1016/j.procs.2018.01.019.

[19] *Announcement of the Industrie 4.0 Project in the 2011 Hannover Fair*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.vdinachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-Dinge-Weg-4-industriellen-Revolution

[20] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, 2018.

[21] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 3680–3689, Jun. 2019.

[22] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3632–3641, Jun. 2019.

[23] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019.

[24] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.

[25] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[26] S. Zhao, S. Li, and Y. Yao, "Blockchain enabled industrial Internet of Things technology," *IEEE Trans. Comput. Social Syst.*, to be published.

[27] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[28] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," 2019, *arXiv:1906.00245*. [Online]. Available: https://arxiv.org/abs/1906.00245

[29] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[30] M. H. Kassab, J. DeFranco, T. Malas, P. Laplante, and V. V. G. Neto, "Exploring research in blockchain for healthcare and a roadmap for the future," *IEEE Trans. Emerg. Topics Comput.*, to be published.

[31] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[32] A. S. Musleh, G. Yao, and S. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.

[33] J. A. Jaoude and R. G. Saade, "Blockchain applications—Usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.

[34] K. Zhou, T. Liu, and L. Zhou, "Industry 4.0: Towards future industrial opportunities and challenges," in *Proc. 12th Int. Conf. Fuzzy Syst. Knowl. Discovery (FSKD)*, 2015, pp. 2147–2152.

[35] R. Davies, "Industry 4.0 digitalisation for productivity and growth," European Parliament PE 568.337, Eur. Parliamentary Res. Service, vol. 1, Sep. 2015. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf

[36] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. IEEE Int. Conf. Ind. Eng. Manage.*, Dec. 2014, pp. 697–701.

[37] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2389–2406, 3rd Quart., 2018.

[38] S. Weyer, M. Schmitt, M. Ohmer, and D. Gorecky, "Towards industry 4.0-standardization as the crucial challenge for highly modular, multi-vendor production systems," *IFAC-Papersonline*, vol. 48, no. 3, pp. 579–584, 2015.

[39] (2019). *The Industrial Internet of Things (IIoT): Innovation, Benefits and Barriers*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/

[40] M. Weyrich and C. Ebert, "Reference architectures for the Internet of Things," *IEEE Softw.*, vol. 33, no. 1, pp. 112–116, Jan./Feb.2015.

[41] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[42] H.-T. Wu and C.-W. Tsai, "Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 65–71, Jul. 2018.

[43] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of Internet of Things infrastructure for secure and smart healthcare," *Computer*, vol. 50, no. 7, pp. 74–79, Jul. 2017.

[44] T. Nugent *et al.*, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, vol. 5, no. 2541, Oct. 2016, doi: 10.12688/f1000research.9756.1.

[45] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[46] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[47] (2018). *NCBI*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4105729/

[48] B. Alangot and K. Achuthan, "Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud," in *Proc. Int. Conf. Ubiquitous Commun. Netw. Comput.*, Bangalore, India. Cham, Switzerland: Springer, Aug. 2017, pp. 189–195.

[49] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.

[50] (2016). *MedRec*. Accessed: Apr. 12, 2019. [Online]. Available: https://medrec.media.mit.edu/

[51] (2019). *Medicalchain*. Accessed: Apr. 12, 2019. [Online]. Available: https://medicalchain.com/en/

[52] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.

[53] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *Proc. 2nd Int. Conf. Contemp. Comput. Inform. (ICI)*, Dec. 2016, pp. 463–467.

[54] G. Perboli, M. Stefano, and R. Mariangela, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018.

[55] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, Feb. 2019.

[56] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID based information architecture for food supply chain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5803–5813, Jun. 2019.

[57] N. Álvarez-Díaz, J. Herrera-Joancomartí, and P. Caballero-Gil, "Smart contracts based on blockchain for logistics management," in *Proc. 1st Int. Conf. Internet Things Mach. Learn.*, 2017, p. 73.

[58] K. Toyod, P. T. Mathiopoulo, I. Sasase, and T. Ohtsuk, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[59] T. M. Fernández-Caramés, O. Blanco-Novoa, M. Suárez-Albela, and P. Fraga-Lamas, "A UAV and blockchain-based system for industry 4.0 inventory and traceability applications," *Multidisciplinary Digit. Publishing Inst.*, vol. 4, no. 1, p. 26, 2018.

[60] T. Scott. (2018). *TradeLens: How IBM and Maersk are Sharing Blockchain to Build a Global Trade Platform*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.ibm.com/blogs/think/2018/11/tradelens-how-ibm-and-maersk-are-sharing-blockchain-to-build-a-global-trade-platform/

[61] (2019). *OriginTrail*. [Online]. Available: https://origintrail.io/

[62] C. Hulseapple. (2015). *Block Verify Uses Blockchains to End Counterfeiting and Make World More Honest*. Accessed: Apr. 12, 2019. [Online]. Available: https://cointelegraph.com/news/block-verify-uses-blockchains-to-end-counterfeiting-and-make-world-more-honest

[63] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, 2018.

[64] E. R. Sanseverino, M. L. Di Silvestre, P. Gallo, G. Zizzo, and M. Ippolito, "The blockchain in microgrids for transacting energy and attributing losses," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jun. 2017, pp. 925–930.

[65] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[66] (2019). *GTM Research Report 2018*. [Online]. Available: https://www.greentechmedia.com/articles/read/four-predictions-for-blockchain-in-energy-in-2018
[67] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[68] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.
[69] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.
[70] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
[71] (2018). *Power Ledger*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.powerledger.io/
[72] (2018). *Power Ledger White Paper*. [Online]. Available: https://powerledger.io/whitepaper/
[73] (2019). *Bankymooon—Blockchain Powered Solutions and Services*. [Online]. Available: http://bankymoon.co.za/
[74] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct./Nov. 2017, pp. 6153–6158.
[75] (2019). *Bitcoin Energy Consumption Index*. [Online]. Available: https://digiconomist.net/bitcoin-energyconsumption
[76] F. Yiannas, "A new era of food transparency powered by blockchain," *Innov., Technol., Governance, Globalization*, vol. 12, nos. 1–2, pp. 46–56, 2018.
[77] 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. IoT Vertical Top. Summit Agricult. Tuscany (IOT Tuscany)*, May 2018, pp. 1–4.
[78] 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. IoT Vertical Top. Summit Agricult.-Tuscany (IOT Tuscany)*, May 2018, pp. 1–4.
[79] P. Lucena, A. P. Binotto, F. D. S. Momo, and H. Kim, "A case study for grain quality assurance tracking based on a blockchain business network," 2018, *arXiv:1803.07877*. [Online]. Available: https://arxiv.org/abs/1803.07877
[80] (2019). *iGrowchain*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.igrowchain.com
[81] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3652–3660, Jun. 2019.
[82] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4197–4205, Jul. 2018.
[83] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A case study for blockchain in manufacturing: 'FabRec': A prototype for peer-to-peer network of manufacturing nodes," *Procedia Manuf.*, vol. 26, pp. 1180–1192, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978918308308, doi: 10.1016/j.promfg.2018.07.154.
[84] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2018.
[85] R. M. Parizi and A. Dehghantanha, "On the understanding of gamification in blockchain systems," in *Proc. 6th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2018, pp. 214–219.
[86] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3527–3537, Jun. 2019.
[87] *IBEF*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.ibef.org/download/Ecommerce-Report-Jan-2018.pdf
[88] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, 2016, pp. 25–30.
[89] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.
[90] M. Turkanovic, M. Hölbl, K. Košic, M. Hericko, and A. Kamišalic, "EduCTX: A Blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.
[91] 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.
[92] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Inform. (SOLI)*, Jul./Jul. 2018, pp. 32–37.
[93] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Netw.*, vol. 86, pp. 72–82, Apr. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1570870518301689, doi: 10.1016/j.adhoc.2018.11.010.
[94] *Bitcoin and Ethereum vs Visa and PayPal Transactions Per Second*. Accessed: Apr. 12, 2019. [Online]. Available: http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/
[95] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, and E. G. Sirer, "On scaling decentralized blockchains," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), J. Clark, S. Meiklejohn, P. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds. Berlin, Germany: Springer, 2016, pp. 106–125. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-662-53357-4_8#citeas
[96] *Ethereum Light Client Protocol*. Accessed: Apr. 12, 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/Light-client-protocol
[97] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[98] X. Li, H. Wang, H.-N. Dai, Y. Wang, and Q. Zhao, "An analytical study on eavesdropping attacks in wireless nets of things," *Mobile Inf. Syst.*, vol. 2016, pp. 1–10, 2016, Art. no. 4314475, doi: 10.1155/2016/4313475.
[99] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17318332, doi: 10.1016/j.future.2017.08.020.
[100] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 375–392.
[101] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.
[102] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, Mar. 2019.
[103] J. Mendling *et al.*, "Blockchains for business process management—Challenges and opportunities," *ACM Trans. Manage. Inf. Syst.*, vol. 9, no. 1, pp. 4:1–4:16, Feb. 2018. [Online]. Available: http://doi.acm.org/10.1145/3183367
[104] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov./Dec. 2016, pp. 1–6.
[105] N. Bozic, G. Pujolle, and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," in *Proc. 3rd Smart Cloud Netw. Syst. (SCNS)*, 2016, pp. 1–8.
[106] *Telehash*. Accessed: Apr. 12, 2019. [Online]. Available: http://telehash.org
[107] *DPOS Description on Bitshares*. Accessed: Apr. 12, 2019. [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html
[108] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Trans. Services Comput.*, vol. 12, no. 3, pp. 429–445, May/Jun. 2018.

[109] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun., IEEE 14th Int. Conf. Smart City, IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2016, pp. 1392–1393.
[110] Cost Per Transaction, "Blockchain: Opportunities for health care," *CP Trans.*, 2016.
[111] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learn. Environ.*, vol. 5, no. 1, p. 1, 2018.
[112] E. E. Bessa and J. S. B. Martins, "A blockchain-based educational record repository," 2019, *arXiv:1904.00315*. [Online]. Available: https://arxiv.org/abs/1904.00315
[113] (2019). *Blockcerts*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.blockcerts.org
[114] Datadriveninvestor. (2019). *What is Blockcerts and How it Issues Verifiable Blockchain Records?* Accessed: Apr. 12, 2019. [Online]. Available: https://www.datadriveninvestor.com/2019/01/15/what-is-blockcerts-how-it-issues-verifiable-blockchain-records/
[115] C. Sitonio and A. Nucciarelli, "The impact of blockchain on the music industry," in *Proc. 29th Eur. Regional Conf. Int. Telecommun. Soc. (ITS)*, in Towards a Digital Future: Turning Technology Into Markets? Trento, Italy, Aug. 2018. [Online]. Available: http://hdl.handle.net/10419/184968
[116] N. Nizamuddin, H. Hasan, K. Salah, and R. Iqbal, "Blockchain-based framework for protecting author royalty of digital assets," *Arabian J. Sci. Eng.*, vol. 44, no. 4, pp. 3849–3866, Apr. 2019. [Online]. Available: https://link.springer.com/article/10.1007/s13369-018-03715-4#citeas, doi: 10.1007/s13369-018-03715-4.
[117] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.
[118] (2019). *Chasyr*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.chasyr.com
[119] A. Rossow. (2019). *Hailing Rides Down Crypto Lane: The Future of Ridesharing*. Accessed: Apr. 12, 2019. [Online]. Available: https://www.forbes.com/sites/andrewrossow/2018/07/18/hailing-rides-down-crypto-lane-the-future-of-ridesharing/

TEJASVI ALLADI received the B.E. degree from the Birla Institute of Technology and Science, Pilani, India, in 2010, and the M.S. degree from North Carolina State University, Raleigh, NC, USA, in 2015. He is currently pursuing the Ph.D. degree with the Birla Institute of Technology and Science, Pilani, India. He has around six years of industrial experience working on embedded systems in MNCs like Qualcomm and Samsung. His research interests include the Internet-of-Things (IoT) security, blockchain, and unmanned aerial vehicles (UAVs).

VINAY CHAMOLA received the B.E. degree in electrical and electronics engineering and master's degree in communication engineering from the Birla Institute of Technology and Science, Pilani, India, in 2010 and 2013, respectively, and the Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2016. In 2015, he was a Visiting Researcher with the Autonomous Networks Research Group, University of Southern California, Los Angeles, CA, USA. He is currently an Assistant Professor with the Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus. His research interests include solar-powered cellular networks, energy efficiency in cellular networks, the Internet of Things, and networking issues in cyber-physical systems.

REZA M. PARIZI (SM'19) received the B.Sc. and M.Sc. degrees in computer science, in 2005 and 2008, respectively, and the Ph.D. degree in software engineering, in 2012. He is currently the Director of the Decentralized Science Lab (dSL), College of Computing and Software Engineering, Kennesaw State University (KSU), Kennesaw, GA, USA. He is a consummate technologist and also a cybersecurity researcher with an entrepreneurial spirit. He is a member of the IEEE Blockchain Community and ACM. Prior to joining KSU, he was an Associate Professor with the New York Institute of Technology. His research interests include Research and Development in decentralized computing, blockchain systems, smart contracts, and emerging issues in the practice of secure software-run world applications.

KIM-KWANG RAYMOND CHOO (SM'15) received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is also a Fellow of the Australian Computer Society, and the Co-Chair of the IEEE Multimedia Communications Technical Committee's Digital Rights Management for Multimedia Interest Group. In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn). In 2015, he and his team won the Digital Forensics Research Challenge organized by the Germany's University of Erlangen-Nuremberg. He is a recipient of the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the Outstanding Associate Editor of 2018 for the IEEE Access, the British Computer Society's 2019 Wilkes Award Runner-Up, the 2019 *EURASIP Journal on Wireless Communications and Networking* (JWCN) Best Paper Award, the Korea Information Processing Society's Journal of Information Processing Systems (JIPS) Survey Paper Award (Gold) 2019, the IEEE Blockchain 2019 Outstanding Paper Award, the International Conference on Information Security and Cryptology (Inscrypt 2019) Best Student Paper Award, the IEEE TrustCom 2018 Best Paper Award, the ESORICS 2015 Best Research Paper Award, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship, in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award, in 2008. His research has been funded by the National Science Foundation, NASA, CPS Energy, LGS Innovations, Texas National Security Network Excellence Fund, Australian Government National Drug Law Enforcement Research Fund, Australian Government Cooperative Research Centre for Data to Decision, auDA Foundation, Government of South Australia, BAE Systems stratsec, Australasian Institute of Judicial Administration Incorporated, and Australian Research Council.