Chapter 3
Fusion of Blockchain Technology with 5G: A Symmetric Beginning

Suneeta Satpathy, Satyasundara Mahapatra, and Anupam Singh

1 Introduction

Blockchain technology is becoming popularized as digital currency in the form of Bitcoin all over the world. It is termed as a distributed database for carrying out transactional operations online and has justified its efficiency and benefits in terms of its key attributes, federalization, secrecy, tenaciousness and controllable features for translating the conventional industrial system [1–3]. On the same hand, 5G is becoming more popularized in mobile technological industries because of its ability to interconnect heterogeneous devices with its broadband, remission services, machine-like communication [4] and enhanced qualitative throughput. 5G has revolutionized the communicational network system with a new set of attributes that have improved the criteria like network security, reliability and ability with smaller latency [5, 6]. Such a communicational network has brought a complete makeover in the industrial organizations in terms of high speed, virtualization among the business sectors and establishing the connection between Internet-operated devices, applications as well as objects. The 5G network [7] has also created many new opportunities for customers as well as business organizers and industries by providing a facility to interconnect communicating devices that can control and connect all spheres of human lifestyle and services. There are several

S. Satpathy (✉)
College of Engineering Bhubaneswar, Bhubaneswar, Odisha, India
e-mail: suneeta@koustuvgroup.ac.in

S. Mahapatra
Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India
e-mail: satyasundara@psit.ac.in

A. Singh
University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
e-mail: anupam.singh@ddn.upes.ac.in

S. Tanwar (ed.), *Blockchain for 5G-Enabled IoT*,
https://doi.org/10.1007/978-3-030-67490-8_3

technical supports like software-defined networking (SDN), cloud computing, network functions virtualization (NFV), edge computing, network slicing and D2D communication that have strengthened the power of 5G network [8, 9]. So 5G network empowered mobile communicating devices are required to be assisted with online digital payment platforms which in turn can be provided by blockchain technology. Again along with the power of 5G communicating technology, many challenges need to be handled like trustworthiness of network, permanency of data, isolation and secrecy of data [10]. On the other hand, Blockchain being popularized in the digital era can efficiently handle the challenges that have been put forth by 5G networks. So blockchain technology with an intent to make the most of cryptocurrency applications [11] can be associated with a 5G network to more securely carry out digital online transactions to prove the positive potential of it. In the recent smartphone being manufactured, the concept of hardware wallets that makes use of hardware cryptocurrency and empowers the blockchain transaction to be conducted safely over 5G communication networks taking the real benefit of 5G networks has been developed. So the features of blockchain can be thought of as a supporting hand for all sorts of future network technologies [12].

So the major focus of this chapter is to lay out the technological backdrop for 5G communications as well as to review how blockchain technology can tune-up with it as a fused component with an objective of considering it as one of the driving factors for the development of next-generation 6G network services. Further, the chapter flows with the description of the concepts of blockchain and its smart-supportive features for the 5G communicational network in Sect. 2 followed by Sect. 3 that briefs the potential features of 5G communication networks. Section 4 narrates the fusion of blockchain technology with 5G-enabled smart automated applications. Then several challenges and issues that are assisted by the technological revolution [13, 14] are addressed in Sect. 5 to outline the future research direction followed by conclusions in Sect. 6.

2 Blockchain and Its Related Concepts

Blockchain technology has been adopted in various market segments because of its potentiality as well as several benefits. Such distributed technology has been adopted in various applications starting from cryptocurrency, IoT and finance-related transactions to various social and risk-oriented tasks and thus is expected to carry out day-to-day activities [15]. Initially, this technology has been used in terms of digital money named Bitcoin which in turn is described as a protocol in the digital communication network. In a better way, blockchain can be thought of as a decentralized composition of digital transactions which is not under the control of individual or company. Again, the technology is named so as because old blocks are not altered or tampered by anyone and new blocks get linked with the existing blocks resulting in a formation of a chain. Blockchain has a stringent set of rules and structure that makes sure that data can only be inserted into the database without doing any alteration to the existing ones which in turn is a long and complicated process of back tracing the entire history of transactional data. Moreover, we can say that blockchain is a group of shared and linked transactional emergent data that are stored digitally in the form of a ledger. The security aspects in blockchain are maintained by cryptographic techniques, digital authenticating signature and distribution agreement that allow freeness of mind among the people to accumulate, swap over and observe the information in a digital platform securely. Blockchain, with a growing transactional data characterized by date and time stamp, is decentralized and dispersed around the communicational networks with the security rules enforced that all the interaction done through it would be visible to all the users, but require authentication verification before augmenting any information into it. On the same hand, users would be able to update the existing data block to which they have been granted access, and the same would be reflected in the entire network. Prior application of blockchain was named through Bitcoin which is regarded as a digital coin to make business. The successful application of Bitcoin has enabled the utilization of blockchain technology in different fields like healthcare facility, IoT, finance-related services, official document management and tracking, insurance-related services, supply chain management, tourism services as well as handling cyberthreats and criminals.

So blockchain technology can be summarized as a mixture of different disciplinary concepts like mathematics, cryptography, networking, economic modelling and distributed consensus algorithms [16] that have made the inclusion of various features such as decentralized, maintaining secrecy and trust, self-sufficient and automated and visible, secure and verifiable as briefed below to make the digital transactions protected and tamper-proof.

Decentralized Blockchain technology implements distributive transactional operations where data can be stocked and updated.

Maintaining secrecy and trust Blockchain technology maintains the user's trust by allowing anonymous data transfer. It allows to send only their blockchain address and not the original identity during transactional operations.

Self-sufficient and automated The blockchain users make a set of rules on the basis of which blockchain technology works. It is not ruled by any single central authorized person; rather, it has one of the components called smart contract which is a computer program with auto executed actions when the contract conditions are fulfilled.

Visible, secure and verifiable Blockchain technology works on the principle of decentralization which means data is not stored in a single place; rather, it is scattered all over. Again transactional data is visible to all the users. Even when any updation occurs, it can be visualized by all, justifying the transparency for each node. Further, the transactional data remains restricted for any change by the users unless otherwise authorized for it.

Blockchain data storage is distributive in nature and thus maintains the security by not being easily accessible to the hackers for taking any illicit attempts. The security is also enforced by encrypting the transactional data and linking it to the existing blocks only when every node user gives their nod of the validated updations if made to it. So blockchain technology has maintained a trust and security factor for various business organizations where data is the most critical asset and possible to be tampered by the intruders.

2.1 *Blockchain Architecture*

The blockchain can be seen as consisting of blocks which are sequentially connected representing a complete transaction record. The blocks are connected with each other through a hash reference of the preceding block known as parent block. The first block does not have a parent, hence known as the genesis block, and every block has the following information:

1. Header
2. Body

The header part of the block contains information like version describing various validation protocols to be adopted, the 256 bit hash value of the parent block, the hash value of the Merkle tree root block indicating hash values of all transactions, date and time stamp of every transaction present in the block, a 4 byte nonce starting with zero that amplifies for each hash value calculation and n-bits representing the present hashing value in a compacted manner. The body part of the block contains transaction counters [17]. The capacity of the block and the size of the transaction decide the total number of transactions that can be present in the block. Figure 3.1 shows the functioning of the blockchain technology.

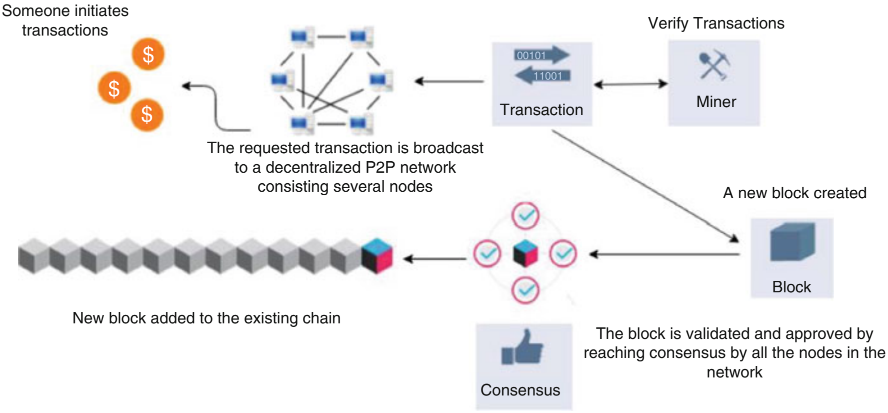
Someone initiates transactions
$
$
$
The requested transaction is broadcast to a decentralized P2P network consisting several nodes
00101
11001
Transaction
Verify Transactions
Miner
A new block created
Block
New block added to the existing chain
The block is validated and approved by reaching consensus by all the nodes in the network
Consensus

Fig. 3.1 Functional diagram of Blockchain network [1]

The legitimacy of the blockchain technology is maintained with the help of asymmetric cryptography that enables digitally authenticated signatures. The legitimacy is also maintained through two phases named as signing with a private key phase and verifying it with the public key phase. Each blockchain user owns a private and public key. The user uses the private key to put a sign on a transaction that is to be distributed around the network. All others who can see the transaction in the network can access it by using their public key.

Blockchain technology is also augmented with a consensus algorithm [18] that makes it more secure and is distributed across the network. The algorithmic function makes sure that the transactional block, whether the updated one or the new block, has been placed into the existing chain properly or not. It also ensures that the block that is added is the one visible to all in the network and is protected from various cyberthreats.

The algorithm works on two principles:

1. Proof of work
2. Proof of stake

The proof of work is able to generate valid proof in a randomized process which is also known as the mining process. In this, each block is associated with a random value designated as the nonce in the block header. The proof of work has to produce a value that can compare the nonce hash value to be smaller than a value already set up as a targeted value. The comparison with the targeted value is done in terms of the time required for generating it. Such a process of the generation that would make a complete coverage of all sorts of data in the block by proof of work decides the acceptance of the block by the users of the network. As an addition to the proof of work, the security protection from different types of cyberthreats is given by the proof of stake.

2.2 Catalogue of Blockchain Architectures

The flavours of blockchain architectures differ in their design layout and architectural description. The architectures can be discussed under the following names:

1. Public blockchain
2. Private blockchain
3. Consortium blockchain

1. Public blockchain

This type of blockchain architecture (Fig. 3.2) defends itself to be completely transparent as every user in the network is provided with the total history of blockchain and each of them is allowed to check and verify the transaction. The user connected to the network with a computer and Internet connection is treated as a node which is allowed to take part and obtain the consensus. The main advantage of such architecture lies in hiding the user credentials. A peer-to-peer transaction is

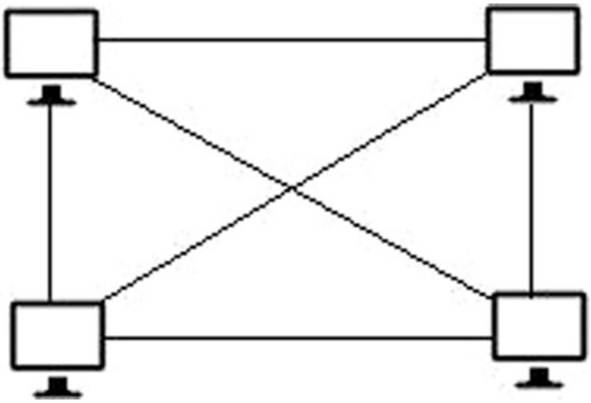

Fig. 3.2 Public blockchain [19]

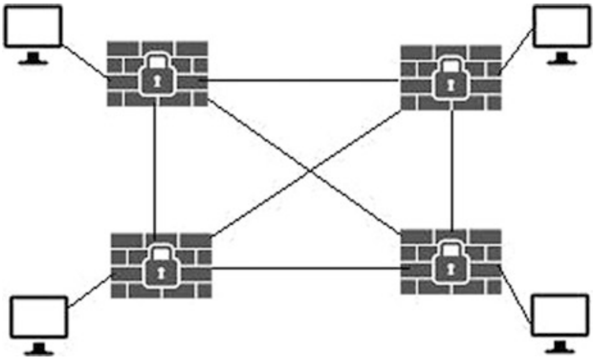

Fig. 3.3 Private blockchain [19]

built up to emphasize decentralization. Such architecture also makes sure that every transaction is linked with blockchain prior to its updation in the system and thus gets synced with each and every node in the network of blockchain.

2. Private blockchain

In comparison to the public blockchain architecture, private blockchain as shown in Fig. 3.3 has restricted settings to access the data in the network. The participation restrictions are applied on the nodes, i.e. only authorized nodes are allowed to participate. The transaction can only be validated and verified by authorized nodes being initiated by a company or organization. Such a feature in the private blockchain architecture enhances the verification and validation process effectiveness. In comparison to the public blockchain, private blockchain keeps the users' information more private by sanctioning the access privileges for them. Such architecture is more inclined towards conventional modelling and e-governance. The private blockchain is more adopted by the private and government sectors because of the security provided by the central authority as well as for its enhanced efficiency and faster transactions.

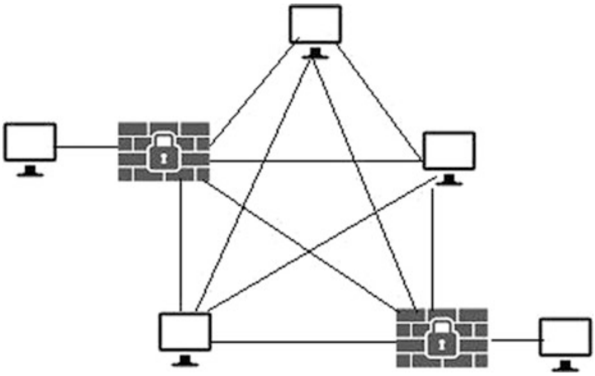

Fig. 3.4 Consortium blockchain [19]

3. Consortium blockchain

This type of blockchain architecture is a mixture of public and private blockchain architectures as shown in Fig. 3.4. That means such architecture makes the blockchain free to the public with a restriction that all the users won't be able to avail the total data. Protocols are defined for access privileges and validation process. In comparison to private blockchain consortium, architecture is partially decentralized. From the total number of nodes, few nodes are treated as trusted nodes that have the responsibility of controlling the consensus process. These nodes also decide the addition of a block to the chain once the consensus is obtained from the validation process. Such architecture is more preferred by the corporate business house in comparison to private blockchain architecture because of its partial decentralization.

3 5G and Its Features

The network communication technology has undergone a transition from the first generation to the fourth generation. The exponential increase in network traffic globally has prompted the development of even more trustworthy, speeder and efficient communication technology named as 5G networks that can fulfil all the limitations and gaps of existing mobile networks [20]. 5G communication technology is also known as global communication technology as it is consumed in various application areas across the globe. It is adopted because of its specific features like broadband connection, low-latency reliability as well as machine-to-machine communication. The adaptation of 5G technology has made a paradigm shift in different industrial business applications. Also the interconnection of the devices creates an ample amount of opportunities for business collaboration. So, 5G communication has made possible to connect all pieces of human life to the network to avail the promising user-oriented services like smart healthcare systems, vehicular networks [21, 22], smart grid and IoT [23, 24] by enabling different talented technologies like cloud computing, SDN, D2D services, network slicing and virtualization features as briefed below.

Cloud computing: The main objective of cloud computing technology is to manage the storage space and resources, thus achieving the challenges and demands of the 5G network. Various 5G network services starting from mobile network management to remote sensor-based services are well handled by virtual computing capability of cloud computing. In addition to the well-powered features of cloud technology, edge computing has also added extra power to 5G networks by providing storage and computing platform with a close relation to low value for transmission [25].

Software-defined networking (SDN): With this feature, it is possible to accomplish different network functions and services with software rather than using hardware. Such adaptability is also enhanced with the flexibility of a 5G network [26] by providing a separation between the control plane and the data plane.

Network functions virtualization (NFV): The main objective of NFV is to bring transformation in the delivery of network services. In addition to the feature of SDN that allows the services to run on the software, NFV encourages the services to run in standardized hardware platforms rather than the exclusive hardware made for them. So, with the features and functionalities of NFV, 5G network services would be enhanced in terms of efficiency, speed and faster services leading to better revenue generation and at the same time simplification of network functionalities.

Network slicing: Due to the versatility nature of the 5G network, it can be used by different applications. Based on the application requirement, there will be a demand for different types of networks leading to network slicing. Network virtualization as well as SDN feature can configure a variety of networks and fulfil the demands of user applications. Thus, it will allow different types of software to be run on the same hardware platform and fulfil different users' demand by providing low latency level for one and other types of the level depending on network performances for other users so that every user gets a taste of a slice of the network.

Device-to-device (D2D) communication: Such a feature allows communication between the IoT devices easily in comparison to conventional signal communication and transmission. Such type of communication makes data transfer between the mobile devices placed in short distance range at a high speed as well as guarantees the latency value at a lower range. It also empowers the 5G communication with flexibility in traffic offloading and enhances efficiency as well as reduces the energy that is supposed to be lost in lengthy data transmission.

Millimetre-wave (mmWave) communication: This communication technology augments novel facilities to 5G communication networks with demanded mobile data dynamically. Such feature also adds on new benefits to 5G networks like high bandwidth with the qualitative transmission, reduced beam, enhanced data accessing ability by ignoring the mobile network traffic, huge number of connected devices and machines with a variety of use cases.

So all these technologies are the augmented features in the 5G network to fulfil the diversified demands of the user applications along with the potential design of the network as summarized below.

3.1 Design Concepts of 5G Network

5G communication network is popular because of its properties as being flexible, scalable and configurable. Such beneficial features are obtained through a variety of software that runs on the hardware platform as per user demand and network virtualization as well as network slicing. Network slicing frees the user from the control panels and introduces dynamic network applications and services leading to ubiquitous platform and infrastructure. The main aim of 5G network is to transform all conventional manual services into automated qualitative services with high data transmission rates. On the same hand, it also aims to overcome the limitations of 4G networks. SDN feature of the 5G network is responsible for the simplification of operations and services by separating the control panel from the data panel. The centrally placed control has the responsibility of controlling the network resources with the help of API that is programmed. Also, network functions virtualization is meant for providing flexibility in carrying out network functions by making an impression of the virtual detachment of hardware platforms from various software-oriented services which results into virtualized gateways, firewalls as well as a network that is flexible enough to fulfil the demands of user applications. In addition to that, cloud computing platform solves the limitation of data storage to keep at par with the growing network traffic created due to the connection of IoT devices [27]. So the main focus of the 5G network is to render novel application-based services as well as amplified mobile network services with low latency value, the flexibility that could improve the quality in comparison to prior generation's network like 3G/4G. But all the benefits of the 5G network should be supported with well-defined security mechanisms which take the form of challenges being faced by the network and thus highlighted in the subsequent section.

4 Challenges Faced by 5G Network and Motivational Gains for Fusing Blockchain Technology with 5G

Any communicational network has to be assisted with authentication mechanisms. It plays a vital role in maintaining the security of the user applications, the identity as well as the underlying network. The authentication technique in the 5G network is handled by a server which takes lots of time even for preliminary authentication. As 5G network gives the assurance of zero latency, maintaining authentication for devices in the network and UEs, sustaining data confidentiality and data integrity, making the network available and having smaller computational complexity value and low cost for communication would be very crucial tasks. Further, it would require enhanced security mechanisms to make it more secure and beneficial. Though there exist security mechanisms for 5G networks to handle data transfer and connections, they are not adequate. So there is a need to have more protocols that can enforce security restrictions, awareness, storage, data transmission and user-demanded software that can form a threat-free valid network. Blockchain technology has the potentiality to handle the challenges put forth in the 5G network. So the integration of both technologies can show promising opportunities for the user to avail the benefits from both [28–30].

The 5G technology follows a centralized architecture which results in dreadful conditions for both network and computing performances. For example, the cloud computing or edge computing feature of 5G communications adopts the Amazon cloud server which is centralized and can have severe security problems. In addition to that, cloud services are mainly popular in fulfilling services as per user demand or choice, but the same cannot be achieved if there is a failure at any single point. IoT-enabled services with multiple user demands are also not possible for a centralized system, if there would be a cyber malware attack. Similarly, NFV provides a virtual environment with multiple cloud services that give the benefit of function chaining in the 5G network, but it can suffer from leakage of data by a few cloud objects. Since the virtual environment is a sharable resource, there is a high probability of threats that can hamper the lucidity and liability of cloud service providers. On the same note, virtualized servers for NFV run through virtual machines that are offering a variety of operating system environment with the help of orchestration protocol, leading to a security concern for the transmission that is established between a VM manager and an orchestrator. The mobile bandwidth data-oriented services like video streaming and a large volume of data processing may require an efficient resource management strategy in 5G communication so that resource usage can be consistent with the avoidance of scarce issues and degradation in performance. Such things can only be achieved by sharing through centralization but that would create the possibility of more cyber-attacks and decreased quality of service, or an authorized person would be devoid of resources. The IoT-enabled services availed through the 5G network making everything smart will also face complex security concerns as a large amount of diversified data would be generated leading to misidentification of malicious objects causing threats [31]. But there is an absolute requirement by the users to get efficient sharing of data along with proper network management assisted with high-throughput and elevated security features. So the limitations and security constraints faced in the 5G communicational network can be overcome to some extent by the fusion of blockchain technology with 5G network services [32].

4.1 Promoting Fusion of Blockchain with 5G

As we know, blockchain technology is considered to be a distributed public ledger associated with properties like being decentralized, maintaining secrecy and trust, being self-sufficient and automated and being visible, secure and verifiable and, hence, has the capability of handling the challenges faced by 5G technology concerning security and management of the network [33]. Moreover, the benefits that blockchain technology can augment to 5G networks can be grouped under enhanced system performance, enforcement of better security features and well-handled and managed network services discussed as follows.

1. Enhanced system performance

The main objective of the 5G network is to maintain qualitative services with low latency. Keeping this into account, blockchain technology is blessed with decentralized nodes with smart contracts that can handle all resource requests intelligently without availing centralized authorization. The integration of blockchain with 5G communication [34] can surely enhance the system performance with better storage and application service administration along with lower value for latency in comparison to conventional SQL-based database platforms [35]. The integration of the technology can provide a flexible data transmission model with a reduced cost supposed to be incurred against management by making direct contact between users and 5G network services. Such a model can still be considered as secure since blockchain makes D2D communication among the users and avail the computational power from its users to manage the network rather than availing from the central authority [36]. Thus, it can achieve lower latency value for communication, for transactional work as well for data accessibility leading to amplified system performance. In addition to that, even if there is a failure at any point due to malicious attacks, the network can still remain useful by the consensus on the publicly distributed ledger.

2. Enforcement of better security features

Blockchain guarantees the enforcement of additional security features such as being decentralized, maintaining secrecy, trust, being self-sufficient and automated and being visible, secure and verifiable. Though cloud computing has a centralized cloud server, blockchain-oriented cloud services facilitate decentralization to enforce an unbiased agreement with the consensus of blockchain technology. It further ignores the failure that can happen at any node and wins the trust of the system as well as the user. Since blockchain technology employs peer-to-peer communication that in turn transfers each device in the network, as a blockchain node, it can have a copy of the ledger to keep an eye on the transactional data to make everything transparent and dependable. In comparison to traditional DBMS, the smart contract feature of blockchain technology makes use of the computing power of authenticated nodes to allow decentralized transaction validation of each node's access [37]. Such a smart contract feature can empower the 5G network with all its services not to be tampered or modified. Further, the immutability characteristics provide security and protection against various cyber-attacks. Protocols for user access along with logic codes in blockchain technology are also capable of providing enhanced authentication mechanisms with contracts that can automate the authorization process for its users without revealing their private identity information as well as discard the intruding ones for 5G networks. The data also remain highly protected in the blockchain platform as those are authenticated by hash values and then get added to the blocks. Along with data protection, the private data when shared in an untrusted communication medium remains in the total control of the blockchain technology that even prevents the users of the node to trace their own data [38].

3. Well-handled and managed network services

Due to the decentralization, blockchain promises the simplification of 5G network services. Practically, the worries of employing a central controlling authority to operate the mobile network services are eliminated with the augmentation of blockchain principles. Both the mobile network service providers and users can avail the 5G services like trading in terms of resources, payments, responses and data access on the distributed decentralized public ledger. Thus, the adoption of blockchain technology can significantly simplify the network and its associated costs. It can enable the sharing of services for both data and spectrum for the 5G network by providing the rights to the nodes for network maintenance and management. The node participants can also be empowered to explore the internal network resources to facilitate better user experience and network services on the mobile platform by fusing blockchain technology with 5G network services [39].

So with the innovative characteristic features of blockchain technology fused with the 5G network services, the challenges in terms of security, privacy, confidentiality and consistency can be definitely get rid of and can become a more powerful.

4.2 The Fusion of Blockchain with 5G Network Leading to Smart Applications and Automations

The potential of 5G network services integrated with blockchain technology has made possible IoT-enabled devices to get connected and set up an environment to render a variety of automated services like auto-sensing, communicating and processing without any human operator across the domain. The features of 5G technology like SDN, NFV, cloud or edge computing integrated with enhanced and inbuilt security mechanisms and with distributed decentralized ledger technology enabled the progression of IoT services across the globe. Many IoT applications are availed by joining together blockchain and 5G network services to suffice the basic needs of human being like smart healthcare, home, city, vehicle, industry, education, grid, trading, etc. which are portrayed as follows.

1. Smart Healthcare

Healthcare services are the industries that cater to the needs of the people by providing medical services and medical insurance facility as well as smoothen the progress of medical facility delivery to patients at the time the need arises. The prospective features of 5G communication technology can modernize the existing healthcare systems to smart medical facilities with reliable trustworthy services [40]. The blockchain technology highlighted with its relevant features like decentralized distributed ledger, improved secure and private platform, qualitative service and simplified network management with low cost can be fused with the most promising 5G networks to provide better assistance to increase performances in healthcare sectors [41]. Various features of blockchain technology like on-demand software can do various network functions through virtualization and enhanced storage through cloud computing to promote the delivery of services at a faster rate so that a survey can be made on patient's health conditions at a very primary stage. Since blockchain promotes peer-to-peer communication, its fusion with 5G network will result in a healthcare database that can encourage the storage of validated transactional data as well as all patient communications in the distributed public ledger. Since the data would be stored in a secured publicly distributed ledger, all the healthcare workers can exchange and share data during the treatment process. In addition, home-based portable medical services with diversified analysis can also be availed through SDN as well as cloud-based modelling. Such portable services are highly secure to maintain communication between patients and doctors privately. The smart contract feature enables accessing privileges to ensure that healthcare data remains secure from malicious threats. The D2D communication enables feature extraction from patient's private data on a high scale which in turn is tagged with hash values and securely placed in the public decentralized ledger to get rid of data seeping out and tampering issues. Blockchain technology is also proudly implemented in a telemedicine service in mobile edge computing that allows the users to use their mobile network and access the services. The protocols defined through consensus also ensure that the patient is taken care of and is the top priority and optimization is achieved for resource allocation and security is maintained for their sensitive information. Also other applications for disease detection are able to take a capture of all medical test data and store it in an offline medium under the supervision of blockchain technology that gives the permission to the patients to access their own medical clinical test-related data authenticated with cryptographic hash values to maintain integrity checks and transparency of the process. Various cloud-based healthcare solutions also adopt the blockchain technology for enhancing the security of electronic health-related data. IoT-enabled healthcare devices can maintain the communication between cloud-based servers with the help of a protocol meant for communication defined under blockchain technology. The mobile app-based cloud blockchain medium is also used to record electronic health data accessible between patients and doctors. In such type of architecture, data is handled by the smart contract technology. So when blockchain is integrated to a cloud computing platform to enable data sharing, lower latency value is achieved with efficient data management and security in contrast to a centralized cloud-based architecture.

2. Smart City

The potential features of 5G technology have made a revolutionary change in transforming the conventional systems providing services into a completely digitalized and cost-effective one. One of such revolution includes smart city formation which may consist of many IoT devices scattered all throughout and connected through different networks with powerful cloud computing servers for carrying out processing tasks. Since the security issues stay with 5G network connecting IoT smart devices, blockchain technology can be useful in providing the same [42]. Such technology for a smart city application can segregate the city into a number of blocks being administered by a block administrator. It can comprise of IoT-required devices like sensors and cameras augmented with secured private blockchain database for sharing the information from IoT devices. Such a system employs fog computing mechanism to deal with data from mobile and IoT devices and machine learning techniques to carry out the data analysis and storage in secure blockchain ledgers. Blockchain technology is also adopted to make an interconnection between smart cities and IoT devices with utmost security. In smart cities as cameras and sensors would be present everywhere to capture an ample amount of data and to analyse those in case of a malicious attack, detecting the object of threat would be a cumbersome task. Such challenges can be well handled by the concept of edge computing done in a distributive manner. Also secure blockchain can interconnect IoT devices, nodes and users to communicate with each other by setting up a decentralized secure platform. As blockchain technology is a distributed ledger with a central cloud-based server, it provides more benefits in comparison to centralized architecture. In a smart city, the transport providers and the travellers communicate through mobile in a platform known as Mobility-as-a-Service (MaaS) which is more prone to malicious attacks and data leakage. Such services can be enhanced if integrated with the blockchain platform to improve the security of the services offered through a mobile platform like smart contract that can enable secure and trustworthy payment forum [18]. The large amount of data generated by IoT devices in a smart city can be efficiently and securely handled by cloud-based servers assisted by blockchain technology to handle auditing issues leading to assemble a data auditing blockchain (DAB) that in turn uses Practical Byzantine Fault Tolerance (pBFT) protocol by consensus algorithm. In such type of systems, each cloud server is treated as a node in blockchain, and the respective happenings can be stored in ledgers that ultimately reduce the risk of malicious attacks and failure at any single node.

3. Smart Transportation

The development of 5G technology has made a significant impact from traditional transport facilities into intelligent transportation systems (ITS) called smart transportation with smart vehicles, thereby providing better services to people. Smart transportation is an end product of IoT-based communication with vehicles in transportation. But due to the centralized architectural system used in such types of services, there is a high risk of security threat in a vehicle-to-vehicle transmission. Blockchain technology with its all essential features of distributed ledger, decentralization, transparency and peer-to-peer communication can set up the security protocols for secure vehicle transportation [43]. The technology can help in building up peer-to-peer transmission between vehicles and roadside units as well as can set up decentralized storage to store all transactional data of electrical vehicles. Vehicle-to-grid (V2G) is a smart and new device used as mobile power storage for a more secure energy platform between the power supply and electronic vehicles. The power supply in the smart city gets connected to the public blockchain where the communicational data between the supplier and user are stored, and thus the payment orders as well as charging and discharging information are also circulated by the electronic vehicles. Since authentication plays an important role in smart vehicle systems, smart contract can be a good approach to authorize and confirm all sorts of transactions related to it [44] with the help of programs. The smart contract also enables authorization of vehicles that are registered without mentioning their full details, thereby reducing the risk of cyber-attacks. Even distributed SDN features of blockchain technology can be used to make a secure VANET [45] that can deal with heterogeneous traffic needs. The important requirement of VANET is to maintain security among EVs and V2G for power transmission and trading. So the need of the hour is to set up a good versatile trading model that can deal with different services related to vehicles. Such demand is fulfilled by blockchain technology by setting up a decentralized energy platform so that decentralized ledger is used for secure storage. Also smart contract is integrated with EV and V2G to form a combined trading platform for authorized low cost and efficient communication and authentication.

4. Smart Home
Modern human life has become smart enough because of the IoT-enabled connected devices like home appliances and smart watch, healthcare devices and other wearables. All smart home-based devices can be further enhanced with the features of blockchain technology. The research work also shows a smart power outlet system for a smart home which is further enhanced with auto-monitoring and controlling remotely with the application of blockchain technology [46]. Blockchain technology is also employed to maintain communication between smart electricity supply and smart home for energy trading. A smart home is also equipped with automatic locking of the door with the application of blockchain technology for authorization check, payment and event recording. The application of blockchain technology is also optimized to maintain security in a smart home case study. IoT-enabled device data is provided with an additional level of security with encryption which is narrated with the employment of consortium blockchain application.

5. Smart Industry
Industry 4.0 with IoT has brought the revolutionary transformation with cyber-physical systems like smart manufacturing, smart sensing, smart supply chain management, etc. These smart industrial applications can further be boosted with blockchain technology. For example, the research work by [8, 9] narrated the augmented blockchain technological applications in industrial IoT-enabled manufacturing, supply chain management, diagnostic operations, machine to machine transactional work as well as product certification, etc. The work also developed a smart contract-based prototype that can diagnose and sense the faulty part of the system and sends a report to the user about the necessity of part replacement in the machine. Smart contract technology of blockchain applications also provides the facility of buying electric power from an energy house [47, 48]. The technology is also successfully implemented in supply chain management for manufacturing and allocation of materials [49] and in credit-based trust systems.

6. Smart Agriculture
The application of IoT has also modernized the agricultural system with smart sensing of the area to be cultivated. IoT-enabled devices are able to monitor

temperature, humidity, insect and plant diseases that contribute greatly towards the prediction of crop cultivation and production dynamically. Blockchain technology has also made its role in a smart agricultural system so that there is an exchange of ideas and knowledge among the farms and government sectors like setting up irrigation canals. Further, blockchain applications have enhanced smart agriculture by adding transparency and backtracking of crops [50]. The research study also proves the application of blockchain with agricultural IoT for storing transactional data for the supply chain [51]. The sensitive and essential information regarding food safety like production, storage, processing and selling against its resources is also publicly exposed with an integrated application of blockchain technology with IoT-enabled smart agriculture. The backtracking of products used in agriculture in the supply chain is also made possible with the combined application of blockchain with RFID.

7. Smart Grid
Smart grid is a smart automated management of electricity through a network connection and IoT devices. IoT devices like sensors and metres can collect the data related to the power supply, consumption and load which can further be used for effective management of electricity resources. But such type of smart management of energy can suffer from some shortcomings like convincing the customers for reliable electricity metre reading, handling energy system complexity, etc. Such limitations can be handled by blockchain technology applications. The research is also done to make a replacement of the local grid by trans-active microgrids which is an application of blockchain for power supply transactions. In such an application, grid nodes are capable of maintaining the privacy of electricity trading individually [52]. The transparency of power consumption is also demonstrated with the help of smart contract for smart energy. Even the close monitoring and recording of consumption of energy is done with the application of blockchain technology. The power trading as well as its price has been optimized with the application of blockchain consortium. Smart grid application of blockchain technology is also used for reliable power trading. Even blockchain has been applied to prevent malicious threats and protect the sensitive data for smart energy applications.

8. Smart Trading and Supply Chain Management
The application of blockchain technology with a 5G network enabling the connection of IoT devices has also brought a revolutionary change to supply chain management [53] to support the effective recording of the product-related information when it is transferred from the manufacturer to the customer. The technological application also enables the monitoring of the quality of products and raw materials [48]. Smart contract features on blockchain technology can be used to create business collaborations which can then be used to carry out transactions in an automated manner without waiting for the traditional process of confirmation. The research work also shows the automated filing of taxes with smart contract feature of blockchain technology.

9. Smart Education
The educational domain has also undergone a paradigm shift from a paper-based world to a paperless environment with the development of smart devices like tablets, smartphones, computers and laptops. All such smart devices have revolutionized the way course context is designed, home assignments are uploaded and examination is conducted. All such smart devices can track learner's behavioural patterns as well as intelligence level automatically leading to smart education. The augmentation of blockchain technology into smart education will add on extra advantages of transparency in the learning process, examination grading and evaluation system as well as in the management of certificates so that the educational system becomes more fair, reliable and trustworthy [34].

5 Revealing Future Challenges for Fusion of 5G Network with Blockchain Technology

Though fusion of blockchain technology with the 5G network brings potential benefits, on the other hand, it suffers from several issues and challenges in terms of security from all perspectives and data privacy. The challenges are briefed as follows.

(a) Expandability with trustworthiness
The major goal of the 5G network is to achieve a low latency rate and, currently, for data and payload application to happen in less than 1 millisecond [54]. To achieve such a latency rate, there is requirement of tight protocols and configuration setup to carry out the transactions with high throughput. The public blockchain applications in terms of Ethereum and Bitcoin are only able to handle transactions up to a range of 10–14 per second, and private blockchain applications can handle 3000–20,000 transactions per second. So there is a need for further research in the future for its expansion and optimization starting from the architecture, increasing the size of each block as well as the smart contracts to meet the goal of achieving higher throughput. Along with such achievement of goals, trustworthiness plays a major factor that is achieved through decentralized distributed ledger with security. Such reliability is maintained for information like images and symbols, so it requires enhancement for different information options. Blockchain architecture itself enables trust and transparency factor, so more collaboration works are supposed to evolve with competition, ignoring intermediate competitors.

(b) Upgradation of smart contracts and resolution of vulnerability issues
Public blockchain applications are equipped with ten million smart contracts, and these smart contracts are to be used for 5G networks which enable interconnection of IoT devices. The smart contract of blockchain technology is vulnerable to cyber-attacks and needs to be securely coded for the 5G network [55, 56]. Moreover, the smart contract once coded is not further upgradable or modifiable in place of

any malicious attack by the hackers. So the smart contract code has to be further researched for upgradation and reporting of vulnerability issues.

(c) Data privacy and malicious threats
Privacy and security are the two faces of a single coin. It is an essential requirement of every individual, organization as well as government. It has to be maintained with 5G network communication too as it deals with customer's sensitive data. The integration of blockchain technology with a 5G network enables privacy with an issue that the data that gets stored in the blocks are not able to be erased because of its immutable property. Also, blockchain only identifies the users' address and never stores their private information. But Bitcoin applications are found to record the personal information of the user to make an exchange of the identity information among the users with the public and private key. Even the smart contract application and Ethereum are also indulged in the exchange of identity information which is a major issue and needs to be dealt with. The cryptography security maintained through the public key and the private key is supposed to be prone to a man in the middle attack [57] where a third person can come in the middle carrying an un-genuine public key and decrypt the sensitive information. Similarly, blockchain technology can be threatened with DDoS attacks which can smash away any platform or network and its resources [58]. On the same note, Bitcoin technology is prone to selfish mining threat that threatens the genuineness of the technology which requires urgent attention.

(d) The cost associated with transaction and cloud server setup
There are costs involved to set up the nodes of blockchain, maintain the blockchain consortium and set up the cloud server. The cost investments would be more if the number is not optimized [59]. In applications like Ethereum, costs are calculated in terms of gas units for each transaction, and gas units are the energy consumption units for smart contracts. So the costs are also calculated concerning the code that is being executed for each transaction. These fees would be required more in order to execute complex coding, if involved in the transaction, so it needs to be taken care of.

6 Conclusion

This chapter has presented the outline description for blockchain technology and its associated potential features as well as 5G network basics to mention the need for fusion of both the technologies. The study also highlighted the smart application areas of the 5G network with interconnected smart devices that have become more effective and secure with the integration of blockchain technology with it. Though there are enough beneficiary gains that are obtained through the fusion of both technologies, the present study also put forth various challenges that come into existence and needed to be sorted out with further research to make the technology accomplish all its desired and directed targets.

References

1. A.A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019). https://doi.org/10.1109/ACCESS.2019.2936094
2. F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, in *Telematics and Informatics* (Elsevier Ltd., 2019). https://doi.org/10.1016/j.tele.2018.11.006
3. K. Christidis, M. Devetsik, Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
4. A. Gupta, R.K. Jha, A survey of 5G network: Architecture and emerging technologies. IEEE Access **3**, 1206–1232 (2015)
5. I. Jovovi'c, S. Husnjak, I. Forenbacher, S. Maˇcek, Innovative application of 5G and blockchain technology in industry 4.0. EAI Endorsed Trans. Ind. Netw. Intell. Syst. **6**(18), e4 (2019)
6. M. Agiwal, A. Roy, N. Saxena, Next generation 5G wireless networks: A comprehensive survey. IEEE Commun. Surv. Tutor. **18**(3), 1617–1655 (2016)
7. N. Panwar, S. Sharma, A.K. Singh, A survey on 5G : The next generation of mobile communication. Phys. Commun. **18**, 64–84 (2016)
8. R. Yang, F.R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Commun. Surv. Tutor. **21**(2), 1508–1532 (2019)
9. D. Sukheja, L. Indira, P. Sharma, S. Chirgaiya, Blockchain technology: A comprehensive survey. J. Adv. Res. Dynam. Control Syst. **11**, 1187–1203 (2019). https://doi.org/10.5373/JARDCS/V11/20192690
10. M. Liyanage, I. Ahmad, A.B. Abro, A. Gurtov, M. Ylianttila, *A Comprehensive Guide to 5G Security* (John Wiley & Sons, Hoboken, 2018)
11. F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **18**(3), 2084–2123 (2016)
12. I. Bhudiraja, S. Tyagi, S. Tanwar, N. Kumar, J.J.P.C. Rodrigues, Tactile internet for smart communities in 5G: An insight for NOMA-based solutions. IEEE Trans. Ind. Inf. **15**(5), 3104–3112 (2019)
13. S. Rouhani, R. Deters, Security, performance, and applications of smart contracts: A systematic survey. IEEE Access **7**, 50759–50779 (2019)
14. S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P.K. Singh, W.C. Hong, Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. IEEE Access **8**, 474–488 (2020)
15. X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things. Comput. Commun. **136**, 10–29 (2019)
16. W. Wang, D.T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D.I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access **7**, 22328–22370 (2019)
17. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564, (2017)
18. P. Mehta, R. Gupta, S. Tanwar, Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. Comput. Commun. **151**, 518–538 (2020)
19. S. Kumar, A. Kumar, V. Verma, A survey paper on blockchain technology, challenges and opportunities. Int. J. Comput. Trends Technol. (IJCTT) **67**(4), 16 (2019). ISSN: 2231-2803, http://www.ijcttjournal.org
20. J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, A.C.K. Soong, J.C. Zhang, What will 5G be? IEEE J. Sel. Areas Commun. **32**(6), 1065–1082 (2014)
21. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Tactile Internet and its applications in 5G Era: A comprehensive review. Int. J. Commun. Syst. **32**(14), 1–49 (2019)

22. T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: A data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2018)
23. A. Singh, S. Mahapatra, Network-based applications of multimedia big data computing in IoT environment, in *Multimedia Big Data Computing for IoT Applications*, Intelligent Systems Reference Library 163, https://doi.org/10.1007/978-981-13-8759-3_17, (2020)
24. Internet of Things (IoT). [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/
25. J.M. Khurpade, D. Rao, P.D. Sanghavi, A survey on IOT and 5G network, in *International Conference on Smart City and Emerging Technology (ICSCET)*, pp. 1–3, (2018)
26. S. Zhang, X. Xu, Y. Wu et al., 5G: Towards energy-efficient, low-latency and high-reliable communications networks, in *Proceedings of the IEEE ICCS*, pp. 197–201, (2014)
27. I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech. Syst. Signal Process. **135**, 106382 (2020)
28. W. Al-Saqaf, N. Seidler, Blockchain technology for social impact: Opportunities and challenges ahead. J. Cyber Policy **2**(3), 338–354 (2017) The Road to the Next Wave of Tech: 5G +Blockchain. [Online]. Available: https://www.asiablockchainreview.com/the-road to-the-nextwave-of-tech-5G blockchain/
29. W.H. Chin, Z. Fan, R. Haines, Emerging technologies and research challenges for 5G wireless networks. IEEE Wirel. Commun. **21**(2), 106–112 (2014)
30. M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: A decentralized blockchain-based authentication system for IoT. Comput. Secur. **78**, 126–142 (2018)
31. J. Liu, Z. Liu, A survey on security verification of blockchain smart contracts. IEEE Access **7**, 77894–77904 (2019). https://doi.org/10.1109/ACCESS.2019.2921624
32. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2), 1676–1717 (2018)
33. M. Chaudhry, Joint IEEE spectrum and comsoc talk, test and measurement virtualization and blockchain: Enablers for 5G networks, Nov 13, (2018)
34. Y. Yu, Y. Li, J. Tian, J. Liu, Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wirel. Commun. **25**(6), 12–18 (2018)
35. J. Wan et al., A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans. Ind. Inf. **15**(6), 3652–3660 (2019)
36. T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey. IEEE Commun. Surv. Tutor. **21**(1), 858–880 (2018)
37. R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, S.W. Kim, Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. IEEE Access **8**, 24746–24772 (2020)
38. Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Netw. **33**(3), 10–17 (2019)
39. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, B. Sadoun, HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0, in *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2019)*, Beijing, China, August 28–31, pp. 6–10, (2019)
40. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Tactile-Internet-based Telesurgery System for Healthcare 4.0: An architecture, research challenges, and future directions. IEEE Netw. **33**(6), 22–29 (2019)
41. J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun. Surv. Tutor. **21**(3), 2794–2830 (2019)
42. S. Talari et al., A review of smart cities based on the internet of things concept. Energies **10**(4), 421 (2017)

43. T. Jiang, H. Fang, H. Wang, Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. IEEE Internet Things J. **6**(3), 4640–4649 (2018)
44. J. Vora, S. Tyagi, N. Kumar, M.S. Obaidat, A systematic review on security issues in VANET. Secur. Priv. J. Wiley **1**(5), 1–27 (2018)
45. A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, pp. 618–623, (2017)
46. J. Al-Jaroodi, N. Mohamed, Blockchain in industries: A survey. IEEE Access **7**, 36500–36515 (2019)
47. K. Rabah, Overview of blockchain as the engine of the 4th industrial revolution. Mara Res. J. Bus. Manag. (ISSN: 2519–1381) **1**(1), 125–135 (2017)
48. M. Tahir, M.H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, K.I. Ahmed, A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. IEEE Access **8**, 115876–115904 (2020). https://doi.org/10.1109/ACCESS.2020.3003020
49. A. Litke, D. Anagnostopoulos, T. Varvarigou, Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment. Logistics **3**(1), 5 (2019)
50. M. Kouhizadeh, J. Sarkis, Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability **10**(10), 3652 (2018)
51. H. Malik, A. Manzoor, M. Ylianttila, M. Liyanage, Performance analysis of blockchain based smart grids with Ethereum and Hyperledger implementations, in *IEEE International Conference on Advanced Networks and Telecommunications Systems 2019*. IEEE, pp. 1–5, (2019)
52. S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. **57**(7), 2117–2135 (2019)
53. M. Petersen, N. Hackius, B. von See, Mapping the Sea of opportunities: Blockchain in supply chain and logistics. it-Inf. Technol. **60**(5–6), 263–271 (2018)
54. B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, B. Stiller, A blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts, in *IFIP International Conference on Autonomous Infrastructure, Management and Security*, (Springer, Cham, 2017), pp. 16–29
55. K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 130 (2018)
56. L. Zhou, L. Wang, Y. Sun, P. Lv, Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation. IEEE Access **6**, 43472–43488 (2018)
57. M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (2018)
58. Market Pulse Report, Internet of Things (IoT). URL: https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf. Accessed 30 Nov 2019
59. P. Daugherty, B. Berthon, *Winning with the Industrial Internet of Things: How to Accelerate the Journey to Productivity and Growth* (Accenture, Dubl'ın, 2015)