Chapter 11

Blockchain technology for next-generation society: current trends and future opportunities for smart era

Meghna Manoj Nair and Amit Kumar Tyagi AQ1

Abstract

Blockchain, a relatively novel technology, is often termed as the internet of value. AQ2 Even though there are predictions that indicate that the future of blockchain is likely to be perilous, it has contributed remarkably and has already brought about revolutionary changes in terms of transactions and digital currencies. This paper is a survey and analysis of one of the fast-evolving technologies called Blockchain. It covers all essential information required for a beginner to venture into this complicated field while also covering necessary concepts that can be useful for experts; the first provides a general introduction and discusses the disruptive changes initiated by blockchain, the second discusses the unique value of blockchain and its general characteristics, the third presents an overview of industries with the greatest potential for disruptive changes, the fourth describes the four major blockchain applications with the highest prospective advantages, and the fifth part of the paper ends with a discussion on the most notable subset of innovative blockchain applications—Smart Contracts, Decentralized Autonomous Organizations (DAOs) and super safe networks—and their future implications. There is also a concluding section, which summarizes the paper, describes the future of blockchain, and mentions the challenges to be overcome. AQ3

11.1 Introduction to blockchain

Blockchain, as the word suggests, is a distributed ledger (refer Figure 11.1) storage technique wherein each block (except for the first block) has a pointer that points to the immediately previous block through a reference mechanism which focuses on the hash values. The very first block in the chain is called the genesis block and it ideally does not have any parent block. The data is stored in each of the block and every block has certain information which includes the block version, the hash value of its parent block, timestamp which records the

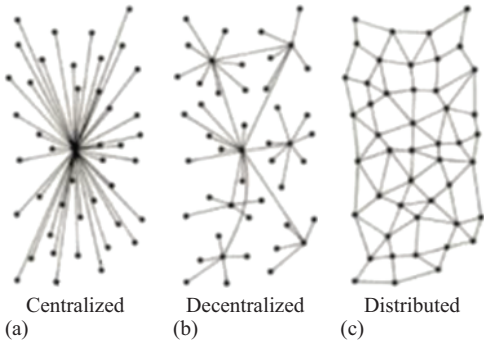

Figure 11.1 Structures in general

input entries into the block, nonce (number used only once) value, the number of transactions recorded in the block and the Merkle root pointer [1]. The recent surge in the use of blockchain technology has been in the field of cryptocurrency systems such as bitcoins because of its security features and decentralized nature of transactions. The main highlight of blockchain is its guarantee of reliable services and safekeeping of data which ultimately generates trust and loyalty by eliminating the requirement of a third-party mediator. One of the major strategies followed is that a given transaction can be successfully recorded within a block only when the involved miners adopt the Proof of Work (PoF) technique so as to acquire bitcoins in the form of rewards. The incentive-based system works by ensuring that the miner who stimulates and broadcasts the block first is the one who will be rewarded. It is also important to note that work done by the miners of finding suitable hash values for the block is excessively time consuming and difficult which is made in such a manner so that a maximum of six blocks can be generated at a steady rate. Once the blocks are generated, they are then chained and linked together in a chronological order. Now Figure 11.1 shows the difference between centralized, decentralized, and distributed structure with respect to blockchain.

The diagram shown in Figure 11.2 elaborates on the work flow of blockchain and procedures involved Consider the case wherein Bob transfers some bitcoins to Alice. This leads to the creation of a new transaction which is stored in a block. Following this, the nascent block is broadcasted to the network and all corresponding nodes. The nodes validate the authenticity and verify the block. If the block is considered to be valid, it is then added to the blockchain and the same process continues each time a new transaction occurs [2].

When considering blockchain, it is extremely important to understand the structure of the blockchain which is a peer-to-peer distributed ledger system. From a common man's view, the platform put forth by this technical concept is where people are able to perform and record transactions of various types without a third-party arbitrator [3]. This database of transaction records is then shared and distributed among the participants of the network through transparent

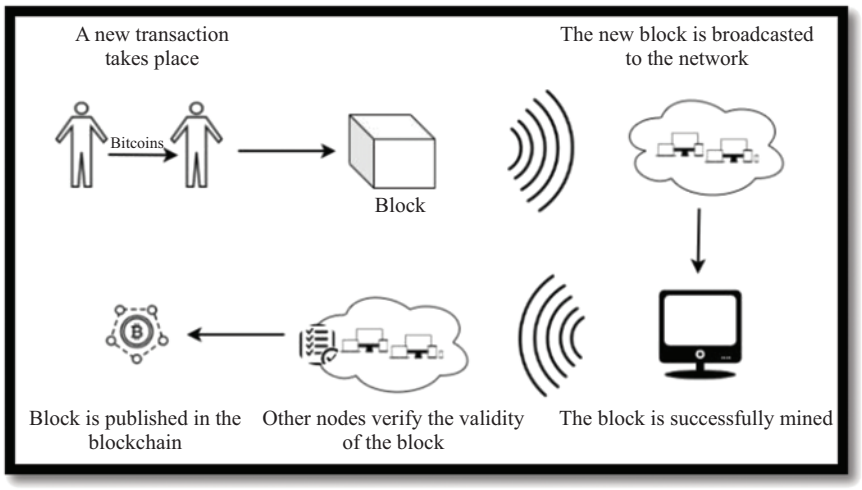

Figure 11.2 Workflow of blockchain

and flexible means which is accessible to all. In terms of managing the database, it is taken care by peer-based networks with a time-stamped server recording every action. Furthermore, the blocks in the chain are organized in such a way that it mainly refers to the contents of the previous block. The architecture of blockchain mainly includes the nodes within a peer-to-peer network, the genesis block, transactions within the block, process of validation and verification through mining, and PoW. The framework of blockchain can be seamlessly comprehended by considering the example of Google documents. Just like how one can open up a Google doc, add editors and track the real-time edits through which people from different parts of the world can work simultaneously on the same document, blockchain system also follows a similar technique that enables the distribution of digital data by adhering to trust, transparency, and data security. The structure and architectural aspect of blockchain is not the same as that of any other conventional database. Here, each participant in the network is capable of maintaining, approving, and updating novel transaction entries and the power, hence, is not vested in the hands of a single node/individual [4]. The blockchain structures mainly fall into one of the three categories—public, private, and consortium blockchain architecture. The public architecture is the one that involves data accessibility to anyone willing to join the network such as Bitcoin, Ethereum, and Litecoin. The private architecture, on the other hand, is completely controlled by users from a certain organization or group who can participate only on invitation.

The last type of architecture, the consortium architecture, is the one owned by a group of organizations wherein, the procedures and rules are set up by the assigned users at the rudimentary level. Figure 11.3 shows an elaborate view of the

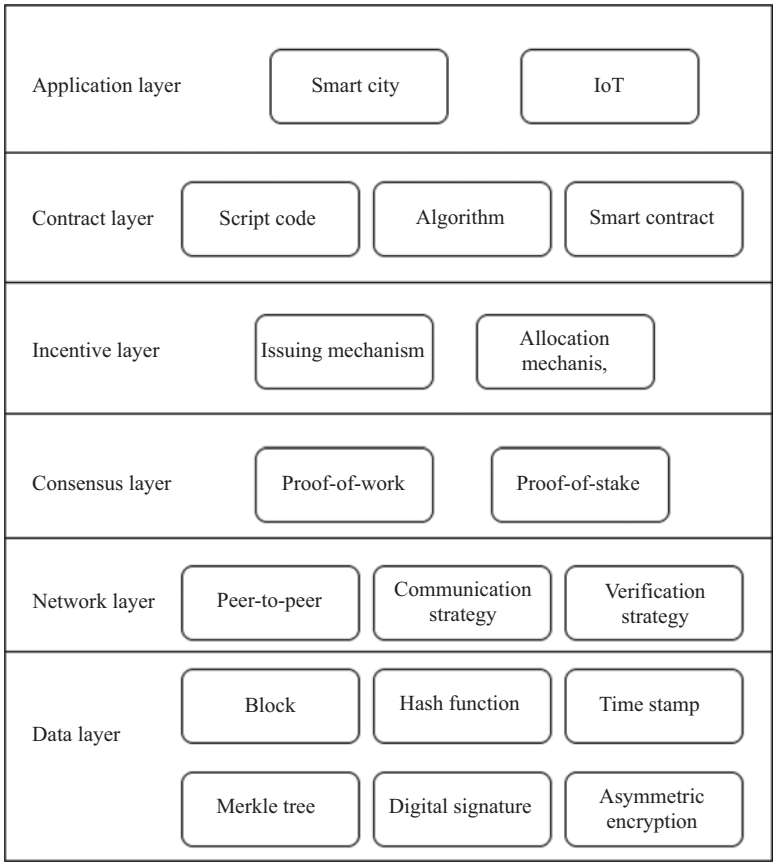

Figure 11.3 Architecture of blockchain

various layers involved in a blockchain architecture including layers like application, contract, incentive, consensus, network, and data layers.

Figure 11.4 elucidates the structure of blockchain. Each block has a set of information which consists of the hash value of previous node, hash value of current node, nonce (number used only once) value, the timestamp at which it was processed, and the Merkle root pointer. Each Merkle root pointer points to a tree-like structure where the transaction details are essentially stored. Also, Figure 11.5 shows the creation of new block in a blockchain network.

The architecture of the can be roughly sketched as consisting of a bottom sensor layer, a middle network layer, and a top application layer. As one of the primary information-acquiring means at the bottom layer of the tags have found increasingly widespread applications in various business areas, with the expectation that the use of RFID tags will eventually replace the existing bar codes in all business areas.

AQ4

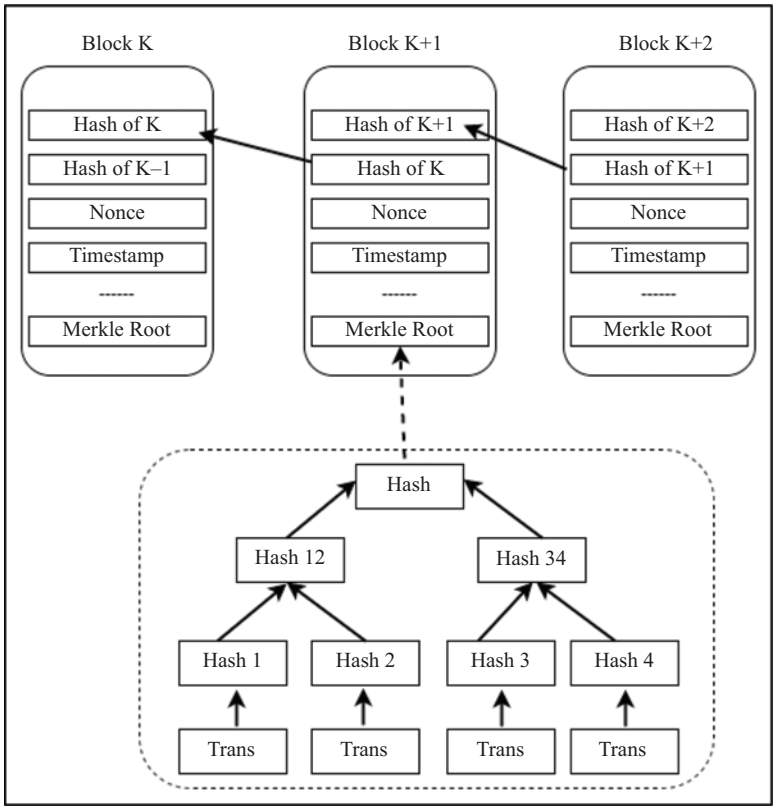

Figure 11.4 Structure of blockchain

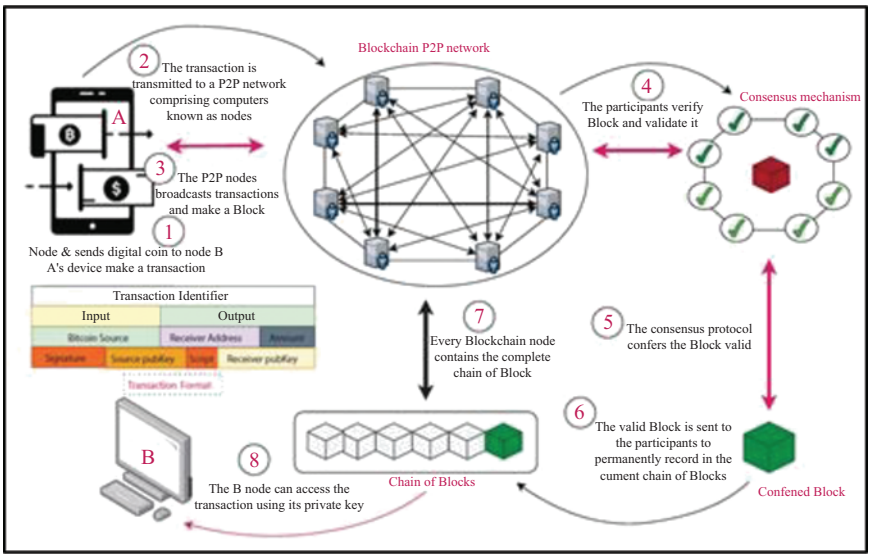

Figure 11.5 Creation of new block in a blockchain network

AQ5

11.2 Related work

There are quite a few similar technologies and concepts of blockchain in use today. Many of the financial transaction records and tracks are maintained through a central controlling authority and a ledger concept is utilized for this purpose. This is because only a ledger can reliably ensure the integrity and safety of highly confidential financial details of customers. In the very first stages, blockchain was majorly known for its core use in cryptocurrency wherein transactions and transmission of amounts from one person to the other did not require the mediation of a third-party central control [5]. In the case of cryptocurrency, the ledgers and storage details of all participating individuals are shared among each other so as to maintain transparency and a sense of loyalty. The possibility of attacks and data breaches by malicious users and crackers is almost impossible because of the decentralized and distributed nature of the blockchain technology and also because of the consent-oriented mechanism followed before recording transactions. In other words, there is no single individual in whose hands the power is vested. This additionally provides a benefit of easing out the process of updating or modifying the blockchain system [6]. The works of authors in [7] focused on the systematic review of blockchain and further initiatives taken up in the same area. They have reviewed and analyzed more than a hundred blockchain research works through which they have curated an opinion that surveys the relevance of blockchain for energy applications. In [8], the research conducted by the authors highlights the societal impacts, possible opportunities and bottlenecks, along with some of the major trends observed in blockchain. Similarly, the work put forth in [9] describes and clarifies the holistic aspect of blockchain technology from the view-point of energy usage of bitcoins. It also elaborates on the various types of blockchain consensus and draws conclusive elucidations. In [10], the basics of blockchain along with a detailed explanation of the various types of blockchain technology are described. It also highlights some of the major attacks and issues that blockchain technology may be exposed to. Note that many useful works related to blockchain can be found in [11–13].

11.3 Evolution and timeline of blockchain

The very first phase of blockchain sparked off with the out surge of transactions. There were many technologies, right from the start, which were based on the logical concept of bitcoins and blockchain long before it actually began. Merkle tree is one among these which is named after the infamous scientist Ralph Merkle which is ideally a data structure that stores and verifies the individual records [7]. However, this was not the only setup stage for blockchain. The very early years of blockchain technology in the 1990s were the contributions of Stuart Haber and W. Scott Stornetta which mainly revolved around the fields of cryptographic implementations to secure a chain of data blocks such that no external attacker would be able to tamper with the data and timestamps. By 1992, this system was further upgraded to integrate the use of Merkle trees so as to increase the efficiency and

allow a greater number of data to be stored within each block. Up until 2008, blockchain did not gain much significance or relevance. However, in 2008, blockchain history comes into spotlight and its beneficial aspect is noticed at large capacities. This was because of the works put forth by the individual/group Satoshi Nakamoto who was the first one to work on bitcoins which is the very first and rudimentary application of the digital ledge technology. In the current world, the application of blockchain has definitely evolved and is being used in several applications apart from cryptocurrencies. After putting forth the ideology and concept of using blockchain technology for bitcoins, Satoshi Nakamoto exited the scene and from then on it was taken up by various core developers across the globe leading to exciting and innovative evolutions [8].

11.3.1 Phase 1 of blockchain evolution

During the years of 2008–2013, which is ideally the first phase of development in the field of blockchain technology. The paper published by Satoshi Nakamoto contained details and information pertaining to an electronic peer-based system. He had curated the very first genesis block on the basis of which further blocks were mined and incorporated leading to one of the longest chains of data-carrying blocks. Ever since this incident, a variety of use-cases have emerged that leverage and utilize the working principle and abilities of the distributed ledger technology [9]. Figure 11.6 sows all of its evolution since 1.0–4.0 in detail.

11.3.2 Phase 2 of blockchain evolution

The years 2013–2015 mark the second phase of evolution in the blockchain history. Among the various developers that were extracting and experimenting with blockchain, Vitalik Buterin was one of the developers who believed that bitcoin

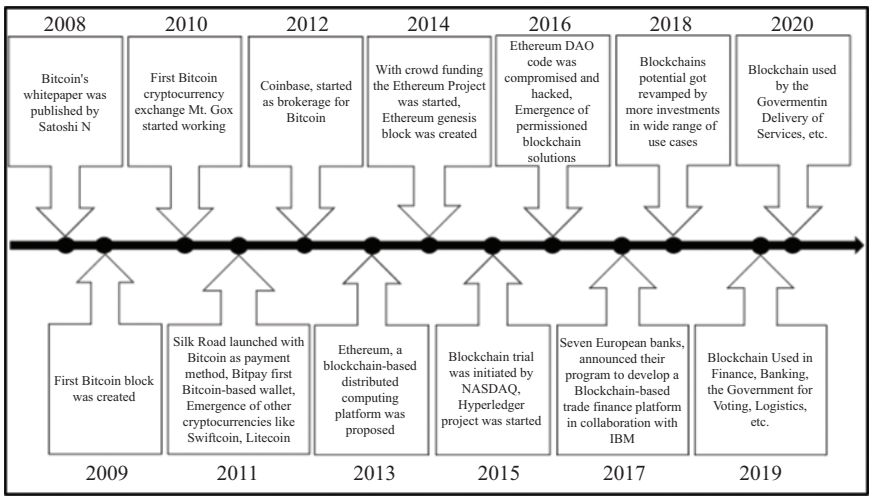

Figure 11.6 Evolution of blockchain since 2008

had not reached its full potential level. He opined that bitcoin still had many limitations and disadvantages and initiated his work on a form of blockchain that was malleable and could perform additional functions apart from a peer-to-peer network. This led to the birth of Ethereum in 2013 which was initiated out of a novel public blockchain technology. Ethereum had nascent capabilities in comparison to bitcoin. This truly was pivotal moment in the evolving history of blockchain [10].

The main difference between Ethereum and bitcoin was that Ethereum has a particular functionality that permits people to record and track information such as slogans and contracts and not just mere transactions. Ethereum was officially launched in the year 2015 and is definitely one of the biggest applications of blockchain considering its capacity to aid smart digital contracts and other functions.

11.3.3 Phase 3 of blockchain evolution

Following the year 2018, a plethora of projects and initiatives that revolve around the advantages of blockchain have emerged and many of the researchers have also highlighted some of the possible deficiencies in the use of bitcoin and Ethereum which are further being worked upon. The rise of many applications such as China's first blockchain platform NEO, integration of blockchain with Internet of Things (IoT), development of other blockchain platforms such as Monero Zcash and Dash. have taken the world by a storm [14]. In 2015, the Linux group initiated one of its side projects that focuses on an open-source blockchain system called Hyperledger and to date, it continues to act as a combined emergence of numerous ledgers. The main aim of Hyperledger is to encourage the advanced utilization of blockchain to enhance the efficiency and reliability of the system for global transactions. In 2017, the birth of EOS took place which is the child of a private firm "blocl.one." Their proposal was a novel blockchain protocol which was fueled by EOS as the original cryptocurrency. The future of blockchain is definitely bright and shiny with an increasing number of applications across the globe in various disciplines and aspects be it finance, supply chains, transportation, etc. [15].

11.4 Blockchain in IoT and other computing platforms

IoT is a broad and rising concept in the modern era which refers to the interconnection and integration of smart gadgets and devices to gather data and information and make suitable decisions. The use of IoT in various aspects of life has been on a rampant increase over the last few years making it ubiquitous and empowering the connection and interconnection of devices. Cloud computation, Machine Learning (ML), information modeling, etc. are some of the technologies that have made use of the IoT fabric for further advancements. Amidst these growing opportunities, one of the dark sides of IOT is in terms of its security and privacy concern. There are more than a 100 "things" or nodes getting connected to the web with every passing second and each of these nodes are involved in exchanging some form of data or information within and outside the network. Blockchain technology is capable of fully addressing these concerns and hence, it is

integration with IoT can efficiently resolve the security concerns. This combination is often termed as BIoT [16]. One of the main reasons why blockchain can provide a secure and stable platform for IoT devices is its need to validate all transactions before confirming and recording the transactions to the ledger. The execution of this approach ensures that there is no single authority or power responsible for making decisions and, therefore, offers a massive amount of trust and reliability to the followers of this network. On the other hand, if the conventional IoT approach is being used, then a centralized system comes into action and the transactions that are published into the ledger are verified by a third-party organization leading to increased expenditure and a single power making decisions. This often results in lack of transparency and high possibility of fraudulent activities.

In terms of publicity, the IoT devices mainly consist of a dynamic and galvanic system, all of which are configured in a way to exchange information and data with the privacy of users remaining protected. When blockchain comes into play, the situation becomes such that the participants can get insights on the transaction details being recorded and each participant will have its own ledger. The fact that each of the nodes in a blockchain have its own ledger and storage facility is what makes the system of BIoT resilient and strong enough to withstand any sort of attack. In case of a node being maliciously captured or compromised, the overall performance would still not be affected as the data stored in the captured node is also available individually to all other nodes. Security is one of the other features that integration of blockchain guaranteed and is a foundational aspect for IoT considering the large number of devices that are linked together over the web [17]. It is also a cost-effective solution in comparison to the alternative solutions which often call for extremely high maintenance costs and infrastructural developments with a centralized framework. Furthermore, the fact that blockchain technology uses a ledger that which is decentralized and distributed ensures that it is immutable in nature and this further warrants for an enhanced privacy and security preserved environment for IoT.

In the case of transactions being processed by blockchain, the anonymity of both the sender and the receiver with respect to their address is maintained with the help of distinctive addresses which are masked to preserve the actual identity. Though this has been exposed to criticism in cryptocurrencies, it has been advantageous for applications such as digital voting and healthcare records. Also, the fact that each node in IoT can be validated easily though BIoT via accessible identity management and its commitment toward accountability and data traceability is what makes it unique [18].

11.5 Characteristics of blockchain over other technologies

The main factor that contributes to blockchain having an upper-hand over other technologies is the following characteristics:

- *Decentralization*: In a conventional system for managing and controlling transactions, the verification process usually takes place through a third-party

agency that is reliable like a bank or government. However, this often adds up the cost and leads to bottlenecks or catastrophic conditions in case of single-point failures. In contrast to this, if blockchain is used, then the transactions are verified between peers without the need for an additional authentication or intervention by a third-party agent or mediator. This helps reduce the cost drastically and mitigate any problems that are likely to arise [19].

- *Immutability*: Blockchain mainly contains a sequential collection of blocks of data which are linked to each other through hash pointers and values. A slight change or modification in the previous block would break the chain and all subsequent blocks would be invalidated. From the point of view of a Merkle tree, the root hash of the tree acts as the hash value of all confirmed transactions such that a change in any of these leads to the generation of a new root. This is what guaranteed the integrity of sustenance of data [20].
- *Non-repudiation*: In blockchain, a private key is notably used to attest or sign a transaction which can further be verified by all other participants using the corresponding public key that is accessible to all [21].
- *Transparency*: Majority of the blockchain frameworks ensure that each of its participants can access and engage with the network on equal grounds. Each of the new transactions is not only validated and recorded in blockchain but is also made available to each of the users in the network [22].
- *Pseudonymity*: Another feature of blockchain to be highlighted is its ability to maintain a certain level of anonymity while also ensuring transparency. This can-not just help in fraud detection but also help in identifying illicit transactions.
- *Traceability*: One of the unique and useful features of blockchain is the easy traceability factor with the help of a timestamp attached to the block in the chain. This comes in handy to validate and trace the origins of past data.

11.6 Types of blockchain and comparisons

Blockchain is generally classified into three main types: public, private, and consortium blockchain.

- *Public blockchain*: It is the type that allows all the stored transactions to be openly and publicly available to the public. The nodes or participants also have the liberty to join or leave the network as per their convenience and each individual can validate and cross-verify the transactions before it gets published. Examples of public blockchain include Bitcoin and Ethereum [6].
- *Private blockchain*: This type of blockchain is completely owned and regulated by a private organization and they provide limited or restricted access only to particular participants. Not every node can actively contribute to the blockchain network. They have stringent management techniques and methods for access to data and regulation policies. Enterprise Ethereum, Tezos, etc. are examples [5].
- *Consortium blockchain*: This type of blockchain is mixture of both public and private consisting of certain nodes that require permission to engage in the

Table 11.1 Types of blockchain

Feature	Private blockchain	Consortium blockchain	Public blockchain
Determining consensus	One organization	Selected number of nodes	All miners
Read permission	Restricted or public	Restricted or public	Public
Immutability	Can be tempered	Can be tempered	Nearly impossible to tamper
Efficiency	High	High	Low
Centralization	Yes	Partial	No
Consensus technique	Permissioned	Permissioned	Permission-less

consortium chain process and other nodes which have the freedom to take part in transactions. This is in fact, a partially decentralized framework. R3CEV and Hyperledger fabric are examples of the consortium blockchain [5].

Table 11.1 shows the differentiation of each type of blockchain based on the major characteristic features as described in the previous section.

11.7 Types of consensus algorithms

Consensus algorithms are crucial in the case of blockchain networks and it is a field that has been researched and worked upon extensively to ensure a robust and reliable architecture. When it comes to blockchain, the consensus algorithms mainly need to deal with malicious, selfish, or faulty nodes such that they do not affect the global state of the chain of nodes. Majority of the consensus algorithms tend to address the three major characteristics through which the efficiency and impact can be determined.

- *Safety*: This property ensures that there is never a possibility of leakage or misuse of data and other confidential information. In general terms, a consensus mechanism is considered to be secure and safe it there is at least one node that generates an authentic output such that every other node receives the same. This leads to the consistency of data and information across the network making it safe and atomic [7,9].
- *Liveness*: The feature of liveness is to guarantee the best possible option to happen with due time and is often termed as a termination of conventional consensus in decentralized and distributed systems. This points to the fact that each genuine process would gradually decide on the same correct value. The consensus algorithm guarantees the feature of liveness and does not contain any tie bound restrictions to decide on a certain value [14,15].
- *Fault tolerance*: Consensus algorithms need to provide a hefty fault tolerance feature to ensure that the system is free from failures and is resilient to external

attacks. There are two possibilities in terms of node failures. One being fail stop category that leads to nodes being disabled from processing for temporary/permanent periods of time. The other failure possibility is a Byzantine failure where the malicious nodes are specifically curated to overcome the features of a consensus protocol [4,23].

11.7.1 Types

The literal meaning of consensus translates to an agreement or mutual understanding between participating nodes. It is essential in analyzing and comprehending the process of authentication of blocks when being added to the chain of blocks. Figure 11.4 elaborates on the various types of consensus techniques. There are two main types of consensus algorithms. The first type is the proof-based algorithm while the second type is the vote-based algorithm. Some very commonly used consensus mechanisms are as follows:

- *Proof-of-Work* (*PoW*): This type of consensus resembles a puzzle which is to be solved and figured out by the various participant nodes so as to mine and add a new block to the existing chain. The principle of this algorithm resonates to the node which has computed the maximum amount of work is the one that receives maximum reward or return of interest. This is the consensus used in bitcoin system. Some of the algorithms that make use of this consensus mechanism include Cuckoo hash function, finding prime numbers, ghost protocol, etc. [24].
- *Proof-of-Stake* (*PoS*): The PoS mechanism requires far less amount of processing and compute power in contrast to PoW and is utilized in scenarios which necessitate an energy efficient technique. The nodes participating in a system using the PoS consensus is least involved in attacking/hacking it and hence, they only need to showcase their engagement gradually through currency [25].
- *Delegated PoS* (*DPoS*): The DPoS is different from the conventional PoS mechanism with regards to the number of participants and only certain selected participants can develop, validate, or adjust the size of the blocks [20].
- *Proof-of-Activity* (*PoA*): This algorithm motivates every involved node and stakeholders in participation leading to the passive and silent nodes also earning rewards [20].
- *Proof-of-Burn* (*PoB*): The PoB consensus mechanism calls for the dedications of node miners with the proof of work in the form of digital currencies. It correlates to the fact that rather than wasting energy, compute power, etc., the currencies need to be burnt [21].
- *Practical Byzantine Fault Tolerance* (*PBFT*): This is one unique consensus mechanism for commercial organizations wherein the participants are partially trusted. The bottleneck of this strategy is the possibility of exponentially rising message counts each time they're added to the set [18].

Apart from the above-mentioned types of consensus algorithms, one of the popular techniques is the distributed consensus algorithm. Coming to a conclusion and mutual understanding of the blocks of data that need to be accepted and added

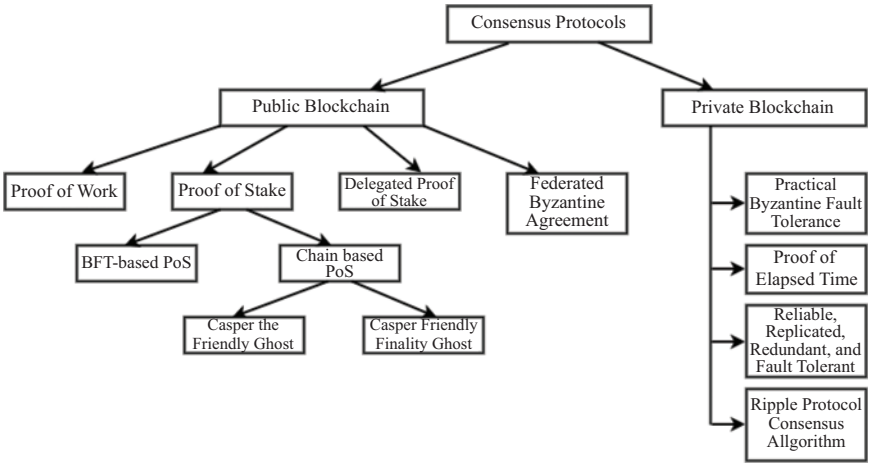

Figure 11.7 Types of consensus mechanisms in blockchain

can be quite challenging and tedious. However, in order to reach an agreement efficiently in a distributed framework, a few conditions are to be met. Termination, agreement, validity, and integrity are the major pillars that contribute to a safe and secure distributed consensus mechanism. The application of this distributed strategy spans along the lines of electing leader nodes in a fault tolerant space to kickstart a global uniform action, maintaining a level of consistency and atomicity in a distributed framework, etc. [22]. Figure 11.7 shows several types of consensus mechanisms in blockchain in detail.

11.8 Applications and use cases of blockchain

The growth of blockchain across the world has led to its implementation in numerous arenas of life and it has given rise to a plethora of use cases, some of which are discussed below.

- *Supply chain*: Integrating blockchain along with supply chains can aid the participants to easily track and keep records of price, location, quantity, quality, etc. which would in turn positively affect the efficacy of the supply chain system. It could not only help reduce the bureaucratic hurdles but also improve the operations in general. This would further prove beneficial as the costs get reduced dramatically. The decentralized structure of blockchain is a guarantee to the fact that it provides space for storage which is permanent and unalterable. Large tech corporations like IBM have invested on and developed blockchain frameworks to complement them in terms of integrating data between the various people and groups involved logistically [1].
- *Agriculture*: The discipline of agriculture and farming surely is a potent area for blockchain technology to dwell on as it helps in securing the possibility of

tracing information and details pertaining to the supply chain in the food avenue. This is further used to innovate and generate ideas for smart farming and index-based insurances for agricultural development. Not only does this technique help in decreasing the environmental footprints, but it also guarantees to cater to the growing demands of increasing population while maintaining transparency throughout [2]. The fact that blockchain technology can be succinctly used for handling forecasted dangers and issues so as to maintain uniformity and consistency throughout the systems is an added advantage. Ranging from initiating a sustainable business and decreasing waste, all the way to ensuring informed customer decisions and smooth transaction processes, all of it can be taken care of with incorporating blockchain in the agricultural sector.

- *Healthcare*: The health industry is yet another field that undergoes evolutionary changes, especially with the incorporation of technology. Incorporating a blockchain network in this field can support the easy ways to preserve and interchange health records of patients and can also contribute towards recognizing risky and dangerous flaws in the medical sector. The main advantage is its ability to revolutionize the process of analyzing health and medical records for the better [5]. Not only does blockchain integrated healthcare facilities ensure a safe way of transmitting medical and health records of patients, but it is also very useful to deal with the healthcare supply chains and aids medical researchers as well. Akiri, a company in California, utilizes a network based blockchain service to protect and preserve the privacy of patients with respect to their health records and information. Similarly, MedicalChain is one of the other companies in England that helps in maintaining the cohesive and integrated nature to protect the identity of its patients.
- *Governance*: Blockchain can be effectively used to provide and substantiate a massive framework for public management and this technology can be utilized at the micro, meso, and macro tiers. This distributed ledger technology has the power and resources to make government operations smooth and seamless. Be it in terms of enhancing the execution and delivery of public services or to establish a higher level of trust, blockchain sure does work for the best. The features of data protection and security, reduced manpower needs, high levels of transparency, and improved robustness are what makes it a great platform to intersect with public governance. In 2020, China had initiated the blockchain-based service network (BSN) to support public blockchain and in 2017, the USA signed a contract with IBM Watson Health to collaborate on blockchain systems to transmit health data safely [8].
- *Transportation*: The sector of transportation and automobiles can derive quite a few benefits from blockchain. Be it for smart delivery tracking, scalable and immediate solutions for validating orders, and what not; blockchain has the potential to resolve these problems with utmost efficiency. It can help as a trustworthy data verification tool in transport and logistics, aid in tracking and monitoring fleets of trucks, accidents, routes, etc. The fact that it helps reduce time and involves a faster and straightforward execution process is what

adheres to the successful integration of blockchain with the transportation sector [9]. It can be clearly observed that blockchain is truly contributing towards the evolution of transportation industries by accelerating its efficiency and customer experience while diminishing costs. It improves the efficiency by enhancing delivery processes and by initiating steps to advance productivity levels, which in turn also strengthens the supply chain process. Therefore, transportation is definitely the perfect solution for the sophisticated and decentralized transportation services in the urban areas today.

- *Smart contracts*: In simple terms, smart contract are programs that are stored and leveraged on a blockchain system which are executed whenever certain conditions are met. They are ideally meant to automate the process of executing agreements such that each node miner can acquire the outcome at the earliest. Using smart contracts ensures that transactions are traceable, irreversible, and transparent. ~~There are~~ Ethereum-based smart contracts~~; these days that~~ can be used to generate digitized token to carry out transactions [15]. The biggest highlight of smart contracts developed on blockchain is its feature to enable loyal transactions and agreement processes to be conducted between anonymous parties and groups without the requirements of a central legal authority or power. AQ6
- *Artificial Intelligence* (*AI*): The combination of blockchain and AI is extremely powerful and has the capacity to upgrade the status quo of anything its being applied to. An integration of these two means that while AI can take care of processing and mining large datasets and discover patterns from experience, blockchain can contribute towards removing bugs and detecting fraudulent or malicious data. On the whole, the outcome would have improved business models, globalized and distributed validating systems, intelligent financing, and creative compliance systems when AI meets blockchain [16]. Companies like CertiK, located in New York, offer tools that are fueled by AI to safeguard blockchain-related applications by detecting any sort of security breaches, supervise data insights, and analyze the movement of crypto-based funds. This insinuating combination of strong technologies offers massive benefits including those of advanced security features, accessing and handling the data market, and optimized use of consuming energy.
- *Cyber security*: The discipline of cyber security is highly relevant in the 21st century world where we tend to thrive on social media and virtual platforms which have access to our personal information and details. In such circumstances, there are high chances of cyberattacks and crimes that can prove to be deleterious. The integration of blockchain technology with that of cyber security would lead to the development of integrity for software download, protection and safeguarded data transmission, decentralized technique of storing critical data, and mitigating denial of services attacks. It would conclusively cover the triad that consists of confidentiality, availability, and integrity [5,17].
- *Cloud/edge computation*: The relationship between blockchain and clod/edge computing is mutual and symbiotic. Edge computing, with its distributed

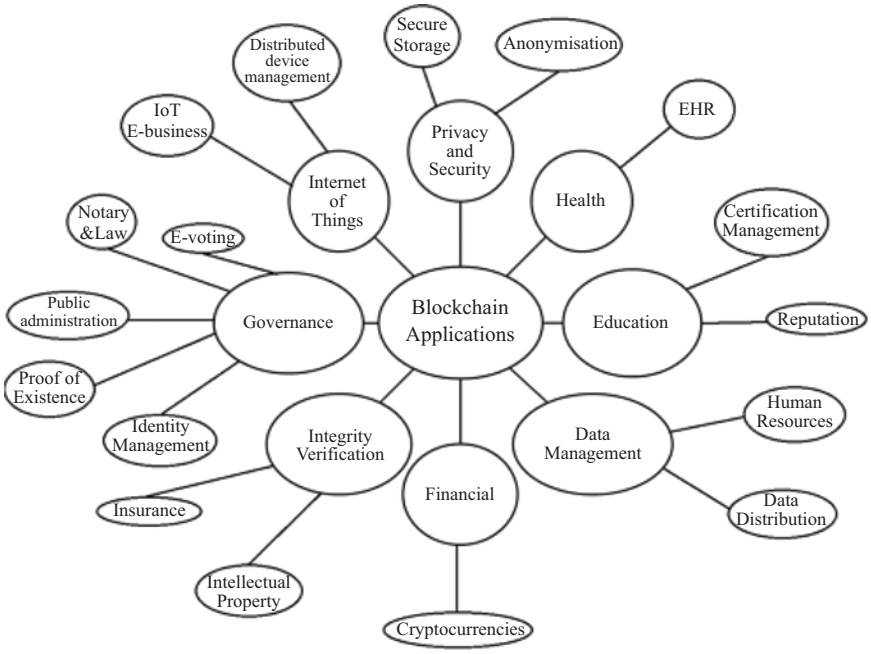

Figure 11.8 Blockchain uses in finance and non-finance applications

framework, can provide the framework for the nodes in blockchain to store the data while blockchain could derive the benefits of using a completely open cloud platform. This combo packed combination can lead to a platform that is perfect for a secure, scalable, and distributed avenue for IoT as well [24]. The balanced mix of blockchain and edge computation can be effectively utilized for various cryptocurrency-based applications, IoT in the industrial sector, healthcare, smart cities, and smart homes for automation purposed. Here too, the major highlighted feature is the safety and integrity of data being utilized across the various edge and cloud-based platforms through a distributed framework.

Figure 11.8 shows several types of applications which are relied on blockchain now a days.

11.9 Attacks and threats

Though blockchain is known for its security features, these systems are also prone to various security and integrity attacks externally. It could be in terms of the PoW (proof of work) consensus-based attacks like the 51% majority manipulation, delay or latency in consensus due to a distributed denial of service, pollution log, etc. [25]. One of the attacks is the selfish mining attack which is performed by the selfish

miners to acquire rewards and returns or to waste the compute powers of the genuine participants and miners. In this case, the attacker would hold back some of the privately discovered blocks and would fork the chain on which they build further. They try to get the private chain to be longer than the actual one and the honest miners would unknowingly mine on the public chain. After the private chain becomes long enough, it gets published by the attacker and the efforts of the genuine miner are at waste. This consolidation and cumulation of power into the favor of the attacker is what undermines the decentralized nature of blockchain at large [26].

One of the other attacks is the DAO attack. DAO is simply a smart contract which is deployed on Ethereum and it basically executes a crowd funding platform. Though it seemed to be a promising and reliant application, one of the hackers brought to light the major flaw of DAO which was able to drain out millions of Ether into a specific private account leading to a massive panic. This was one of its kind and highlighted the grey areas that surround the world of cryptocurrency and blockchain systems [27].

The Border Gateway Protocol (BGP) Hijacking attack is one other malicious attack. BGP is a de-facto routing protocol that focuses on maintaining and regulating the transmission of IP packets to their respective sources. In order to interject the traffic in the network, hijackers often manipulate the routing of this protocol and gains control over the network operators. The fact that blockchain is a decentralized system indicates that the entire system would be adversely affected in case of a BGP hijack event. Furthermore, even if the attack is detected or recognized, it costs a lot of money and computations to restore the system back to its altering configuration and calls for large amounts of manpower [28].

The type of attack that facilitates its attackers and hackers to grab away all of the incoming and outgoing connections of the victim, desolating the attacked from the peer network, is called the Eclipse attack. On successfully attacking, the attacker is capable of filtering and parsing through the victim's view of blockchain or cost up the compute power of the victim unnecessarily. The power extracted during the attack can also be used by the attacker to perform his/her own malicious activities. The botnet and infrastructural attacks come under the umbrella of the Eclipse attack [29].

Last but not the least is the liveness attack that has the potential to delay and interject latency pertaining to the confirmation time for as long as possible during the transaction period. This attack is carried out in three phases—preparation phase, transaction denial phase, and blockchain retarder phase. Ultimately, the attacker tends to build on the private chain so as to gain an undue advantage over the public chain. Following this, the attacker would publish the private chain of theirs to retard the growth of the original public chain [30,31].

11.10 Challenges and future trends

Blockchain, a revolutionary technology, is sure to exist and contribute to some of the major fields in the long run. Considered as the heart and soul of Web 3.0, the

advancement in this technology seems to approaching ahead of its time. Even though blockchain is often associated with cryptocurrencies, it no longer is the only field of relevance. Health sector, supply chain, transportation, finance, etc. are some of the many aspects in which blockchain has made ground breaking progress [32–34]. The blockchain market is growing at a rampant pace with the financial and insurance sectors leading the way. If you take a look at the current and possible future trends, it is very evident that blockchain technology is modifying the conventional financial system with around 90 countries already investing in central bank digital currencies. Furthermore, non-fungible tokens (NFT) have also been gaining increases momentum over the last year or so and are sure to remain efficiently prevalent in the coming years [35,36]. NFT's have proven to be a great means of income generation for artists across the world through their virtual and digital art forms. One of the other leading trends which is likely to take a massive leap in the future is the Blockchain-as-a-Service (BaaS) concept with tech giants like Amazon and Microsoft already implementing the same. BaaS will not only act as a cloud service but will also provide the added benefits of blockchain in terms of scalability and efficiency. Furthermore, blockchain is likely to grow a fanbase for enhancing social networking and e-commerce in the coming years [37].

Blockchain, without doubt, is one of the most significant technical developments that has impacted the society at a positive level over the last few years with an exponential growth in its adaptation [33]. However, this revolutionary industry also poses challenges and hurdles. Large level scalability continues to be a challenge for blockchain as it does offer difficulty in managing many users at a time which severely affects the processing power and speed of transactions [34,38]. Blockchain also tends to lack a collection of regulations to be followed globally leading to a volatile base and higher chances of manipulation [39]. Lack of awareness in technology is also one of the major challenges that often tends to leave blockchain as a distant dream [40].

11.11 Conclusion

Blockchain is a novel technology that definitely has a massive scope in the present and future generations but also has quite a number of challenges to overcome and hustle through. This decentralized, transactional ledger storage base has enhanced and led to developments across the globe. It supports users to validate, preserve/store, and synchronize the contents of a data sheet which is mined and worked upon by various users. Due to the vast and enormous possibilities of applications, it is expected that blockchain will complement in trusted transactions. The emergence of Bitcoins is what gained maximum attention for blockchain and its framework. This paper provides a detailed analysis and survey of what is blockchain, its architecture and framework, the history and evolution of blockchain, its types, its applications, and possible attacks.

References

[1] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, 2019.

[2] J.A. Jaoude and R. George Saade, "Blockchain applications–usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.

[3] V. Chang, P. Baudier, H. Zhang, *et al.*, "How blockchain can impact financial services – the overview, challenges and recommendations from expert interviewees," *Technol. Forecast. Soc. Change*, vol. 158,2020, Article 120166.

[4] C.S. Tang and L.P. Veelenturf, "The strategic role of logistics in the industry 4.0 era," *Transport. Res. E Logist. Transport. Rev.*, vol. 129, pp. 1–11, 2019.

[5] C.M.S. Ferreira, R.A.R. Oliveira, J.S. Silva, *et al.*, "Blockchain for machine-to-machine interaction in Industry 4.0," in *Blockchain Technology for Industry 4.0*, Springer, Singapore, 2020, pp. 99–116.

[6] P. Sandner, A. Lange, and P. Schulden, "The role of the CFO of an industrial company: an analysis of the impact of blockchain technology," *Future Internet*, vol. 12, no. 8, p. 128, 2020.

[7] M. Andoni, V. Robu, D. Flynn, *et al.*, "Blockchain technology in the energy sector: a systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, 2019.

[8] P. Dutta, T.M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: applications, challenges and research opportunities," *Transp. Res. Part E: Log. Transp. Rev.*, vol. 142, p. 102067, 2020.

[9] B. Esmaeilian, J. Sarkis, K. Lewis, *et al.*, "Blockchain for the future of sustainable supply chain management in Industry 4.0," *Resour. Conserv. Recycl.*, vol. 163, 2020, Article 105064.

[10] Golosova, J. and Romanovs, A., "The advantages and disadvantages of the blockchain technology," in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*. IEEE, 2018, pp. 1–6.

[11] A.K. Tyagi, S. Chandrasekaran, and N. Sreenath, "Blockchain technology: a new technology for creating distributed and trusted computing environment," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, pp. 1348–1354, doi:10.1109/ICAAIC53929.2022.9792702.

[12] A.K. Tyagi and A. Abraham (eds.), *Recent Trends in Blockchain for Information Systems Security and Privacy,* 1st ed.. CRC Press, 2021. https://doi.org/10.1201/9781003139737

[13] A.K. Tyagi, G. Rekha, and N. Sreenath (eds.), *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*. IGI Global, 2021. 10.4018/978-1-7998-3295-9

[14] J.W. Leng, G. Ruan, P. Jiang, *et al.*, "Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: a survey," *Renew. Sustain. Energy Rev.*, vol. 132, 2020, Article 110112.

[15] G. Zyskind, O. Nathan, and A.S. Pentland, "Decentralizing privacy: using blockchain to protect personal data," in *Proceedings of the IEEE Security and Privacy Workshops*, pp. 180–184, May 2015.
[16] J.J. Xu, "Are blockchains immune to all malicious attacks?", *Financial Innov.*, vol. 2, no. 1, pp. 1–9, 2016.
[17] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innov.*, vol. 2, p. 24, 2016.
[18] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government, services—use cases, security benefits and challenges," in *Proceedings of the 15th Learning and Technology Conference (LT)*, Feb. 2018, pp. 112–119.
[19] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: a structured literature review," in *Proceedings of the 8th International Conference on Exploring Service Science*, 2017, pp. 12–23.
[20] R. Hull, V.S. Batra, Y.M. Chen, A. Deutsch, F.F.T. Heath, and V. Vianu, "Towards a shared ledger business collaboration language based on data-aware processes," in Q. Z. Sheng, E. Stroulia, S. Tata, and S. Bhiri, (eds.), *Service-Oriented Computing (Lecture Notes in Computer Science)*, vol. 9936, Cham, Switzerland: Springer, 2016, pp. 18–36, doi: 10.1007/978-3-319-46295-0_2.
[21] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 839–858.
[22] G. Zyskind, O. Nathan, and A.S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proceedings of the IEEE Security and Privacy Workshops*, May 2015, pp. 180–184.
[23] J.J. Xu, "Are blockchains immune to all malicious attacks?" *Financial Innov*., vol. 2, no. 1, pp. 1–9, 2016, doi: 10.1186/s40854-016-0046-5.
[24] M.M. Crossan and M. Apaydin, "A multi-dimensional framework of organizational innovation: a systematic review of the literature," *J. Manage. Stud*., vol. 47, no. 6, pp. 1154–1191, 2010.
[25] D. Tapscott and A. Tapscott, "The impact of blockchain goes beyond financial services," *Harvard Business Review*, 2016. https://hbr.org/2016/05/the-impact-of-the-blockchain-goesbeyond-financial-services
[26] C. Wood, B. Winton, K. Carter, S. Benkert, D. Lisa, and B. Joseph, "How blockchain technology can enhance EHR operability," in Proc. Ark Invest Gem, 2016, pp. 1–13.
[27] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommun. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
[28] R. Cole, M. Stevenson, and J. Aitken, "Blockchain technology: implications for operations and supply chain management," *Supply Chain Manage*, *Int. J*., vol. 24, no. 4, pp. 469–483, 2019.
[29] N. Kshetri and E. Loukoianova, "Blockchain adoption in supply chain networks in Asia," *IT Prof.*, vol. 21, no. 1, pp. 11–15, 2019.

[30] H. Kakavand, N.K. De Sevres, and B. Chilton, ''The blockchain revolution: an analysis of regulation and technology related to distributed ledger technologies," *Social Sci. Res. Netw. (SSRN)*, New York, NY, Tech. Rep. 2849251, 2017, pp. 1–27, doi: 10.2139/ssrn.2849251.

[31] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *Proceedings of the IEEE Technology, Engineering, Management Conference (TEMSCON)*, Jun. 2017, pp. 137–141.

[32] 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, 2019.

[33] J. Mendling, I. Weber, W.V. Aalst, *et al.*, "Blockchains for business process management–challenges and opportunities," *ACM Trans. Manage. Inf. Syst.*, vol. 9, no. 1, pp. 1–16, 2018, doi: 10.1145/3183367.

[34] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments,'' in Proc. Coin Rivet, 2016, pp. 1–59. [Online].Available: https://coinrivet.com/research/papers/the-bitcoin lightningnetwork-scalable-off-chain-instant-payments/

[35] M. Pilkington, "Blockchain technology: principles and applications," in Z.F. X.O. Majlinda and E. Edward (eds.), *Handbook on Digital Transformations,* Cheltenham, UK, 2016, doi:10.4337/9781784717766.00019 AQ7

[36] A. Lazarovich, "Invisible ink: Blockchain for data privacy," *Massachusetts Inst. Technol.*, Cambridge, MA, *Tech. Rep.*, 2015, pp. 81–85.

[37] R. Kestenbaum, Why bitcoin is important for your business. *Forbes*, 2017. https://www.forbes.com/sites/richardkestenbaum/2017/03/14/why-bitcoinis-important-for-yourbusiness/3/#2da6d4c72b3b

[38] E. Munsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *Proceeding of the IEEE Conference on Control Technology and Applications* (CCTA), Aug. 2017, pp. 2164–2171.

[39] R. Ali, J. Barrdear, R. Clews, and J. Southgate, "Innovations in payment technologies and the emergence of digital currencies," *Quart. Bull.*, vol. 53, no. 4, pp. 262–275, 2014.

[40] Y. Li, B. Wang, and D. Yang, ''Research on supply chain coordination based on block chain technology and customer random demand," *Discrete Dyn. Nature Soc.*, vol.2019, pp. 1–10, 2019, doi: 10.1155/2019/4769870.

Chapter 11

Blockchain technology for next-generation society: current trends and future opportunities for smart era

Author Queries

AQ1: Please provide the affiliations to the authors.

AQ2: Please check the section heading "Abstract".

AQ3: Please supply Keywords.

AQ4: please note that the paragraph "The architecture . . . " has been deleted as it has been repeated twice.

AQ5: Please provide better quality figure in Figure 11.5.

AQ6: Please check the edit made in the sentence "There are Ethereum-based smart . . . ".

AQ7: Please provide the publisher name in Re. [35].