Wireless Personal Communications (2022) 123:1201–1243
https://doi.org/10.1007/s11277-021-09176-7

A Review of Blockchain-Based Applications and Challenges

Pratima Sharma[1] · **Rajni Jindal**[1] · **Malaya Dutta Borah**[2]

Accepted: 16 September 2021 / Published online: 26 September 2021

Abstract
The deployment of blockchain technologies for multiple use cases has been widely investigated in the academic and business sectors over the last few years. The blockchain model has attained considerable attention due to its decentralized, persistent, anonymous, and auditable features. This review does a comprehensive literature analysis of broad blockchain implementations across several domains. The study's key objective is to present a thorough overview of the widespread deployments of blockchain technology and demonstrate how particular aspects of this innovative technology can change the business community's activities. Several papers are addressing the feasibility of using blockchain technologies in various fields. However, we include a description of blockchain concepts and comparative analysis of the application in six main fields: the Internet of Things, artificial intelligence, supply chain, cloud, healthcare, and multimedia networks. For each area, we analyze in-depth the approaches proposed by the research community and industry. This paper also discussed the different problems involved in each area. Finally, we explore the critical issues needed for the broader implementation of blockchain technologies in these sensitive areas.

Keywords Blockchain technology · Applications · IoT · Healthcare · Cloud storage · Supply chain · Multimedia

1 Introduction

Nearly a decade ago, the anonymous person behind Bitcoin, Satoshi Nakamoto, explained how blockchain technology, a decentralized peer-to-peer connected system, can be utilized to address the issue of preserving the transactions sequence and avoiding the problem of double-spending attack [1]. Bitcoin combines the transactions in a system of limited capacity called blocks that share the identical timestamp. The network entities can connect the blocks in sequential order to each other, with each block containing the preceding block hash to create a chain of blocks [2]. Therefore the framework of the blockchain continues to provide a secure and correct record of all transactions. Blockchain presented severe

✉ Pratima Sharma
sharmapratima9818@gmail.com

[1] Delhi Technological University, Delhi, India

[2] National Institute of Technology Silchar, Silchar, Assam, India

disruptions to traditional procedures as applications and transactions that need centralized structures or trusted third parties to confirm them can now work with the same level of certainty in a decentralized manner. The blockchain architecture can support inherent features such as transparency, reliability, auditability, and security [3, 4]. A blockchain is a decentralized registry structured in ordered blocks, where the published blocks are unchangeable. It is appropriate in the banking industry since banks can collaborate using the single blockchain structure and submit users' transactions. Thus, blockchain allows the verification of transactions beyond transparency. Organizations collaborate in this technology as they view the capability to decentralize their architectures and minimize their transaction costs as they inherently turn to be secure, reliable, and transparent.

The cryptocurrencies represent the significance of blockchain, which is currently more than 1900 and still growing [5]. Due to the heterogeneity of cryptocurrency implementations, such a growth rate could eventually cause interoperability [6] [7]. Also, the ecosystem is changing rapidly, as blockchain is utilized in many areas besides cryptocurrency, with smart contracts play a crucial part. Szabo gave the smart contract concept in 1994 as: "a computerized transaction procedure executing the terms of the agreement" [8]. It enables the transformation of the contract agreements into embeddable code [9], thereby minimizing external engagement and threat. Therefore, a smart contract is a contract between participants who do not trust each other, automatically enforces the contract terms. Smart contracts are codes running in a decentralized manner within the blockchain context and saved in the blockchain [4] without depending on any third authority. In particular, blockchain supports smart contracts that allow complicated processes and connections to create a new paradigm for many applications.

Thus blockchain technology has become increasingly relevant [10]. Nearly 33 percent of executives are already involved or consider blockchain technology for implementation [11] [12]. Analyzers and researchers are now aware of the latest technology's potential and research the growing applications across various industries [4]. Depending on the target audience, three types of blockchain can be identified [10]: blockchain 1.0 defines applications that allow digital crypto-currency transactions; blockchain 2.0 covers smart contracts and a range of services expanding outside crypto-currency transactions; and blockchain 3.0 covers applications in fields outside the previous two, like IoT, health, supply chain, and government.

Although many studies on blockchain technologies [13], we contend that there is little focus on surveys based on blockchain-enabled applications. Blockchain applications are not completely explained in many review papers [14]. Indeed, some studies aimed at the blockchain application and include the privacy and security challenges faced by the applications. These reviews consider only a few applications [16] and mainly focused on the security aspect [15] [18]. Other studies lack the technical details of the blockchain applications [17]. Some surveys also consider the particular area of blockchain and include the details of decentralized IoT applications [21] and big data management [20]. Other reviews consider the blockchain's privacy problems [22] [23] and their potential for trust in service systems [24] and P2P networks [25]. In [26] and [27], some technical details of blockchain structure such as its consensus methods [26], smart contract vulnerabilities [27], and other features like size, bandwidth, usability, data integrity, and scalability were also studied. Furthermore, other studies, such as [28–32], are based on the currency dimension of blockchain and the provided protection and security concepts.

Table 1 presents a comparison of existing literature reviews and survey papers. The existing studies lack a detailed and comprehensive analysis of the state-of-the-art applications allowed by blockchain and its challenges. Hence, this is the motivation behind this

Table 1 Comparison of related work

Review papers	Year	Focus area	Remarks
[15]	2019	General study and privacy analysis	The survey provides an analysis of blockchain applications and discusses the associated security and privacy issues
[16]	2019	General study	Present an analysis of three blockchain-based applications: IoT, healthcare, and business
[17]	2018	General study	Conducts a systematic literature review of blockchain applications
[18]	2018	Privacy	Survey the privacy issues of blockchain technology
[19]	2018	Trust model	A systematic review of literature, areas of blockchain technology based on the trust model
[20]	2017	Big data	Review the blockchain solutions and challenges in the field of big data
[21]	2017	IoT security	Present the survey of IoT security and identify the blockchain solutions and challenges
Proposed Work	2020	General study and comparative analysis	Conducts a systematic literature review of six blockchain applications. The proposed work performs a comparative analysis of each application category-wise, identifies the challenges of blockchain architecture in each domain, and generates future trends

work. In particular, we review the current literature and explore the numerous benefits and problems of blockchain use. In fact, by addressing the following three questions, we attempt to resolve this: (1) How do blockchain-based applications evolve? (2) What are the different working areas of blockchain-based applications? (Categories identification). (3) What are the challenges of the blockchain architecture in different procedures/processes of applications? Which limitations are those? Our research leads to a comprehensive analysis of blockchain technology applications. Based on a systematic review approach, we outline the academic community's interest and define three main work fields. First, the description of blockchain technology across a wide variety of sectors. Then further category-wise analysis of blockchain-based applications, taking into account the various limitations posed by the applications. In the end, we are guiding researchers through a roadmap of promising research areas, challenges, and opportunities needed for future research. It is important to note that this study cannot be considered exhaustive since blockchain technology is continuously increasing.

The proposed work covers the following new contributions:

1. The authors provide a complete review of six areas of blockchain, including blockchain core research area, the IoT, healthcare, cloud storage, supply chain, and the latest research domains like AI and multimedia.
2. The proposed review includes the latest findings, articles, and documents in the areas mentioned above. It provides a systematic approach to studying the domain areas based on identified categories such as security and privacy, information storage, access control, consensus mechanism, and smart contract.
3. The various open challenges posed by the blockchain applications are thoroughly discussed, followed by analyzing recent advances, solutions, and future improvements.

The rest of this work is organized according to the following. A brief description of blockchain architecture shall be given in Sect. 2. The method followed for the systematic review of literature is highlighted in Sect. 3. The literature review descriptive analysis is presented in Sect. 4, while various blockchain applications are presented in Sect. 5. Related challenges and different lines of study are explored in Sect. 6. Section 7 highlights the recent advances and solutions for the open challenges. Finally, the paper concludes in Sect. 8.

2 Blockchain Overview

The developments in cryptography and distributed computing have introduced a modern computer technology called a blockchain. Blockchain is a distributed ledger that replicates and exchanges data through peer-to-peer (P2P) networks. Satoshi Nakamoto initially introduced blockchain, which created Bitcoin to directly trade digital currencies without third parties [33, 34]. Nakamoto has developed this paradigm of a network of nodes working to maintain a decentralized and secure database. As the name suggests, blockchain is an ordered list of blocks. By referencing the previous block's hash, each block is distinguished by the hash sequence and ties to the preceding block. The only anomaly is the first block, called the genesis block, which does not have the previous block's hash value [35]. Blockchain is the main backbone of cryptocurrencies. It can be regarded as both a technical breakthrough and financial advancement. It provides a solution to any problem, where

Table 2 Types of blockchain

	Public blockchain	Private blockchain	Consortium blockchain
Access	No access restrictions	Invitations only by network administrators	Restricted to selected members
Transact	Anyone can transact	Only designated individuals	Selected consortium members only
View	Anyone can view	Restricted	Restricted to selected members
Type	Large, decentralized, e.g., Bitcoin, Ethereum platform	Middle ground platform: record keeping and accounting	Participating companies equally involved in consensus, e.g., R3, Consensys

a trustworthy ledger is required in a decentralized setting, and there is no trust among the entities. Various literature reviews review the blockchain technology are application-specific like business applications [36], e-governance [37], healthcare [38], etc., but this paper reviews the six blockchain technology applications without being specific to particular applications, thus addressing its current trends, classifications, and challenges. Furthermore, blockchain technology is an information technology that can be used in software, business, and trade sectors [39]. The blockchain is viewed mainly as an accounting book or digital distributed database [40–45]. The architecture of the blockchain is illustrated in Fig. 1.

Blockchain technology is a distributed network that combines distributed data storage, cryptographic algorithms, and decentralized consensus mechanisms. Hence, this technology enables individuals to concur on a specific situation and record that ascension safely and undeniably in a different type of blockchain structure (Table 2) [46–48].

3 Research Methodology

This section presents scientific and systematic literature to give a transparent and reproducible review of applications based on the blockchain. The literature review presented by [49] has been suggested to understand their limitations. The presented methodological approach consists of the following essential steps:-

1. A review protocol has been developed by identifying the need for blockchain users and presented a review proposal.
2. Identification of various studies from the scientific journals by accessing their quality in terms of data extraction and synthesizing the data.
3. The results of the developed review protocol have been reported.

4 Research Studies

The primary research question has been addressed by initiating research in August 2019 without any time restrictions, and results were subsequently updated during March 2020. Google Scholar is considered the main database in which blockchain and associated terms have been searched in the main title block. Firstly, recent papers of 2019 have been

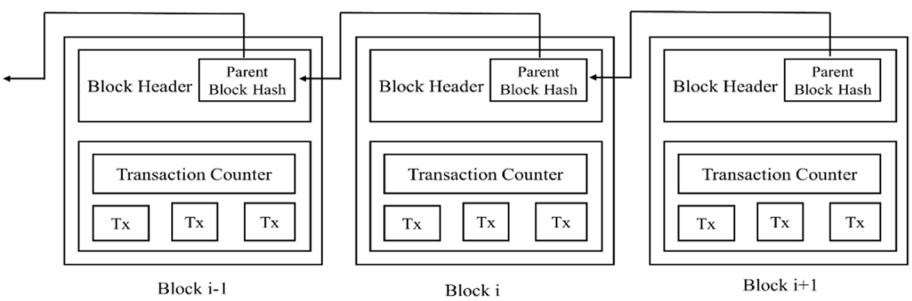


Fig. 1 Blockchain architecture

searched to determine the research gap. Additionally, referenced work in the searched article is also considered called a snowball effect. Consequently, grey literature was composed of unpublished work and reports commissioned through the public institutions identified through the electronic media. Other words, such as 'application' and 'blockchain challenges' was used to enhance the search procedure. The past grey literature in reports and policy draft reviews from the private and government sectors has been reviewed.

The strategy implemented to enhance the search paradigm is depicted in Fig. 2. Also, refinement studies from IEEE, Elsevier, and Springer are extensively described in the presented research. The abstract and conclusion of the past research have been studied, and when the abstract was not described, the full article has been retrieved as per its relevancy, such as m = 161 in the presented research. The articles having full text irrelevant to the research have been eliminated, such as m = 25. The articles having more citations and published in high-impact journals have been considered to enhance the research.

4.1 Assessment of Quality and its Evaluation

The study was conducted following the elimination criteria in which two exclusion principles were used to retrieve the meaningful data in the presented research. One was entirely based on the titles, and the other was based on the abstract and conclusion. The papers related to non-engineering concepts were eliminated. For instance, papers that discuss the ethical issues and economic aspects of the blockchain and cryptocurrencies were eliminated. Finally, the remaining papers from different domains of the blockchain have been included in the list. The selected articles were evaluated based on their quality and finally included in the introduction and literature section—the retrieval and elimination process of the research articles given in Table 3.

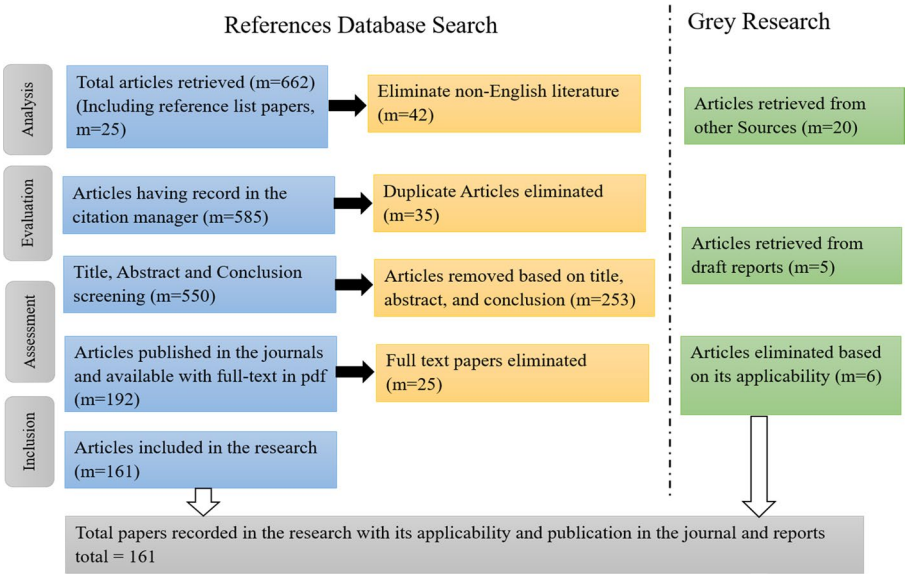


Fig. 2 Search mechanism

Table 3 Retrieval and elimination process

Selection strategy	Scientific journal papers	Grey research
Assessment	Articles related to blockchain in different domains (Journal papers, conference papers, reviews, surveys, book chapters, editorial notes, etc.)	Draft reports
Analysis	Cited in the citation manager	Reports related to blockchain are analyzed firmly
Evaluation	During abstract and title screening	
Elimination	During abstract and full-text screening	Generic reports having no relevant data eliminated
Inclusion	Remaining screened articles	

4.2 Data Synthetization and its Analysis

All the research papers and articles fitted in the inclusion criteria were analyzed using analysis software such as MAXQDA11. The thematic analysis was performed by the authors independently. Afterward, three groups were constructed in which previous review articles related to blockchain were placed in the first group, articles of blockchain, with its application placed in the second group. Finally, the third group consists of challenges faced by the researchers related to blockchain.

5 Descriptive Research Analysis

This section analyses the various research articles to understand the blockchain technology research trends worldwide with the proposed research analysis discussion.

5.1 Timeline of Blockchain Research

We have studied the various bibliometric analysis of blockchain technology to identify the current research status [161–165]. Figure 3 presents the year-wise distribution of publications to illustrate the proliferation of blockchain research in the last 5 years [162]. As shown in Fig. 3, the number of blockchain papers is increasing rapidly in recent years. As the number of published papers in blockchain increases, we can also see an increasing trend in citations year-wise [163–165]. We can see there are only 57 citations in 2016. This is followed by drastic changes in the citations numbers in 2017 and 2018, increasing from 556 to 1246 citations. Further, the number of citations from 2018 to 2019 increases at the double rate for the blockchain articles indexed by Web of Science (WoS) [162].

Similarly, in Fig. 4, we have analyzed the various domain-wise bibliometric studies to identify the current trends in blockchain technology applications [163–165]. According to the research study by Taylor et al. [161], IoT is the most trendy topic in blockchain technology, and most of the research is done in this area [163]. Then, blockchain in cloud storage and sharing is the second most popular topic, followed by healthcare, supply chain, AI,

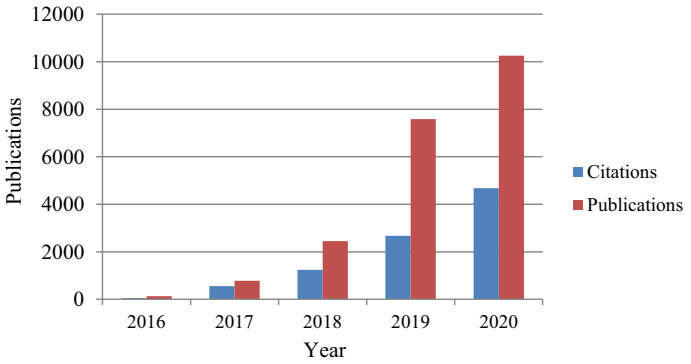


Fig. 3 WoS indexed publications and citations of blockchain

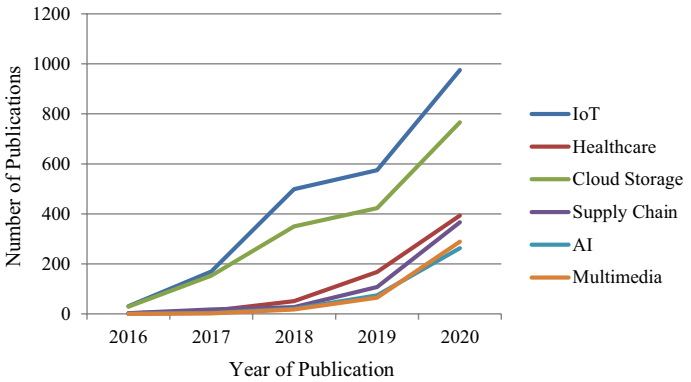


Fig. 4 Application-wise worldwide number of publications

and multimedia. As per the studies, 45% of the blockchain technology research papers are based on IoT, whereas 16% of papers use cloud data storage and sharing system followed by the other domain fields [161–165]. Figure 4 indicates the potential and opportunities of this advanced technology in various application areas. It is showing tremendous growth in IoT, cloud, and healthcare to indicate further improvements. Whereas, for other domain areas such as supply chain, AI, and multimedia, it indicates a baseline for researchers to initiate or bring new blockchain-based projects.

5.2 Proposed Work Research Analysis

The authors have analyzed the research papers related to blockchain and its applications published between 2015 and 2019—the grey research, including draft reports and generic reports extracted from descriptive analysis. The research analysis of descriptive types provides interesting facts about the blockchain, applications, and challenges. The analysis provides depth knowledge about blockchain implementation in different areas. The thematic content was prepared based on two criteria: the content published by type and content published over time. In this paper, year-wise, papers published in various international journals

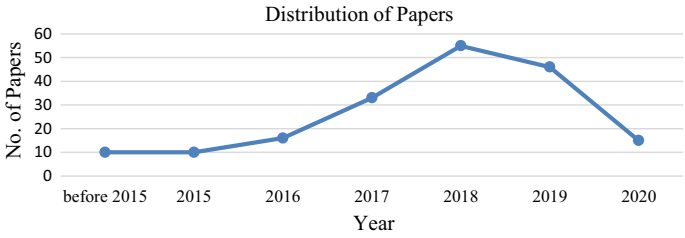


Fig. 5 Number of publications from 2015 to 2020

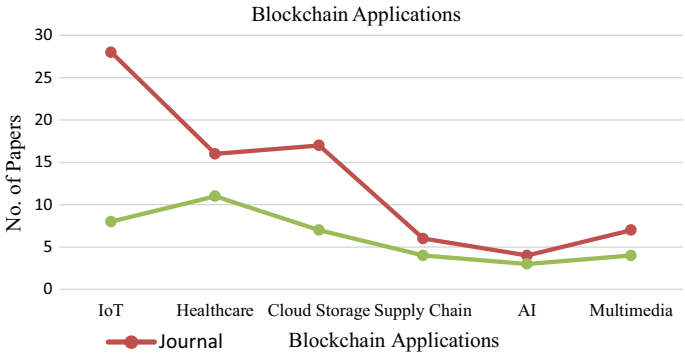


Fig. 6 Blockchain applications wise paper distribution

and conferences are illustrated in Fig. 5. The graph obtained shows that interest in blockchain techniques has risen from the year 2015 onwards. It is also observed that from the year 2015 to date, there is a rise in blockchain applications publications in vivid fields. Figure 6 summarizes the important references that have been referred to in the current review study. It lists the references that published the blockchain applications between the years 2015 and 2019.

6 Blockchain-Based Applications

Blockchain technology has greatly influenced the trade, business, and research sectors. The blockchain-based applications are analyzed based on the following categories, security, data storage, access control, consensus, and smart contracts. The following are some of the solutions offered by the blockchain applications:

Security and privacy: To researchers, the greatest fear is having the year-long study and findings hacked. Similarly, in every sector, the security of online data attracts attention. Thus, the question is how to share the data related to various transactions while preserving data safety. Blockchain answers these questions by adjoining the security of common transactions in social and academic sectors. Blockchain offers a great platform and provides solutions with full attention to security and privacy issues.

Information Storage: Data form an essential part of any organization and enterprise. Reliability issues with data storage can be successfully answered with blockchain

technology. The technology decentralizes the data and provides solutions to manage the data digitally. In the decentralization process, the data are not handled by a single agency and are distributed among numerous blocks. This system of storage is also useful in data management.

Access Control: Access control is a method that regulates access to resources at the system in the computer domain. The existing control systems suffer from many problems, such as third-party interference, inefficiency, and lack of privacy. Blockchain can address these issues, which have received considerable attention in recent years and has several potential benefits.

Consensus: A consensus mechanism is a method by which all blockchain network members reach a shared agreement on the distributed ledger's present state. Thus, consensus algorithms attain durability in the blockchain network and build trust in a distributed computing system between unknown peers. The consensus protocol essentially ensures that every new block added to the blockchain is the only version of the truth accepted by all of the blockchain members.

Smart Contract: A smart contract is a computerized transaction protocol that helps users translate contractual clauses into a coded form, minimizing external risks. It is defined as decentralized scripts that are processed and stored without any requirement of trusted parties and provide a solution for limitless applications. Thus, the applicability of blockchain has rapidly increased [50]. National and international trading requires open collaborations for business growth. Blockchain technology offers a solution to inter-organizational business processes by developing contracts where enterprises can automate the transaction processes without manual confirmation [51].

Figures 7 and 8 list various blockchain applications studied in the present review along with the corresponding references to publications in those fields. These applications have been discussed category-wise in the following section.

6.1 Blockchain and Internet of Things (IoT)

The Internet of Things is an interface of heterogeneous smart devices. The different application areas of IoT are based on a centralized architecture. The centralized system has problems like failure of a single point, trust management, and privacy problems. The blockchain-based architecture for the IoT system connects all devices in a distributed manner and provides a more secure method to share resources or data. As shown in Fig. 9, the centralized architecture of IoT is converted into distributed

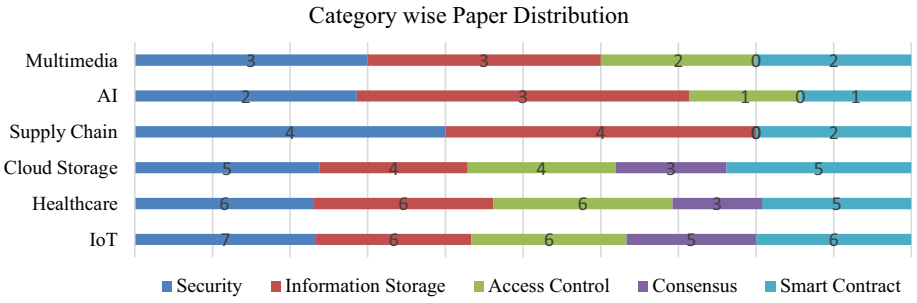
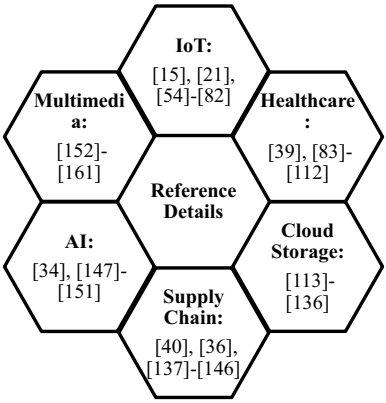


Fig. 7 Category-wise paper distribution

Fig. 8 References details



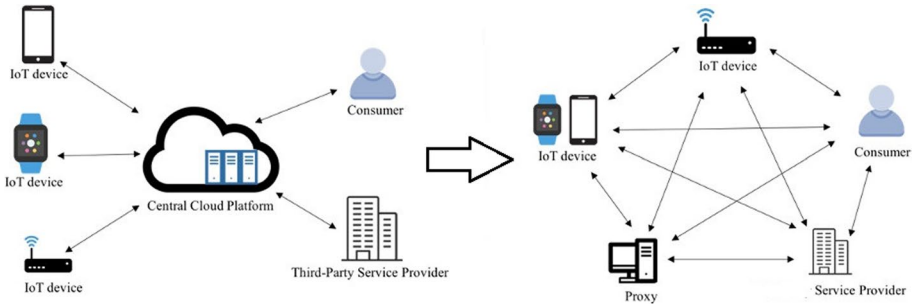


Fig. 9 Centralized and blockchain-based IoT architecture

blockchain-based architecture to resolve the security and single failure problems. The integration of IoT and blockchain technology makes the device robust and tamper-proof. The paper [52] clarified the blockchain-based trust protocol in the IoT scheme. The detailed description of IoT applications and security problems are summarized in [53]. It explained the IoT architecture and described the details of the thread model. In [54], the authors proposed a blockchain-based authentication method for IoT devices that generated zero-knowledge proof to validate the device and used the signature concept for the verification process. Similarly, [55] described the encryption and digital signature methods with IoT model-based applications. In [56], the authors surveyed the industry IoT architecture concepts and analyzed the implementation process's security requirements. The paper [57] described the primary architecture models, communication models, security, and privacy problems of the various IoT applications.

There are many research application areas of IoT by using blockchain. This paper categorized the blockchain-based IoT application into five categories, as shown in Table 4. It presents the category-wise comparative analysis of various applications in the field of blockchain-based IoT systems.

Table 4 Blockchain-based IoT applications

Factor	References	Year	Method	Contribution
Security	[58]	2019	Lightweight, scalable blockchain	Proposed a blockchain-based lightweight, scalable architecture for the IoT system. It used overlay nodes to ensure scalability and reduce overhead. It also proposed a distributed time-based consensus algorithm with blockchain to provide security
	[59]	2020	Lightweight integrated blockchain	Designed an integrated blockchain model deployed in a smart home environment. It utilized overlay networks, certificate less cryptography, and distributed management schemes to verify resource-constrained IoT devices' security and privacy
	[60]	2018	Blockchain-based security management	Introduced blockchain-based security architecture to resolve the security issues of application, network transmission, and perception layer of IoT framework. It utilized a device identification-based key algorithm to guarantee security and reliability
	[61]	2018	Blockchain mechanism for IoT security	Highlighted various IoT environments where the blockchain mechanism provides an important role to ensure IoT security
	[62]	2018	Blockchain-based authentication	Suggested a bubble of decentralized trust architecture to provide robust identification and authentication of IoT devices. It created secure virtual zones (bubbles) to identify the devices and maintain trust between them
Information storage	[63]	2018	IoT devices ownership management	Proposed a blockchain-based architecture for managing the ownership details of IoT devices without a trusted party. It defined the ownership rules with the help of smart contracts
	[64]	2019	Trust management system	A blockchain-based trust management system is deployed to establish trust between IoT devices. It is divided into two layers: the IoT layer and distributed fog layer. The IoT layer provides communication between devices, whereas the fog layer maintains trust values between the devices
	[65]	2020	Blockchain-based data allocation	Suggested a new context-aware data allocation method determining the ranking value of each IoT data request to determine its allocation on-chain

Table 4 (continued)

Factor	References	Year	Method	Contribution
	[66]	2020	IoT device location storage system	Designed a blockchain-based location chain storage system for IoT devices. To provide location privacy service, blockchain technology maintains location information
	[67]	2018	Blockchain-based secure storage	Proposed a blockchain-based threshold system for IoT service called BeeKeeper. The system server used homomorphic computations to process the user's data
Access control	[68]	2015	Attribute-based access control	Proposed a novel access control mechanism for the IoT system. Each device is described using predefined system attributes and assigned by attribute authority as per the identity or ability. Blockchain is utilized to store attributes distribution in the form of a ledger
	[69]	2018	Distributed access control	Designed blockchain-based distributed access control architecture to assign roles and permissions in IoT. It addresses the issues with managing constrained IoT devices by not including them in the blockchain network, thus making integration easier
	[70]	2019	Attributed-based access control	A lightweight and robust access control mechanism is designed to address privacy and security issues for the IoT system. The integration of FairAccess and Privacy-preserving access control provided a more secure environment for the IoT environment
	[71]	2019	Access right delegation	Developed a secure access control model to address delegation issues of the IoT system using blockchain technology. It supports two blockchain networks for transferring the access rights in the IoT framework and also ensures security
	[72]	2017	Hierarchical access control	Proposed a blockchain-based privacy-oriented key management system to achieve hierarchical access control. It combines the blockchain concept with cloud and fog computing to achieve decentralization, scalability, privacy, and access control in the IoT system

Table 4 (continued)

Factor	References	Year	Method	Contribution
Consensus	[73]	2020	Proof of X consensus protocol	Designed a Proof-of-X consensus protocol for the IoT system. It used attributes of the participants of the network
	[74]	2019	Storage compression consensus (SCC)	Proposed an SCC algorithm to compress blockchain in each IoT device to ensure storage capacity
	[75]	2014	Distributed consensus algorithm	Proposed a distributed decision-making consensus algorithm for service detection, processing, classification, and data composition for the IoT system
	[76]	2019	Two-layer consensus algorithm	Designed a blockchain-based two-layer consensus algorithm to optimize the IoT device resource requirements
Smart contract	[77]	2018	IoT-edge framework using blockchain and smart contract	Proposed a blockchain and smart contract-based edge-IoT framework to address security and scalability challenges. It uses a credit-based resource management method to control the resource requirement of IoT devices
	[78]	2016	Blockchain and smart contract for IoT	Provided a detailed description of the integration of blockchain-based smart contracts and IoT system. It identified the potential use cases of the IoT framework with blockchain
	[79]	2018	Smart contract based monetization of IoT data	Proposed a smart contract-based monetization framework in which payment and token access issues automatically to the IoT owner without any third party
	[80]	2019	Auditing scheme with smart contract for IoT	Proposed a decentralized auditing scheme that supports dynamic auditing, public auditing, and batch auditing. Smart contracts are used to store deposits which can pay for auditing and punishment
	[81]	2019	Contract learning approach for resource sharing and task offloading	Introduced two-layer architecture for resource sharing and task offloading in the IoT system. It combined the contract concept with computational intelligence. The first layer uses an incentive method, and the second layer uses a task offloading algorithm to minimize delay in the IoT system

6.2 Blockchain-based Healthcare System

The healthcare system is an information-intensive medical environment where large amounts of data are routinely generated, obtained, and disseminated. Due to the sensitive nature of data and restricting factors such as protection and privacy, storing and distributing this vast volume of data is crucial and significantly challenging [82]. In healthcare, secure information protection has been innovated throughout the last decade through a vast number of platforms, software, and communication technologies, all aimed at improving the security of healthcare records. The first health records of paper were translated into Electronic Health Records (EHRs) [83]. EHRs must be regularly distributed and exchanged by various healthcare centers, doctors, pharmacy manufacturers, and administration to provide a realistic way for a patient's health background to prompt treatment. In the case of a conventional client–server data management healthcare system, each hospital/healthcare center retains its database of sick person medical records; the delivery of EHRs becomes a slow and costly task. Web-based health information monitoring methods [84–86] have been presented previously to solve the accessibility, data usage, single failing point, safety, and security issues in the client–server architecture. There is still a single failure in cloud-based systems, information protection, and the patient's security threat occurring in the platform. Blockchain is a recent development in computer technology. Blockchain technology offers transparent, shared, and digitized ledger. All the entities participating offer shared resources without a single failing point, thereby eliminating the possibility of central point bottlenecks, as shown in Fig. 10.

Many study results have employed the technology to fix the weaknesses in existing EHR. Many research publications [87–91] utilized blockchain to solve health documents' privacy and security issues by maintaining cloud information hash within the blockchain. Several studies either introduce new data encoding/decoding techniques [92–94], or a more modern digital signature method [95], or a protected scheme of information transmission [96, 97] or keys generator method [98] used by the blockchain for health information. The various blockchain-based healthcare applications are summarized in Table 5.

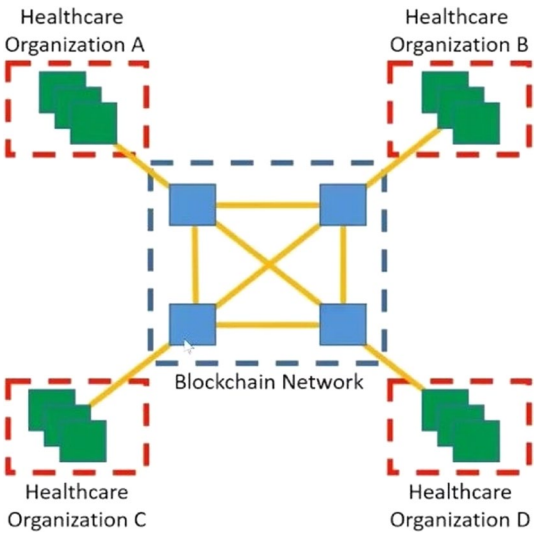


Fig. 10 Blockchain-based healthcare architecture

6.3 Blockchain-based Cloud Storage Service

Cloud computing outsourcing service provides potential benefits to the cloud users. This service addresses the limitations of computationally weak devices by outsourcing their data in the cloud with the help of a pay-per-use approach [112]. The user can rent and pay the storage services or utility computation depending on cloud infrastructure requirements. For the data, confidentiality is vital because of the privacy requirement, and the service provider is not trusted. The researchers' major challenge explored and highlighted is the processing and storing of data into the cloud. The cloud environment and the technology of the blockchain are adapted for this usability. Therefore, for the improvement in existing applications' performance, these two approaches are combined [113]. Hence, blockchain is one of the decentralized or secure networking environments containing several computers called nodes. Furthermore, this technology to improve increases accuracy.

A lot of new technologies and frameworks have been introduced with the current keen interest in blockchain technology. Numerous review articles were published to demonstrate the advantages of blockchain for existing applications. For example, reference [114] provides a detailed overview of privacy and security concerns in cloud computing, covering potential threats and detection methods based on blockchain. Reference [115] presents key concepts of various sharding mechanisms focused on blockchain technology. In [116], the authors address safety, security, and transaction processing issues regarding the use of blockchain for cloud exchange. Moreover, [117] is dedicated to blockchain for edge computing systems and their potential uses. This paper provides a detailed overview of the usage of blockchain technology in cloud computing. From a research point of view, lots of work has been done in the cloud computing field using blockchain; these are summarized in Table 6.

6.4 Blockchain-based Supply Chain

Supply chains are currently becoming extremely complex in structure, challenging in terms of tasks and diverse stakeholders. Several businesses do not have an integrated view of the entire supply chain. Several global companies have developed their own identities and platforms to retain global operational exposure and have the ability to direct their suppliers. They have to focus on centralized administrative or intermediary bodies. In terms of confidentiality, traceability, authentication, and verification method, this low transparency causes many problems and difficulties in the supply chain process. Blockchain is a revolutionary computer technology that can support many possible operations and supply chain-related applications. It is important to notice that blockchain is well suited to the complexities of supply chains. Blockchain technologies can also contribute to the domain of operations and the supply chain [136]. For example, Fig. 11 represents the blockchain-based supply chain management architecture for tracing product details. The architecture utilized a blockchain ledger to store the product details in the form of blocks with the help of smart contracts, and customers are allowed to trace the product by using product RFID code through the mobile application. Thus it is vital to implement blockchain technology, with its immutability, openness, and trustworthiness functionality [137], to have more transparency and security in the supply chain domain. Table 7 summarizes the analysis of supply chain applications that focused on blockchain technology.

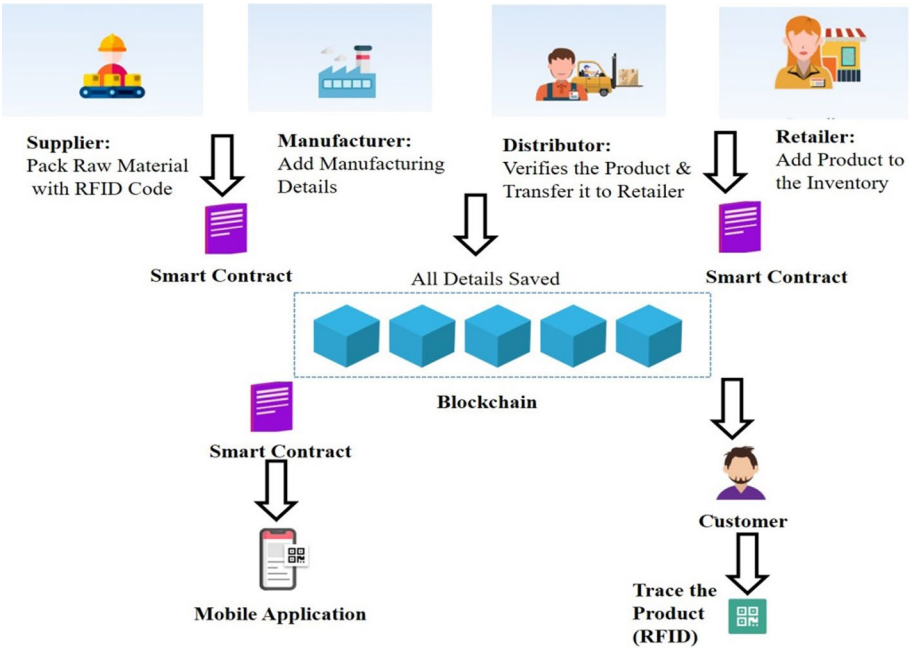


Fig. 11 Blockchain-based product traceability in supply chain system

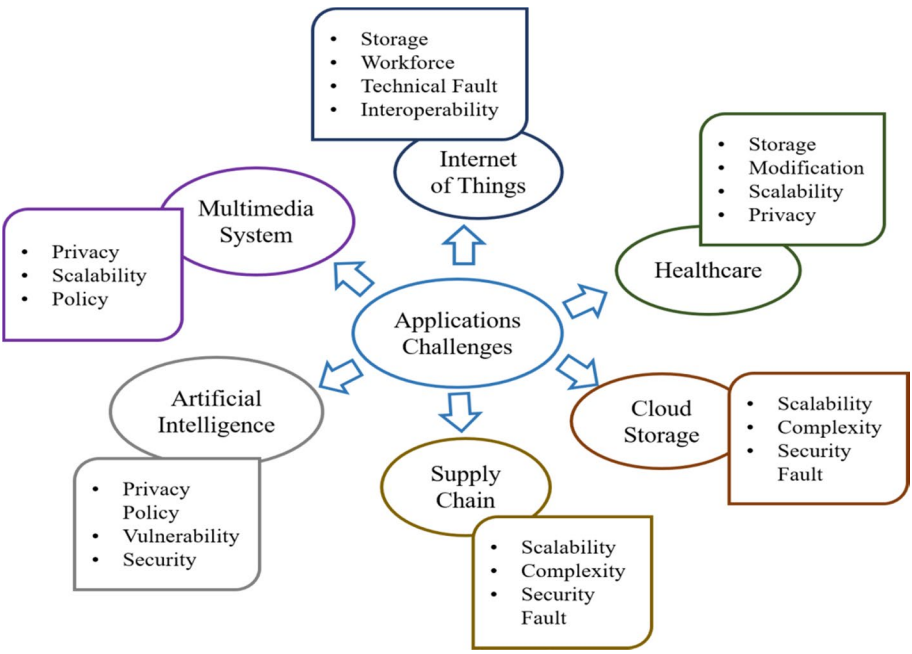


Fig. 12 Challenges of blockchain applications

Table 5 Blockchain-based healthcare applications

Factor	References	Year	Method	Contribution
Security	[99]	2018	Blockchain-based key management scheme	Proposed a solution that integrates the health blockchain and body sensor networks. It designed a lightweight backup and efficient recovery method for the keys of health blockchain
	[100]	2018	Privacy-preserving healthcare data management method	Presented a patient-centric blockchain-based healthcare data management. Cryptographic functions are used to encode the patient's data and ensure privacy
Information storage	[101]	2019	Blockchain-based smart healthcare system	Proposed a secured and smart healthcare system using blockchain to provide security and privacy to preserve the healthcare system
	[102]	2019	Blockchain-based electronic health record	Proposed a Hyperledger based electronic healthcare record sharing system with the use of chain code. It proposed an access control policy algorithm to improve the data accessibility between healthcare providers
	[103]	2020	Off-chain storage of patient diagnostic reports	Proposed a distributed off-chain storage system for patient record management with the help of IPFS storage. It preserves patient privacy and provides accessible healthcare data
	[104]	2019	Mobile cloud-based E-health system using blockchain	Presented the implementation of Ethereum blockchain in a real scenario with a mobile app and Amazon cloud computing. It preserves private health information with smart contracts, access control, security, and privacy features
Access control	[105]	2018	Block-based access control in e-health	Presented a block-based access control method to exchange blockchain-based electronic health records
	[106]	2019	Secure sharing and accessing of medical data	Proposed a MedBloc architecture to allow patients and healthcare providers to access and share data securely. It used encryption and smart contract to regulate access to the records
	[107]	2016	Medical data access and permission management using blockchain	Proposed a MedRec architecture to manage authentication, authorization, and access control method. It used a modular approach to design permission management systems in the healthcare domain

Table 5 (continued)

Factor	References	Year	Method	Contribution
Consensus	[108]	2018	PBFT consensus mechanism in healthcare blockchain domain	Presented a continuous-time Markov Chain model to evaluate the performance of the healthcare blockchain network. It analyzed the factors like mean network delay, primary node delay, and replica node delay
	[109]	2019	IoT healthcare consensus	Proposed a blockchain-based IoT healthcare architecture called IoBhealth that collects the data from IoT sensors. It provided secure access and management of patient data and summarized the various consensus algorithm used in the healthcare domain
Smart contract	[110]	2018	Secure remote healthcare system for hospitals using smart contract	Proposed a remote healthcare system that provides privacy and security of health information with the help of a smart contract. It implemented a processing mechanism to filter the data from the sensors
	[111]	2018	Blockchain and smart contract in decentralized health structure	Presented a decentralized model for the healthcare system. It used a scheme to distribute registered data for the creation of electronic medical records. It also proposed an algorithm for the use of a smart contract in the model

Table 6 Blockchain-based cloud storage applications

Factor	References	Year	Method	Contribution
Security	[118]	2017	Blockchain-based integrity framework	Proposed an integrity checking system using blockchain technology. The designed system allows consumers and data owners to perform trustworthy integrity verification without depending on a trusted third party
	[119]	2019	Privacy and auditing scheme	Suggested an architecture based on blockchain and rank-based Merkle AVL tree structure to provide a privacy-preserving cloud storage environment
	[120]	2019	Encryption based searching	Developed keyword searching technique using public-key encryption method called SEPSE that provides security against keyword guessing attacks. The system allows users to encrypt keywords using the threshold from specific key servers
	[121]	2019	Medical data storage using cloud and blockchain	Designed a blockchain-based architecture to store healthcare data using cloud storage techniques. The system provides security and privacy to the stored healthcare data using blockchain technology
	[122]	2019	Secure healthcare framework using cloud and blockchain	Suggested secure eHealth architecture to provide integrity, correctness, and confidentiality features to the outsourced electronic health records. The healthcare records generated by the doctor during the period were recorded as transactions in the blockchain structure

Table 6 (continued)

Factor	References	Year	Method	Contribution
Information storage	[123]	2019	Decentralized storage	Proposed a provenance information storage system using blockchain technology and IPFS (InterPlanetary File System) with validity checking options
	[124]	2019	Blockchain-based on-chain and off-chain storage	Designed an auction-driven reward system with on and off-chain storage facility using blockchain technology. The proposed system was designed using hyperledger fabric to provide security to the on-chain data, whereas the auction system assessed the off-chain data performance
	[125]	2017	Distributed storage	Suggested a reliable distributed BlockDS system to provide searching and storage services using blockchain technology
	[126]	2018	Distributed cloud storage	Introduced a distributed blockchain-based cloud storage architecture that allows users to divide their data into multiple encrypted chunks and store them randomly to a P2P network
Access control	[127]	2018	Role-based access control	Implemented a role-based access control technique using smart contracts to provide a trans-organizations information sharing system
	[128]	2019	Access control based decentralized method	Designed a blockchain-based distributed system to secure cloud data using the access control method. The proposed work utilized the conventional attribute-based encryption technique using Ethereum smart control concept. It provides a distributed environment that is independent of central authority and a trusted third party
	[129]	2018	Fine-grained access control	The proposed system combines the attribute-based encryption technique with the Ethereum blockchain network. The system using the decentralized storage system IPFS to store the encrypted user data in an off-chain manner. The data owner shared the secret key with the user and specified the access policy rules using the fine-grained access control approach

Table 6 (continued)

Factor	References	Year	Method	Contribution
Consensus	[130]	2019	Proof of stake consensus method	Designed blockchain-based provenance architecture for the cloud computing environment called as BlockCloud. The suggested system implemented a PoS consensus mechanism to reduce the computational overhead compared to the PoW method
	[131]	2019	Synchronous Byzantine Fault Tolerance consensus algorithm	Suggested a Synchronous Byzantine Fault Tolerance (SBFT) algorithm to provide higher efficiency and maintain data consistency than Byzantine Fault Tolerance (BFT) and Practical Byzantine Fault Tolerance algorithm
	[132]	2019	Proof of Work algorithm using maximum factorization statistics	Discussed a PoW consensus approach for cloud and fog computing by using a statistical method. It used the expectation–maximization and matrix factorization algorithm to reduce energy and memory consumption
Smart contract	[133]	2018	Ethereum smart contract	Proposed Ethereum-based blockchain architecture to control the access and provide storage facility with the help of smart contracts deployed functions
	[134]	2018	Decentralized auditing method	Designed a decentralized public auditing system for the cloud storage environment using blockchain technology. The designed system eliminated the need for third-party auditors required for the auditing service with the help of smart contract functionality
	[135]	2018	Deduplication method using smart contract protocols	Proposed a smart contract-based deduplication approach to store files on multiple servers using blockchain technology without a central authority

Table 7 Blockchain-based supply chain applications

References	Year	Method	Contribution
[138]	2018	Double chain based agriculture supply chain system	Proposed a double chain-based blockchain architecture for the agriculture supply chain system. It supports adaptive rent-seeking and matching between supply and demand of resources
[139]	2019	Blockchain in operations and supply chain	Demonstrated the architecture of the blockchain-based logistics monitoring system using the Ethereum platform
[140]	2019	Blockchain architecture for containerized food chain	Demonstrated the architecture using Hyperledger fabric to provide secure information sharing, enhance process access, and prevent risks in containerized food supply chain systems
[141]	2020	Blockchain-based Indian agricultural supply chain	Investigated the barriers to the adoption of blockchain in the Indian agriculture supply chain. Then, the identified barriers are modeled in the proposed architecture and evaluate the performance
[142]	2017	Blockchain-based supply chain management for information sharing	Suggested blockchain-based information sharing architecture that brings benefits to supply chain management. It also used a homomorphic encryption solution without a third party
[143]	2019	Blockchain-based construction supply chain system for key protection	Designed a blockchain-based private-key distribution framework to preserve key security and recovery. It provides payment security in the construction supply chain by using a key management scheme
[144]	2020	Blockchain-based safety management system in grain supply chain	Designed a multi-storage architecture for the grain supply chain system. It is characterized by data security, reliability, information interconnection, sharing, and whole process tracing features
[145]	2020	Secured information sharing in supply chain management	Proposed a cryptographic key distribution mechanism using a smart contract. It designed a blockchain-based information sharing framework in the pharmaceutical supply chain using a smart contract and consensus mechanism

6.5 Blockchain and Artificial Intelligence (AI)

AI and blockchain prove to be a powerful integration that changes almost every sector in which they are applied. Blockchain and AI collaborate to improve all fields, from food procurement distribution to an automated system sharing health care information. Integrating AI and Blockchain includes many fields like secure AI, decision making, and prediction models. AI can efficiently mine and develop new scenarios through a huge dataset and find patterns based on data behavior. Blockchain effectively supports the elimination of bugs and malicious data sets. New AI-generated classifiers and patterns can be verified using a distributed blockchain network. It may be utilized in any user-based company, such as retail purchases. Information captured from users can be used to create marketing automation through AI and the blockchain infrastructure. Perhaps AI and blockchain's integration produces the most robust technology that enabled the decision-making mechanism in the world, which is practically tamper-proof, offering vital perspectives and decisions. It has several advantages, such as improved business models, transparent systems, smart models, etc. Table 8 lists the various application in the domain of artificial intelligence and blockchain technology.

6.6 Blockchain in Multimedia

Multimedia protection, material rights, music files, pictures, and video/movies become a problem for distributors, creators, and artists [152]. Media processing and dissemination are typically supported by CDs, DVDs, pen drives, or email. One of the most known examples of a security violation being the illegal electronic distribution of multimedia before the scheduled release date, which resulted in a major loss for the show's creators and distributors [155]. To avoid these incidences and to identify and convict the individual culprits, it is critical that the media file owner should have full access, permission, and a safe channel to exchange his data [151]. If data were leaked, the owner would be able to claim his rights over the content. Digital technology, such as online cloud storage such as Dropbox or peer-to-peer networking, is the best possible platform for quick and secure data exchange [152].

Multimedia violations over the last few years have raised issues about privacy in this area. Each time a problem is raised, innovations and work are pursued to mitigate it. Therefore, multimedia breaches allow developing alternative solutions that allow customers to save and exchange the data securely. The system should support the owner's authorization and protection controls to track a third party's operation [153]. There are presently many studies underway in this field, and various views and approaches have originated. Many research works have concluded with the owner deliberately disclosing specific information [154]. Even though cloud infrastructure is extremely powerful and more secure than computers, there are many external and internal threats to data integrity. Occasionally there are occurrences of cloud data leakage. It is important to notice that blockchain is well adapted to tackle multimedia issues. Thus, it is significant to implement blockchain technology with its immutability, openness, and trustworthiness functionality to have further protection in this field. Table 9 presents the multimedia applications using blockchain.

Table 8 Artificial intelligence applications using blockchain

References	Year	Method	Contribution
[146]	2019	Integrated blockchain and artificial intelligence solution for autonomous cars	Proposed an integrated solution in which each car is connected to the public ledger and share the experience to learn when to stop. Thus, it eliminates the task of training each car separately
[147]	2019	Blockchain-based intelligent IoT with AI	Implemented an effective big data analysis using blockchain-enabled intelligent IoT architecture. It supports both qualitative and quantitative analysis
[148]	2020	Blockchain and AI for decentralize healthcare system	Proposed a blockchain-based decentralized healthcare system, and AI provided the roadmap for data analysis to discover drug and preventive healthcare
[149]	2019	Decentralized AI model network	Introduced a decentralized AI model to improve the accuracy of machine learning models. It maintained an append-only ledger to store the log of the details of who trains the model and improvement in accuracy
[150]	2019	Securing data using blockchain and AI	Proposed a model to enable secure data sharing, computing, and large-scale sharing with three key components, i.e., blockchain-based data sharing, AI-based computing, and trusted exchange mechanism for security

Table 9 Multimedia applications using blockchain

References	Year	Method	Contribution
[156]	2019	Detection of tempered images using blockchain	Proposed a blockchain-based architecture to register information about ownership and rights of the author and descriptive details of the image to detect a violation
[157]	2019	Blockchain-based video integrity verification	Suggested a blockchain-based approach to combine hash-based message authentication and elliptic curve cryptography to verify the video's integrity
[158]	2018	Multimedia privacy and provenance protection using blockchain	Proposed a blockchain-based multimedia protection framework that enables the users to take full control of data without trusted authority
[159]	2019	Music streaming using blockchain technology	Introduced a blockchain model using Ethereum and IPFS storage to remove delays and transparency problems in the exiting centralized methods
[160]	2019	Global music industry using blockchain	Proposed a novel actor enabled the model to capture the unique properties of digital entrepreneurship

7 Open Issues and Challenges

In this section, we discuss and identify the current challenges associated with combining blockchain technology with different domains as shown in Fig. 12. Despite the exciting advantages and the incredible foreseen potential of blockchain, there are major obstacles in implementing and delivering existing and proposed networks that would require further investigation. Some of the potential challenges faced by blockchain applications are explained in the following subsections.

7.1 Internet of Things

Despite the exciting advantages and the incredible foreseen potential of Blockchain and IoT, there are significant obstacles that would require further investigation:

Restriction with Storage Facility: In the IoT environment, the storage space needed for sensors and devices is less than that of the blockchain ledger. In IoT, strong, unified server storage is enabled, whereas each ledger needs to be stored at each node in the blockchain. Compared to the current capacity in IoT devices, this increases the data size over time.

Workforce Scarcity: Trained workforce for the blockchain platform is very low, and the figure is incredibly small when blockchain is integrated into the IoT concept. This implies that there is a very less-skilled worker who knows about the blockchain-integrated IoT concept.

Variation of Computational Capabilities: IoT networks are distributed and linked over a large network; this structure becomes more complicated when the blockchain is combined with IoT. It is essential that all things connected to the blockchain-based IoT system run the encryption. In such cases, not all of the algorithms used to run the encryption may have similar computing capabilities, thus results in variation problems.

Complex Technical Challenges: The challenges related to scalability, safety, cryptographic implementation, and reliability specifications of novel blockchain-based IoT applications still need to be addressed. Additionally, blockchain systems face design drawbacks in communication efficiency, authentication protocols, or smart contract implementation, which require further investigation.

Interoperability and Standardization: To achieve complete interoperability and the implementation of blockchain in IoT would require the cooperation of all stakeholders and the integration of existing systems. It will require collaborative applications and international standards to protect access control, authentication, and authorization.

7.2 Healthcare

While there are various advantages offered by blockchain technology, some inherent disadvantages pose some challenges. Storage, scalability, alteration, safety, and policies are the primary healthcare issues facing this technology.

Storage: Healthcare and medical records generate massive volumes of data from the patient and wearable IoT devices. While the blockchain architecture enables limited data storage, various operations on blockchain data are also expensive if the data size is larger. Thus, this factor should be considered while designing a blockchain application.

Modification: On the one hand, blockchain data immutability features to protect the system, but on the other hand, it does not provide the data updating and deleting operation. Either there is a need to build a new block out of all nodes by consensus or create a new

chain. These two approaches are expensive and not beneficial. Therefore, the development of blockchain applications must be the lowest need to modify the data.

Scalability: The scalability problem is less severe because of the decentralized architecture. Nevertheless, there are millions of customers of various networks, including healthcare centers, business research agencies, insurance providers, patients, IoT businesses, etc. It is highly unlikely that they will all be able to maintain the same blockchain distributed structure. Blockchain also requires high computing capacity that needs high network equipment electricity consumption. To make blockchain popular, the healthcare scalability issue needs to be considered seriously.

Privacy and Regulations: Blockchain significantly increases the confidentiality of the data. Cryptographic, open, autonomous, and immutable blockchain features can ensure complete protection of the information. Healthcare data is all about storing confidential patient information. In contrast, it can be dangerous to have a copy of such data in each node which requires further consideration.

7.3 Cloud Storage

Although blockchain provides disrupting services to a cloud environment, its development still suffers from various vital complexity, scalability, and security issues. Here are a few reasons why blockchain is not quite ready for large-scale usage cloud application needs.

Scalability: The existing blockchain networks have extreme bottlenecks in scalability, with minimal availability, power, and cost. Due to block size constraints, many blockchains have lengthy processing periods for transactions to be appended onto the chain. Hence the block creation time is rapidly increasing, limiting the overall throughput of the system. Additionally, if all transactions are stored in a chain, this increases the blockchain's capacity. Considering complicated cloud computing environments, consumer data is massive, leading to exponential growth in blockchain size, making it impossible to handle large data volumes. Because of these constraints, many application developers do not consider blockchain a viable option for large-scale industries.

Complexity: In the blockchain-based cloud environment, cloud users execute the consensus algorithm to process the complicated mathematical puzzles that need powerful computing hardware to implement transaction validation. However, due to cloud infrastructure limitations, this is difficult to fulfill these specifications. Also, the blockchain process's complexity can cost expensive energy and human capital resources for devices with relatively small processing capabilities.

Security Fault: The main blockchain disadvantage is an unavoidable security flaw. When more than half of the computers operate as blockchain nodes to monitor processing resources, attackers can change consensus structures and keep new transactions from having permission for malign access. It is also called an attack of 51 percent. Blockchain can be at risk of a data breach and system damage without having comprehensive management of transactions.

7.4 Supply Chain

The following lists some of the potential challenges of a blockchain-based supply chain system:

Privacy: Concerning technological problems and specifications, a primary concern is data protection and consumer security. This, along with the drawbacks of IT infrastructure,

particularly for medium-sized businesses, are the main technical factors that cause resistance among market participants and make them hesitant to apply blockchain technology to their use cases. The researchers explore the features and criteria of the possible blockchain systems specifically for supply chain integration, mainly between companies. They point to the inefficiency of the current status of businesses and analyze the expected requirements and functionalities of supply chains offered by the blockchain network.

Scalability: The major concern is the scalability problem of blockchain technology, which reduces the transactions and data that can be handled and controlled in a limited time with the available technology. Because most businesses are part of large and complicated structures, the present state of blockchain is creating concern about the scale and scope of use cases that can be applied at this time. The need to implement the smart contracts in the system and the constant updates of the digital profiles were identified as critical challenges that impede the usage of blockchain in the supply chain system.

Policy and Regulations: Because of the technology's distributed nature, its success depends heavily on conformance and basic agreement among the various supply chain parties. It also suggests a heavy reliance on blockchain operations and a need for trust between different parties and between businesses and technologies themselves. From a technical point of view, these concerns are appropriate requirements rather than challenges, and it is clear that all of these constraints affect both the industry and the financial sector.

7.5 Artificial Intelligence

This section addresses and describes the emerging problems of integrating AI and Blockchain technology. The following lists some of the conceivable challenges of merging and incorporating both technologies:

Privacy Policy: Public blockchain ledgers facilitate safe and accurate data collection, but the data obtained is publicly available and open to all readers. That can be evasion and a privacy concern. Data privacy can be secured by promoting encryption and providing managed access to private blockchain ledgers. Nonetheless, these private blockchain systems may limit access and transparency to the vast amount of data AI might need to manage and perform reliable and correct decision-making and analytics.

Blockchain Security: Blockchain's distributed ability may suffer from exploitation and misuse. Although blockchain offers effective predictive processing schemes, the blockchain networks are vulnerable to cyber-attacks, such as 51 percent attacks. Depending on the miner's hashing power, the consensus algorithm can be corrupted and can work around a few mining entities that control consensus as a centralized platform. For shared blockchains like Ethereum and Bitcoin, this security issue is more apparent. Private blockchain systems suffer less from this problem, as protocols of consensus between parties are predefined.

Vulnerability of Smart Contracts and Deterministic Implementation: Ensuring that the deployment of a smart contract is bug-free, security breaches, and secure from attacks is crucial. Protecting the coding and details on the network is critical, as they can be susceptible to attack. This can present a crucial problem for distributed AI, in which decision-making algorithms and machine learning are carried out by the mining nodes using smart contracts, in which the execution result is typically not deterministic but somewhat arbitrary and unreliable. This results in an innovative approach for working with provisional calculation and designing consensus protocols for mining nodes to agree on outcomes with a limited degree of reliability, precision or consistency, and extremely fluctuating data content.

Governance: Implementing, designing, and controlling a blockchain structure among various stakeholders and members is complicated. For a private cooperative blockchain, significant problems emerge relating to the blockchain type to be implemented, who administers and troubleshoots the blockchain, which codes the smart contracts, conflict resolution, protocols for off-chain operations, implementation of side channels, and control of side channels. This requires research aimed at developing governance models.

7.6 Multimedia

Blockchain has generated some hype, and it's still under discussion on how the technology can be implemented for mass adoption in the entertainment industry. There is a need to set regulations and standards to maximize the value blockchain can create. The process of introducing new technology is costly and time-consuming.

Blockchain Architecture: A robust platform or network that can satisfy all the criteria for using blockchain in multimedia systems must be built. Many research methods address commitment, privacy, and security depend on policy and controls across domains. The governments, for example, should establish a blockchain structure to provide public interest cases.

Storage: Large quantities of records to be kept at the blockchain nodes due to the number of "transactions" (images, streams, videos, etc.) across all channels of the multimedia system. Conversely, the blockchain model enables minimal on-chain storage of data. Blockchain's distributed and hashed architecture is too expensive to store the data. Similarly, if the size of multimedia is larger, access, maintenance, and functions on blockchain data can also be costly. Hence blockchain applications must be designed with these factors in mind.

Regulations: Absence of legislation, vague advantages, and communication gaps between technical experts and policy-makers are major problems that do not promote technology implementation. Common standards for blockchains still need to be agreed upon. Many potential stakeholders in the multimedia system must approve common blockchain platforms and interoperable blockchain standards.

8 Recent Advances

This section identifies the solutions and recent advances to the identified open challenges and also explores the chances of further improvements.

Storage: To resolve the storage requirement, researchers utilize off-chain storage solutions like bigchainDB, Swarm, IPFS, Filecoin, Sia, Storj, etc. [166]. BigchainDB expands the blockchain features as a big data distributed system increases the throughput with immutability and decentralized blockchain system [167]. Other necessary decentralized storage solutions manage a large amount of data since it is difficult to store them inside the blockchain structure. The decentralized storage system provides a peer-to-peer distributed file-sharing system that increases blockchain-based systems' efficiency and storage capability [166]. The decentralized storage network utilizes the blockchain structure to store the meta details and allow the users to access the information at any time.

Workforce: The demand for professionally qualified blockchain developers is increasing dramatically, whereas the existing blockchain-based domains suffer from a shortage of trained or skilled people. According to [168], the demand for blockchain developers has

increased by 2000% from 2017 to 2020. Therefore it is a major concern in the current scenario for the organizations. The blockchain is still evolving. Thus it requires time for the educational institutions to introduce relevant courses to alleviate the market demand.

Scalability: The recent Blockchain platforms have severe bottlenecks of scalability. Many blockchains have long waiting times to add new transactions, making it difficult to process high volumes of data due to block size restrictions. Also, transaction validation is the key component of blockchain technology that uses consensus protocol to validate the transaction of each block. The computational power required to generate a block depends on the number of transactions in a block, which affects the transactions confirmation times. Thus, the consensus algorithms have a direct impact on blockchain technology scalability. Recent advances such as GHOST [171] utilize the chain selection rule to improve the scalability of the bitcoin network. Bitcoin-NG [169] proposes a new consensus protocol to improve the latency of the transaction. Similarly, the off-chain storage solutions [172] perform the transactions offline and increase the blockchain network bandwidth. Another proposal Litecoin [170], confirms the transactions faster and improves the storage efficiency due to the reduction of block generation time.

Privacy: To increase privacy, the Hawk [173] compiler is designed that stores encrypted transactions. The Hawk translates the generic code into cryptographic primitives to enable transaction anonymity. Similarly, the Enigma [174] solution splits the data into multiple chunks and distributes them into peer-to-peer networks so that no node accesses the data. It uses the distributed hash table to store data references details in a decentralized offline manner. Also, the privacy problem in private blockchain networks resolves by using the private permissioned blockchain structures such as Quorum [175], Hyperledger Fabric [176], a blockchain that utilizes access control and membership functionality.

Security/Technical Fault: The most common 51% attack or majority attack [177] is a significant security concern in blockchain technology. If more than half of the Blockchain nodes act maliciously, they may risk a data breach and prevent new transaction confirmations. The researchers propose many consensus algorithms for blockchain technology to prevent majority attacks. In reference [178], the authors discuss the solo mining incentive or peer-to-peer mining concept to alleviate this problem. Still, the proposed consensus mechanism is susceptible to 51% attacks, specifically those that utilize the centralized consensus among a limited number of users.

Policy and Regulations: The absence of central authority makes blockchain technology suspected of promoting and facilitating illegal conduct. Due to the lack of governance, many countries are developing new regulations to legalize virtual currency and distributed technology [179–181]. The legal implication of virtual currency is a significant concern as it directly or indirectly affects blockchain applications. Thus, the key to increasing confidence in blockchain technology could be requiring governments' or companies' policies and regulations in their development. Current initiatives such as Alastria [182] aim to consider multiple authorities to develop a blockchain-based national regulation system for public notaries, universities, and private organizations. These initiatives allow a legal wallet or account for each person that represents digital proof of possession. This information is used for many services like storing healthcare, cloud, or IoT data legally or trustworthy.

Interoperability: Blockchain applications want to implement interoperability in their platform to create an ecosystem to enable communication between different blockchains. The interoperable blockchain relies on several functionalities like integration with existing systems, request transactions in other systems, conduct transactions with other blockchains, integrating with applications, and provide easy switch between the platforms. Specifically, one blockchain network cannot meet a given transaction's needs in the supply chain, IoT,

healthcare, finance, etc. In reference [183], the authors propose a chain of things platform to provide identity, security, and interoperability in the blockchain-based IoT system. It presents three case studies to focus on interoperability, identity, and security features. The majority of interoperability solutions are based on public blockchain; therefore, there is a need to provide a blockchain solution that provides cross-communication between public networks, private networks, and private and public networks.

Smart Contract Vulnerability: To address the smart contract vulnerability, some tools should be deployed to test smart contracts' vulnerabilities or bugs before deployment to evaluate the smart contracts' security states [184]. In reference, [185], the authors present Hawk a privacy-preserving smart contract that ensures on-chain privacy and cryptographically hides the contract details from the public's view. Similarly, in [186], the authors propose a ChainSpace that gives privacy-preserving extensibility in the smart contract platform. The suggested platform provides a highly scalable and secure platform by using a sharding mechanism with the help of the S-BAC distributed atomic commit protocol.

Modification: In reference [187], authors develop building information modeling (BIM) that allows manipulation of information, data and management flow. It combines BIM as a cloud service to the blockchain network for the big data sharing process. The timestamp concept is utilized to trace and allow modification in history records. Similarly, in [188], the authors design a smart provenance system using distributed blockchain technology that prevents malicious modification in the captured data and utilizes the smart contract concept to record immutable data trials.

Complexity: The blockchain network relies on complex algorithms to provide security and establish consensus on the distributed network. Complex algorithms must run to prove that the user can update the chain, which requires much computing power and cost. Thus, to reduce the complexity of the consensus algorithms utilized in blockchain technology, some alternative consensus algorithms are developed, such as Proof of Stake, Proof of Burn, Proof of Importance, Proof of Capacity, Paxos, etc. That reduces the computational power requirement [189].

Blockchain technology is still a new technology in many domains, and new ways to employ it can still be found and researched. Each blockchain solution or system is formed for a specific platform and designed for a specific goal. Each recent advance or solution to overcome the existing challenges of each domain can be causal for the future direction. For further improvement, certain key issues are found in the above solutions that need to be focused on while using blockchain. These include the issues related to throughput and speed while maintaining the large volume of data, node synchronization issues, risk management problems, security challenges, encryption algorithms security issues, and regulatory-related problems. Although many solutions exist for the above issues still there is a need to provide more optimized, efficient, and reliable solutions for blockchain technology.

9 Conclusions

Blockchain technology is a decentralized, peer-to-peer network and the distributed ledger that is available to all nodes. Since 2008 Bitcoin and Blockchain have been the two most significant innovations in the information system. Numerous applications use blockchain to carry out operations in a trustworthy environment without any trusted authority. This study initially discusses the research method, followed by the introduction of blockchain. Then six applications where blockchain provides a solution to the existing centralized

architecture problems in a decentralized manner are analyzed. Some of the most potential domains have been outlined, such as IoT, healthcare, cloud computing, supply chain, etc. Also, we described the individual features that are mostly required for each application area. This allows the selection of blockchain and the appropriate structuring methods to the application's actual needs.

References

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
2. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation 2*, 6–10.
3. Greenspan, G. (2015). Ending the bitcoin versus blockchain debate, http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate
4. Barker, J. F., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2019). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management 51*, 102029.
5. Coin Market Cap, (2017). Cryptocurrency market capitalizations, https://coinmarketcap.com/.
6. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials 18*(3), 2084–2123.
7. Haferkorn, M., & Quintana Diaz, J. M. (2015). seasonality and interconnectivity within cryptocurrencies–an analysis on the basis of Bitcoin Litecoin and Namecoin. In A. Lugmayr (Ed.), *Enterprise applications and services in the finance Iidustry* (pp. 106–120). Springer.
8. Szabo, N. (1994). Smart contracts.
9. Szabo, N. (1997). The idea of smart contracts.
10. Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation, 2*(1), 28.
11. IBM. (2017). Three ways blockchain explorers chart a new direction, https://www-935.ibm.com/services/studies/csuite/pdf/GBE03835USEN-00.pdf.
12. IBM. (2017). 10 Key marketing trends for 2017, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN.
13. Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. H. (2017). A critical review of blockchain and its current applications. In: 2017 International Conference on Electrical Engineering and Computer Science (ICECOS) IEEE. pp. 109–113.
14. Zheng, Z., Xie, S., Dai, H.-N., & Wang, H. (2016). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services, 14*(4), 352–375.
15. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: a survey on applications and security privacy challenges. *Internet of Things.* https://doi.org/10.1016/j.iot.2019.100107
16. Ali, T., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: problems and recommendations. *IEEE Access* https://doi.org/10.1109/access.2019.2957660
17. Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics* https://doi.org/10.1016/j.tele.2018.11.006
18. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2018.10.020
19. Brandão, A., Mamede, H. S., & Gonçalves, R. (2018). Systematic review of the literature, research on blockchain technology as support to the trust model proposed applied to smart places. In Á. Rocha, H. Adeli, L. P. Reis, S. Costanzo (Eds.), *Trends and advances in information systems and technologies. WorldCIST'18 2018. Advances in Intelligent Systems and Computing*, vol 745, (pp. 1163–1174). Cham: Springer. https://doi.org/10.1007/978-3-319-77703-0_113
20. Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: a literature review. In: IEEE EUROCON 2017–17th International conference on smart technologies IEEE. pp. 763–768.
21. Khan, M. A., & Salah, K. (2017). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computing System, 82*, 395–411.

22. Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: Areview. *IEEE Access, 6*, 10179–10188.
23. Seebacher, S., & Schüritz, R. (2017). Blockchain technology as an enabler of service systems: A structured literature review. In Za S., Drăgoicea M., Cavallari M. (Eds.), *Exploring Services Science. IESS 2017. Lecture Notes in Business Information Processing,* vol 279, (pp. 12–23). Cham: Springer. https://doi.org/10.1007/978-3-319-56925-3_2
24. Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research Applications, 29*, 50–63.
25. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?–A systematic review. *PloS One, 11*(10), e0163477.
26. Sankar, L.S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. In: 2017 4th International conference on advanced computing and communication systems (ICACCS) IEEE. pp. 1–5.
27. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In: International conference on principles of security and trust Springer. pp. 164–186.
28. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., & Felten, E.W. (2015). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In: 2015 IEEE Symposium on security and privacy (SP) IEEE. pp. 104–121.
29. Tsukerman, M. (2015). The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future. *Berkeley Tech LJ, 30*, 1127.
30. Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A brief survey of cryptocurrency systems. In: 2016 14th Annual conference on privacy, security and trust (PST) IEEE. pp. 745–752.
31. Khalilov, M.C.K., & Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Communications surveys &tutorials. pp. 1–1.
32. Conti, M., Sandeep Kumar, E., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3422.
33. Maxmen, A. (2018). AI researchers embrace Bitcoin technology to share medical data. *Nature, 555*(7696), 294.
34. Baynham-Herd, Z. (2017). Enlist blockchain to boost conservation. *Nature, 548*(7669), 523–523. https://doi.org/10.1038/548523c
35. Ahmed, S., & ten Broek, N. (2017). Blockchain could boost food security. *Nature, 550*(7674), 43–43. https://doi.org/10.1038/550043e
36. Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., & Decker, S. (2018). Blockchain for business applications: A systematic literature review. In: International Conference on Business Information Systems. Springer, pp. 384–399. https://doi.org/10.1007/978-3-319-93931-5_28
37. Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: A systematic literature review. In: 19th Annual International Conference on Digital Government Research: Governance in the Data Age. pp. 1–9. https://doi.org/10.1145/3209281.3209317
38. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare, 7*(2), 56. https://doi.org/10.3390/healthcare7020056
39. Lee, J. H., & Pilkington, M. (2017). How the blockchain revolution will reshape the consumer electronics industry [future directions]. *IEEE Consumer Electronics Magazine, 6*(3), 19–23. https://doi.org/10.1109/MCE.2017.2684916
40. Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. H. (2017). A critical review of blockchain and its current applications. In: International Conference on Electrical Engineering and Computer Science (ICECOS). pp. 109–113. https://doi.org/10.1109/ICECOS.2017.8167115
41. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In: Big Data (BigData Congress). IEEE International Congress on IEEE. pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85
42. Mosakheil, & Hayat. J. (2018). Security threats classification in blockchains. Culminating Projects in Information Assurance. 48. https://repository.stcloudstate.edu/msia_etds/48
43. Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. In: Advanced Computing and Communication Systems (ICACCS). 2017 4th International Conference on IEEE. https://doi.org/10.1109/ICACCS.2017.8014672

44. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal, 4*(6), 1832–1843. https://doi.org/10.1109/JIOT.2017.2740569
45. Vyas, C. A., & Lunagaria, M. (2014). Security concerns and issues for bitcoin. National Conference cum Workshop on Bioinformatics and Computational Biology, NCWBCB-2014.
46. Wright, A., & Filippi, P. D. (2015). *Decentralized blockchain technology and the rise of lex cryptographia.* https://doi.org/10.2139/ssrn.2580664
47. Lin, C. I., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01
48. Li, X., Jiang, P., Chen, T., & Luo, X. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems* https://doi.org/10.1016/j.future.2017.08.020
49. Anascavage, Robert, and Davis, N. (2018). Blockchain technology: A literature review. SSRN Electronics Journal
50. Zhao, J. L., Fan, S., & Yan, J. (2011). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation, 2*, 28.
51. Vishnevsky, V. P., & Chekina, V. D. (2018). Robot versus tax inspector or how the fourth industrial revolution will change the tax system: A review of problems and solutions. *Journal of Tax Reform, 4*, 6–26.
52. Shala, B., Trick, U., Lehamnn, A., Ghita, B., & Shiaeles, S. (2019). Novel trust consensus protocol and blockchain-based trust evaluation system for m2m application services. *Internet of Things, 7*, 100058.
53. Aly, M., Khomh, F., Haoues, M., Quintero, A., & Yacout, S. (2019). Enforcing security in internet of things frameworks: A systematic literature review. *Internet of Things., 6*, 100050.
54. Prada-Delgado, M. Á., Baturone, I., Dittmann, G., Jelitto, J., & Kind, A. (2020). PUF-derived IoT identities in a zero knowledge protocol for blockchain. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100057
55. Lee, In. (2019). The internet of things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100078
56. Wang, Q., Zhu, X., Ni, Y., et al. (2019). Blockchain for the IoT and industrial IoT: A review. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100081
57. Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*. https://doi.org/10.1016/j.iot.2018.11.003
58. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A lightweight scalable blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing, 134*, 180–197.
59. Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems, 102*, 1027–1037.
60. Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., & Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering, 72*, 266–273.
61. Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things., 1–2*, 1–13.
62. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security 78*, 126–142. https://doi.org/10.1016/j.cose.2018.06.004
63. Alblooshi, M., Salah, K., & Alhammadi, Y. (2018). Blockchain-based ownership management for medical IoT (MIoT) Devices. In: International Conference on Innovations in Information Technology (IIT). https://doi.org/10.1109/innovations.2018.8606032
64. Frahat, R. T., Monowar, M. M., & Buhari, S. M. (2019). Secure and scalable trust management model for IoT P2P network. In: 2nd International Conference on Computer Applications & Information Security (ICCAIS). https://doi.org/10.1109/cais.2019.8769467
65. Yanez, W., Mahmud, R., Bahsoon, R., Zhang, Y., & Buyya, R. (2020). Data allocation mechanism for internet of things systems with blockchain. *IEEE Internet of Things Journal* https://doi.org/10.1109/jiot.2020.2972776
66. Li, D., Hu, Y., & Lan, M. (2020). IoT device location information storage system based on blockchain. *Future Generation Computer Systems, 109*, 95–102. https://doi.org/10.1016/j.future.2020.03.025
67. Zhou, L., Wang, L., Sun, Y., & Lv, P. (2018). BeeKeeper: A blockchain-based IoT system with secure storage and homomorphic computation. *IEEE Access.* https://doi.org/10.1109/access.2018.2847632

68. Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access.* https://doi.org/10.1109/access.2019.2905846
69. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/jiot.2018.2812239
70. Ouaddah, A. (2018). A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees. *Advances in Computers* https://doi.org/10.1016/bs.adcom.2018.11.001
71. Pal, S., Rabehaja, T., Hill, A., Hitchens, M., & Varadharajan, V. (2019). On the Integration of blockchain to the Internet of Things for enabling access right delegation. *IEEE Internet of Things Journal* https://doi.org/10.1109/jiot.2019.2952141
72. Ma, M., Shi, G., & Li, F. (2019). Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. *IEEE Access.* https://doi.org/10.1109/access.2019.2904042
73. Wang, E. K., Sun, R., Chen, C.-M., Liang, Z., Kumari, S., & Khurram Khan, M. (2020). Proof of X-repute blockchain consensus protocol for IoT systems. *Computers & Security* https://doi.org/10.1016/j.cose.2020.101871
74. Kim, T., Noh, J., & Cho, S. (2019). SCC: Storage compression consensus for blockchain in lightweight IoT network. In: IEEE International Conference on Consumer Electronics (ICCE). https://doi.org/10.1109/icce.2019.8662032
75. Li, S., Oikonomou, G., Tryfonas, T., Chen, T. M., & Da Li, Xu. (2014). A distributed consensus algorithm for decision making in service-oriented internet of things. *IEEE Transactions on Industrial Informatics, 10*(2), 1461–1468. https://doi.org/10.1109/tii.2014.2306331
76. Bai, H., Xia, G., & Fu, S. (2019). A two-layer-consensus based blockchain architecture for IoT. In: IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), pp. 1–6, https://doi.org/10.1109/ICEIEC.2019.8784458.
77. Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., & Zhao, Y. (2018). EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal* https://doi.org/10.1109/jiot.2018.2878154
78. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access., 4*, 2292–2303. https://doi.org/10.1109/access.2016.2566339
79. Salah, K., Suliman, A., Husain, Z., Abououf, M., & Alblooshi, M. (2018). Monetization of IoT data using smart contracts. *IET Networks*. https://doi.org/10.1049/iet-net.2018.5026
80. Fan, K., Bao, Z., Liu, M., Vasilakos, A. V., & Shi, W. (2019). Dredas: decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Future Generation Computer Systems* https://doi.org/10.1016/j.future.2019.10.014
81. Zhou, Z., Liao, H., Gu, B., Mumtaz, S., & Rodriguez, J. (2019). Resource sharing and task offloading in IoT fog computing: A contract-learning approach. *IEEE Transactions on Emerging Topics in Computational Intelligence* https://doi.org/10.1109/tetci.2019.2902869
82. Griebel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., Engel, I., & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC Medical Informatics and Decision Making* https://doi.org/10.1186/s12911-015-0145-7
83. Jamoom, E., Yang, N., & Hing, E. (2016). Adoption of certified electronic health record systems and electronic information sharing in physician offices: United States, 2013 and 2014. US department of health and human services, Centers for disease control and prevention, National Center for Health Statistics, NCHS Data Brief. 1–8.
84. Bahga, A., & Madisetti, V. K. (2013). A cloud-based approach for interoperable electronic health records (EHRs). *IEEE Journal of Biomedical and Health Informatics, 17*(5), 894–906.
85. Fernández-Cardeñosa, G., de la Torre-Díez, I., López-Coronado, M., & Rodrigues, J. J. P. C. (2012). Analysis of cloud-based solutions on EHRs systems in different scenarios. *Journal of Medical Systems, 36*(6), 3777–3782.
86. Zangara, G., Corso, P. P., Cangemi, F., Millonzi, F., Collova, F., & Scarlatella, A. (2014). A cloud-based architecture to support electronic health record. *Studies in Health Technology and Informatics 207*, 380–389.
87. Saravanan, M., Shubha, R., Marks, A. M., & Iyer, V. (2017). SMEAD: Asecured mobile enabled assisting device for diabetics monitoring. In: IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). pp. 1–6.
88. Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). pp. 1–5.

89. Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal, 25*(4), 1398–1411.
90. Juneja, A., & Marefat, M. (2018). Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In: IEEE EMBS International Conference on Biomedical and Health Informatics (BHI), Las Vegas, Nevada, USA, 393–397.
91. Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems* https://doi.org/10.1007/s10916-018-0982-x
92. Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute based cryptosystem and blockchain. *Journal of Medical Systems* https://doi.org/10.1007/s10916-018-0994-6
93. Zhang, X., & Poslad, S. (2018). Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In: IEEE International Conference on Communications (ICC). pp 1–6.
94. Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier blockchain framework for IoT-EHRs systems. *Procedia Computer Science, 141*, 159–166.
95. Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access., 6*, 11676–11686.
96. Zhang, J., Xue, N., & Huang, X. (2016). A secure system for pervasive social network-based healthcare. *IEEE Access., 4*, 9239–9250.
97. Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating health activity data using distributed ledger technologies. *Computational and Structural Biotechnology Journal, 16*, 257–266.
98. Hussein, F., Arunkumar, N., Ramírez-González, G., Abdulhay, E., Tavares, J. M. R., & de Albuquerque, V. H. C. (2018). A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cognitive Systems Research Journal, 52*, 1–11.
99. Zhao, H., Bai, P., Peng, Y., & Xu, R. (2018). Efficient key management scheme for health blockchain. *CAAI Transactions on Intelligence Technology, 3*(2), 114–118. https://doi.org/10.1049/trit.2018.0014
100. Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems* https://doi.org/10.1016/j.future.2018.12.044
101. Tripathi, G., Ahad, M. A., & Paiva, S. (2019). S2HS-a blockchain based approach for smart healthcare system. *Healthcare*. https://doi.org/10.1016/j.hjdsi.2019.100391
102. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications 50*, 102407. https://doi.org/10.1016/j.jisa.2019.10240
103. Kumar, R., Marchang, N., & Tripathi, R. (2020). Distributed off-chain storage of patient diagnostic reports in healthcare system using ipfs and blockchain. In: International Conference on Communication Systems & NETworks (COMSNETS). https://doi.org/10.1109/comsnets48256.2020.9027313
104. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE Access.* https://doi.org/10.1109/access.2019.2917555
105. Zhang, X., Poslad, S., & Ma, Z. (2018). Block-Based access control for blockchain-based electronic medical records (EMRs) query in eHealth. In: IEEE Global Communications Conference (GLOBECOM). https://doi.org/10.1109/glocom.2018.8647433
106. Huang, J., Qi, Y. W., Asghar, M. R., Meads, A., & Tu, Y.-C. (2019). MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data. In: 18th IEEE International Conference On Trust, Security and Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). https://doi.org/10.1109/trustcom/bigdatase.2019.00085
107. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD). https://doi.org/10.1109/obd.2016.11
108. Zheng, K., Liu, Y., Dai, C., Duan, Y., & Huang, X. (2018). Model checking PBFT consensus mechanism in healthcare blockchain network. In: 9th International Conference on Information Technology in Medicine and Education (ITME). https://doi.org/10.1109/itme.2018.00196
109. Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2020). Blockchain for IoT-based healthcare: Background, consensus, platforms, and use Cases. *IEEE Systems Journal* https://doi.org/10.1109/jsyst.2020.2963840
110. Pham, H. L., Tran, T. H., & Nakashima, Y. (2018). A secure remote healthcare system for hospital using blockchain smart contract. In: IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 1–6, https://doi.org/10.1109/GLOCOMW.2018.8644164.

111. Novikov, S. P., Kazakov, O. D., Kulagina, N. A., & Azarenko, N. Y. (2018). Blockchain and smart contracts in a decentralized health infrastructure. In: IEEE International Conference quality management, transport and information security, information technologies (IT&QM&IS). doi:https://doi.org/10.1109/itmqis.2018.8524970
112. Wang, C., Ren, H., & Wang, J. (2016). Secure optimization computation outsourcing in cloud computing: A case study of linear programming. *IEEE Transactions on Computers, 65*(1), 216–229.
113. Xu, C., Wang, K., & Guo, M. (2017). Intelligent resource management in blockchain-based cloud data centers. *IEEE Cloud Computing 4*(6), 50–59.
114. Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges and solutions. *Symmetry*. https://doi.org/10.3390/sym9080164
115. Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J. A., & Liu, R. P. (2019). Survey: Sharding in blockchains. *IEEE Access.* https://doi.org/10.1109/ACCESS.2020.2965147
116. Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H. N., & Imran, M. (2019). Blockchain for cloud exchange: A survey. *Computers & Electrical Engineering* https://doi.org/10.1016/j.compeleceng.2019.106526
117. Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2018). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials* https://doi.org/10.1109/COMST.2019.2894727
118. Liu, Bin, Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. In: IEEE International conference on web services (ICWS). 468–475. https://doi.org/10.1109/ICWS.2017.54
119. Wang, H., Wang, X. A., Xiao, S., & Zhou, Z. (2019). Blockchain-based public auditing scheme for shared data. In: International Conference on innovative mobile and internet services in Ubiquitous computing. Springer, pp. 197–206. https://doi.org/10.1007/978-3-030-22263-5_19
120. Zhang, Y., Xu, C., Ni, J., Li, H., & Shen, X. S. (2019). Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage. *IEEE Transactions on Cloud Computing* https://doi.org/10.1109/TCC.2019.2923222
121. Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems, 43*(1), 5. https://doi.org/10.1007/s10916-018-1121-4
122. Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences, 485*, 427–440. https://doi.org/10.1016/j.ins.2019.02.038
123. Hasan, S. S., Sultan, N. H., & Barbhuiya, F. A. (2019). Cloud data provenance using ipfs and blockchain technology. In: 7th International workshop on security in cloud computing. 5–12. https://doi.org/10.1145/3327962.3331457
124. Chen, W., Chen, Y., Chen, X., & Zheng, Z. (2019). Toward secure data sharing for the IoV: A quality-driven incentive mechanism with on-chain and off-chain guarantees. *IEEE Internet of Things Journal* https://doi.org/10.1109/JIOT.2019.2946611
125. Do, H. G., & Ng, W. K. 2017. Blockchain-based system for secure data storage with private keyword search. In: IEEE World Congress on Services (SERVICES). 90–93. https://doi.org/10.1109/SERVICES.2017.23
126. Li, J., Wu, J., & Chen, L. (2018). Block-secure: Blockchain based scheme for secure P2P cloud storage. *Information Sciences, 465*, 219–231. https://doi.org/10.1016/j.ins.2018.06.071
127. Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-based access control using smart contract. *IEEE Access, 6*, 12240–12251. https://doi.org/10.1109/ACCESS.2018.2812844
128. Wang, S., Wang, X., & Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.2929205
129. Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access, 6*, 38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611
130. Tosh, D., Shetty, S., Liang, X., Kamhoua, C., & Njilla, L. L. (2019). Data provenance in the cloud: A blockchain-based approach. *IEEE Consumer Electronics Magazine, 84*, 38–44. https://doi.org/10.1109/MCE.2019.2892222
131. Zhu, Z., Qi, G., Zheng, M., Sun, J., & Chai, Y. (2019). Blockchain based consensus checking in decentralized cloud storage. *Simulation Modelling Practice and Theory*. https://doi.org/10.1016/j.simpat.2019.101987
132. Kumar, G., Saha, R., Rai, M. K., Thomas, R., & Kim, T. H. (2019). Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. *IEEE Internet of Things Journal* https://doi.org/10.1109/jiot.2019.2911969

133. Sukhodolskiy, I., & Zapechnikov, S. (2018). A blockchain-based access control system for cloud storage. In: IEEE Conference of Russian young researchers in electrical and electronic engineering (EIConRus), Moscow. 1575–1578. https://doi.org/10.1109/EIConRus.2018.8317400
134. Yu, H., & Yang, Z. (2018). Decentralized and smart public auditing for cloud Storage. In: IEEE 9th International conference on software engineering and service science (ICSESS). pp. 491–494. IEEE. https://doi.org/10.1109/ICSESS.2018.8663780
135. Li, Jingyi, Wu, J., Chen, L., & Li, J. (2018). Deduplication with blockchain for secure cloud storage. In: CCF Conference on big data, Springer. pp. 558–570. https://doi.org/10.1007/978-981-13-2922-7_36
136. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*(1), 2.
137. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments, 5*(1), 1.
138. Leng, K., Bi, Y., Jing, L., Fu, H.-C., & Van Nieuwenhuyse, I. (2018). Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Future Generation Computer Systems, 86*, 641–649. https://doi.org/10.1016/j.future.2018.04.061
139. Helo, P., & Hao, Y. (2019). Blockchains in operations and supply chains: A model and reference implementation. *Computers & Industrial Engineering* https://doi.org/10.1016/j.cie.2019.07.023
140. Bechtsis, D., Tsolakis, N., Bizakis, A., & Vlachos, D. (2019). A blockchain framework for containerized food supply chains. In: 29th European Symposium on Computer Aided Process Engineering. 1369–1374. https://doi.org/10.1016/b978-0-12-818634-3.50229-0
141. Yadav, V. S., Singh, A. R., Raut, R. D., & Govindarajan, U. H. (2020). Blockchain technology adoption barriers in the Indian agricultural supply chain: An integrated approach. *Resources, Conservation and Recycling, 161*, 104877. https://doi.org/10.1016/j.resconrec.2020.104877
142. Dwivedi, S. K., Amin, R., & Vollala, S. (2020). Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications, 54*, 102554. https://doi.org/10.1016/j.jisa.2020.102554
143. Xiong, F., Xiao, R., Ren, W., Zheng, R., & Jiang, J. (2019). A key protection scheme based on secret sharing for blockchain-based construction supply chain system. *IEEE Access, 7*, 126773–126786. https://doi.org/10.1109/access.2019.2937917
144. Zhang, X., Sun, P., Xu, J., Wang, X., Yu, J., Zhao, Z., & Dong, Y. (2020). Blockchain-based safety management system for the grain supply chain. *IEEE Access* https://doi.org/10.1109/access.2020.2975415
145. Nakasumi, M. (2017). Information sharing for supply chain management based on block chain technology. In: IEEE 19th Conference on business informatics (CBI). https://doi.org/10.1109/cbi.2017.56
146. Gandhi, G. M., & Salvi. (2019). Artificial intelligence integrated blockchain for training autonomous cars. In: Fifth International Conference on science technology engineering and mathematics (ICONSTEM). https://doi.org/10.1109/iconstem.2019.8918795
147. Singh, S. K., Rathore, S., & Park, J. H. (2019). BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems* https://doi.org/10.1016/j.future.2019.09.002
148. Lobo, V. B., Analin, J., Laban, R. M., & More, S. S. (2020). Convergence of blockchain and Artificial Intelligence to decentralize healthcare systems. In: Fourth international conference on computing methodologies and communication (ICCMC). https://doi.org/10.1109/iccmc48092.2020.iccmc-000171
149. Teerapittayanon, S., & Kung, H. T. (2019). DaiMoN: A decentralized artificial intelligence model network. In: IEEE International conference on blockchain (Blockchain). https://doi.org/10.1109/blockchain.2019.00026
150. Wang, K., Dong, J., Wang, Y., & Yin, H. (2019). Securing data with blockchain and AI. *IEEE Access* https://doi.org/10.1109/access.2019.2921555
151. Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In: IEEE Symposium on security and privacy. pp. 180–184.
152. Bhowik, D., & Feng, T. (2017). The multimedia blockchain: A distributed and tamper-proof media transaction framework. In: 22nd International conference on digital signal processing (DSP), London. pp. 1–5.
153. Torre, I., Koceva, F., Sanchez, O. R., & Adorni, G. (2016). A framework for personal data protection in the IoT. In: 11th International conference for internet technology and secured transactions. pp. 384–391.

154. Farkas, C., & Stoica, A. G. (2004). Correlated data inference. Data and applications security XVII. Springer US. p. 119132.
155. https://en.wikipedia.org/wiki/Game_of_Thrones_(season_7) Retrieved : June, 2018
156. Ghimire, S., Choi, J. Y., & Lee, B. (2019). Using blockchain for improved video integrity verification. . *IEEE Transactions on Multimedia* https://doi.org/10.1109/tmm.2019.2925961
157. Vishwa, A., & Hussain, F. K. (2018). A Blockchain based approach for multimedia privacy protection and provenance. In: IEEE symposium series on computational intelligence (SSCI). https://doi.org/10.1109/ssci.2018.8628636
158. Jnoub, N., & Klas, W. (2019). Detection of tampered images using blockchain technology. In: IEEE International conference on blockchain and cryptocurrency (ICBC). https://doi.org/10.1109/bloc.2019.8751300
159. Chavan, S., Ghuge, S., Warke, P., & Deolek, R. V. (2019). Music streaming application using blockchain. *6th International Conference on computing for sustainable global development (INDIACom)* (pp. 1035–1040). New Delhi.
160. Chalmersa, D., Matthewsb, R., & Hyslopb, A. (2018). Blockchain as an external enabler of new venture ideas: Digital entrepreneurs and the disintermediation of the global music industry. Journal of Business Research.
161. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. R. (2019). A systematic literature review of blockchain cyber security. *Digital Communications Network,* https://doi.org/10.1016/j.dcan.2019.01.005
162. Dabbagh, M., Sookhak, M., & Safa, N. S. (2019). The evolution of blockchain: A bibliometric study. *IEEE Access, 7*, 19212–19221. https://doi.org/10.1109/ACCESS.2019.2895646
163. Kamran, M., Khan, H. U., Nisar, W., Farooq, M., & Rehman, S. U. (2020). Blockchain and Internet of Things: A bibliometric study. Computers and Electrical Engineering, 81.
164. Rejeb, A., Trieblmaier, H., Rajeb, K., & Zailani, S. (2021). Blockchain research in healthcare: A bibliometric review and current research trends. *Journal of Data, Information and Management, 3*, 109–124. https://doi.org/10.1007/s42488-021-00046-2
165. Chang, S. E., & Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access, 8*, 62478–62494. https://doi.org/10.1109/ACCESS.2020.2983601
166. Benisi, N. Z., Aminian, M., & Javadi, B. (2020). Blockchain-based decentralized storage networks: A survey. *Journal of Network and Computer Applications, 162*, 102656.
167. Bigchaindb: The scalable blockchain database powering ipdb., https://www.bigchaindb.com/, 2017.
168. Blockchain trends, https://www.leewayhertz.com/blockchain-trends/
169. Eyal, I., Gencer, A. E., Sirer, E. G., Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA. pp. 45–59.
170. Litecoin, (2018). Retrieved from 2018–02–04 https://litecoin.org/, 2011.
171. Sompolinsky, Y., & Zohar, A. (2013). Accelerating bitcoin's transaction processing, fast money grows on trees, not chains. IACR Cryptology ePrint Archive 881.
172. Decker, C., & Wattenhofer, R. (2015). A fast and scalable payment network with bitcoin duplex micropayment channels. In: Symposium on self-stabilizing systems, Edmonton, AB, Canada, Springer. pp. 3–18.
173. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 839–858). CA, USA, IEEE.
174. Zyskind, G. Nathan, O., Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. arXiv preprint
175. Quorum whitepaper, (2016). Available online: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf.
176. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., & Manevich, Y. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. arXiv preprint
177. Eyal, I., & Sirer, E. G. 2014. Majority is not enough: Bitcoin mining is vulnerable. In: International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, Springer. pp. 436–454.
178. Bonneau, J., Felten, E. W., Goldfeder, S., Kroll, J. A., & Narayanan, A. (2016). Why buy when you can rent? Bribery attacks on bitcoin consensus.
179. Bitlegal, (2017). http://bitlegal.io/.

180. R3, (2018). https://www.r3.com/.
181. Trusted IoT alliance, (2017). https://www.trustediot.org/.
182. Alastria: National blockchain ecosystem, (2018). https://alastria.io/,
183. Chain of things, (2017). https://www.chainofthings.com/.
184. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems. (In press)
185. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on security and privacy (SP). pp. 839–858. doi:https://doi.org/10.1109/SP.2016.55.
186. Al-Bassam, M., Sonnino, A., Bano, S., Hrycyszyn, D., & Danezis, G. (2017). Chainspace: A sharded smart contracts platform. arXiv preprint
187. Zheng, R., Jiang, J., Hao, X., Ren, W., Xiog, F., & Ren, Y. (2019). bcBIM: A blockchain-based big data model for bim modification audit and provenance in mobile cloud. *Mathematical Problem in Engineering, 2019*, 1–13.
188. Ramachandran, A., & Kantarcioglu, M. (2018). SmartProvenance: A distributed, blockchain based dataprovenance system. In: Eight ACM conference of data and application security and privacy. pp. 35–42.
189. Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing System, 14*(1), 101–128.

Ms. Pratima Sharma is a Research Scholar, Department of Computer Science & Engineering at Delhi Technological University, India. Prior to this she worked as an Assistant Professor, at Inderprastha Engineering College, Ghaziabad, for nearly three years. She received the M.Tech. and B.Tech. degrees in Computer Science and Engineering from Guru Gobind Singh Indraprastha University, Delhi, India, in 2013 and 2015, respectively. She developed HoneyDos Application for preventing system from Malicious Packets and Denial of Service Attack Using Support Vector Machine Technique during the Post—Graduation degree. Her research and publication interests include Blockchain Technology, Honeypot, Network Security, Information Security and Data Mining. She has presented papers at International/ National conferences, published articles and papers in various journals.

Dr. Rajni Jindal is working as Professor and Head at Computer Engineering Department, Delhi Technological University, Delhi. She received her M.E. from Delhi College of Engineering. She completed her Ph.D. (Computer Engineering) from Faculty of Technology, Delhi University, Delhi. She also worked as Professor (IT), Dean (Research and Collaboration) at Indira Gandhi Delhi Technical University for women, Delhi for 3 years. She possesses a work experience of around 31 years in research and academics. Her major area of interests are Database Systems, Data Mining, Operating Systems and Compiler Design. She has authored around 140 research papers and articles for various national and international journals/conferences and also 5 books. She is a senior member of IEEE and life member of CSI.

Dr. Malaya Dutta Borah is working as an Assistant Professor in the Department of Computer Science & Engineering at National Institute of Technology (NIT) Silchar, Assam. Her research areas are Blockchain Technology, Data Mining and Cloud Computing. She has authored/co-authored around 45 research papers in International/National Journals/Conferences/Books of repute. She has published 2 patents. She is the Editor of three upcoming edited books (publishers-CRC press, IGI Global and Springer) in the field of Blockchain technology. She is Treasure of IEEE Silchar subsection. She has experience of organising International conferences and workshops. She is a member of IEEE, CSI, ACM and MIR Lab.