Hindawi
Journal of Sensors
Volume 2022, Article ID 9077348, 14 pages
https://doi.org/10.1155/2022/9077348

Review Article

Next Generation IoT and Blockchain Integration

Sarvesh Tanwar,[1] Neelam Gupta,[1] Celestine Iwendi,[2] Karan Kumar,[3] and Mamdouh Alenezi[4]

[1]*Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida, India*
[2]*School of Creative Technologies, University of Bolton, Bolton BL3 5AB, UK*
[3]*Electronics and Communication Engineering Department, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar (Deemed to Be University), Mullana, Ambala, 133207 Haryana, India*
[4]*College of Computer & Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia*

Correspondence should be addressed to Celestine Iwendi; celestine.iwendi@ieee.org, Karan Kumar; karan.170987@gmail.com, and Mamdouh Alenezi; malenezi@psu.edu.sa

Received 15 July 2022; Accepted 11 August 2022; Published 24 August 2022

Academic Editor: Sweta Bhattacharya

The Internet of Things (IoT) refers to the interconnection of smart devices to collect data and make intelligent decisions. However, a lack of intrinsic security measures makes next generation IoT more vulnerable to privacy and security threats. With its "security by design," Blockchain (BC) can help in addressing major security requirements in IoT. Blockchain is an ever-growing list of records that are linked and protected using cryptographic methods. It offers its users the flexibility to conduct transactions with lower costs and faster speeds. Blockchain ledgers are also decentralized and a ledger is maintained at each node in the network. Blockchain's security and adaptability help in making even entire systems on it a much easily task with the benefit of decentralization. BC capabilities like immutability, transparency, auditability, data encryption, and operational resilience can help solve most architectural shortcomings of IoT. In the vision of the Internet of Things, traditional devices are becoming smarter and more autonomous. This vision is becoming reality as technology advances but there are still challenges to be resolved. This is especially true in a security domain like data trust, and with the expected evolution of the IoT in the coming years, it is important to ensure that this great source of data arrives. This paper began with an overview of blockchain and IoT, as well as explore the IoT blockchain application challenges. This article also focuses to review the most relevant tasks to analyse how IoT blockchain can improve and examine current research concerns and developments in the use of blockchain-related techniques and technologies in the context of IoT security in depth. One of the best parts of working or learning about blockchain and its application is the curiosity about how it can impact the things that we have been accustomed to without trying to improve and make things more efficient and productive.

1. Introduction

Recently, the rapid advancement of blockchain technology and digital currencies has had an impact on the financial industry, resulting in the creation of a new crypto economy. These usages are growing with the number of areas such as Internet, banking sector, industry, and medical center security. In addition, IoT [1] has expanded its adoption by the development of urban development around the world. The IoT has evolved into a collection of technologies ranging from wireless sensor networks (WSN) to radio frequency identification. (RFID) is used to identify, exploit, and communicate on the Internet. Today, IoT devices can range from wearables to hardware development platforms to electronic devices. IoT plays an important role in transforming today's cities into smart cities with a wide range of applications that can be used in many sectors of society. Various research [2] reports predict that the number of connected devices will reach 20 to 50 billion by 2020, mainly due to the large number of devices that IoT can deploy.

The IoT envisions a fully connected world where measurable information can communicate and interact with

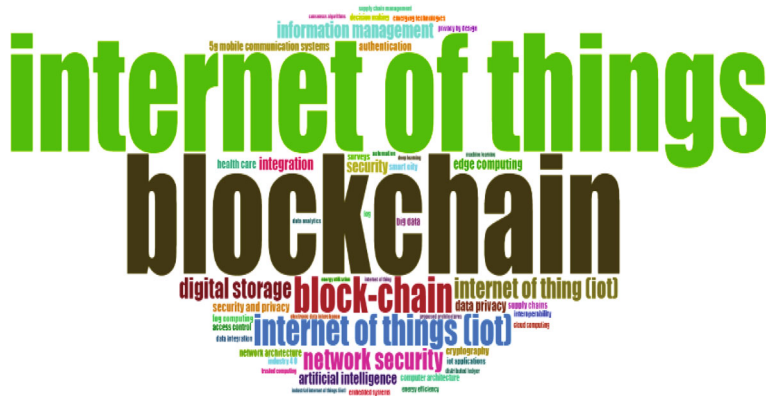


Figure 1: A snapshot of a word cloud built in the research utilizing the most commonly appearing author's keywords.

objects. This allows a digital representation of the real world, and it can develop many smart applications in various industries, including smart home, wearables, smart city, healthcare, automotive, environment, smart water, and smart grid. A screenshot of a word cloud built in the research is utilizing the most commonly appearing author's keywords, as shown in Figure 1. To increase productivity, IoT applications [3] in the digital industry are very clear, generating large amounts of data requires a long connection and energy. Limited storage, compute, networking, and power supply capabilities pose a number of challenges. Standard mechanisms and protocols must support the massive expansion of IoT. This separation has led to a decrease in vertical silos and the adoption of IoT to reduce the diversity present in the region. However, in addition to the diversity and inclusion challenges that exist in the IoT, data credibility is also an important issue to consider when dealing with data from financial and government institutions. But how can we ensure that information received from external parties and other external bodies. IoT companies will not be distorted/altered/falsified in any way? This question is difficult to answer in a centralized architecture [4, 40]. Unreliable organizations may modify the information according to their own interests. As such, the information they provide may be completely uncertain. This raises the need to verify that the data has never been updated. One way to trust IoT data is to use a distributed service that all stakeholders trust to ensure that the data remains unchanged. If all participants have data, there is a way to verify that the data has not been tampered with since it was first defined. Moreover, a system that guarantees the reliability of information will enable governments to securely share and share information with citizens.

The appearance of smart contracts, which are personal computer conventions meant to work with, confirm, and sanction naturally the exchange and arrangement among various deceptive gatherings, has therefore resulted in cutting edge decentralized apps without the involvement of a presumed outsider. Despite the positive aspects of clever agreements, a few concerns, like security risks, flaws, and real concerns, continue to sabotage their acceptance. For over 10 years, the blockchain [5] has been laid out as an innovation where a circulated data set records every one of the exchanges that have occurred in a distributed organization. Viewed as a disseminated figuring worldview effectively beats the issue connected with the trust of an incorporated party. Hence, in a blockchain network, a few hubs work together among them to get and keep a bunch of shared exchange records in a disseminated manner without depending on any confided in party. In 2008, Satoshi Nakamoto presented Bitcoin that was the main proposed cryptographic money presenting the blockchain as an appropriated infrastructural innovation. It permitted clients to safely move cryptographic forms of money, known as bitcoins without a unified controller. In addition, Ethereum, NXT, and Hyperledger Fabric (world greatest open source blockchain made by Linux Establishment in which organizations like IBM were a giver) were likewise proposed as blockchain-based frameworks utilized for the digital money [6]. Not at all like Bitcoin, they can utilize shrewd agreements. Blockchain innovation covers conventional agreements by including the terms of arrangements between at least two gatherings, however, outperforms them because of brilliant agreements via computerizing the execution of arrangements in a dispersed climate when conditions are met.

Despite the fact that smart contracts have recently acquired traction, they nevertheless face numerous challenges. For example, due to its re-entrancy weakness, the Decentralized Independent Association (DAO) agreement was controlled to take around 2 million Ether (50 million USD at the time) [2, 7]. Aside from the issue of weakness, brilliant agreements confront a number of challenges, including questions of protection, legality, and execution.

The following paper is represented as follows: Section 2 presents about Internet of Things with IoT security and security using blockchain. The literature review about integration of IoT blockchain and timeline over the last six year is presented in Section 3. Section 4 describes the blockchain and IoT integration with importance of integration. Challenges of integration of IoT in blockchain are presented in Section 5. The final section of the paper includes some concluding observations.

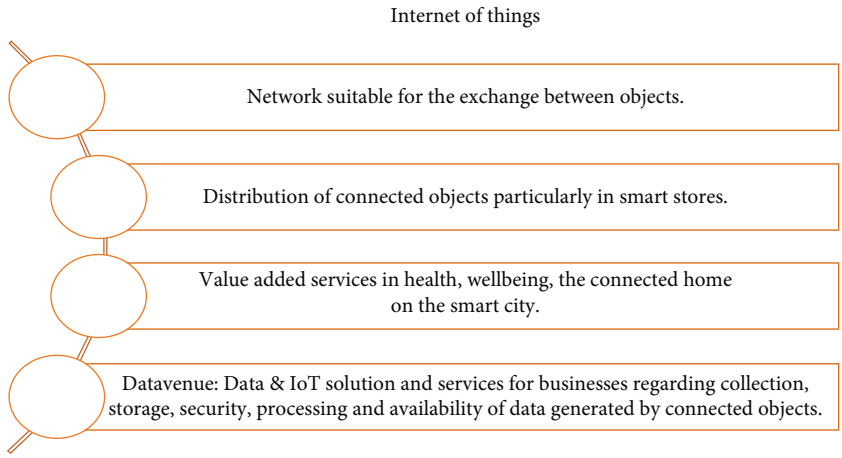


Figure 2: Internet of Things.

1.1. Authors' Contributions. Authors addressed major security requirements in IoT and provided solution by introducing BC capabilities to overcome IoT security issues. Searching relevant documents is an important component of performing a systematic review. This article focused on the review of the most relevant publications in the field of IoT and BC integration. The investigation is based on publications found in the Scopus electronic database to analyse how IoT BC can be improved and examined current research.

2. The Internet of Things

The way we interact with the environment and each other has changed dramatically Internet of Things (IoT) technology is a very widespread technology. It should shape human life. Make big financial gains IoT and blockchain technology can present a variety of challenges. Some IoT devices are sold with built-in functionality to connect to the embedded blockchain [8]. The company responsible for Ethereum allows the use of nodes on devices such as Odroid, Beaglebone, and Ethereum. Raspberry Pi Similarly, EthRaspbian, and Raspnode have the ability to install Bitcoin, Litecoin, and Ethereum nodes on the Raspberry PI. The Raspnode Wi-Fi Router Wallet also supports Litecoin and Bitcoin. Anrouter R-LTC also has this capability. Litecoin is mined, so this router can be easily installed on the IoT network as part of the Fog computing platform. It is still in its infancy and requires a lot of research for further integration. Some IoT devices also have a mining function. Not all IoT devices have this capability. Because it requires high-end hardware and invalidation on IoT devices, IoT mining is often not found to solve these challenges. The Internet of Things (IoT) offers a multitude of aspects of life. Our daily life is strongly influenced by the many applications in areas such as healthcare and manufacturing. IoT plays an important role in transforming homes into smart homes and cities. Blockchain has to deal with many inherent complexities of IoT [9] to become a smart city. Isolated integrating blockchain with IoT will build trust between customers and devices and reduce costs such as cutting out middlemen. Transactions will be much faster, and for blockchain integration to work primarily for IoT purposes, it is necessary to connect some aspects like scalability. Collaboration security requires transcending blockchain into the IoT. Blockchain is for them to harness the power of each other. Blockchain and IoT are interdependent and evolving. Blockchain is an opportunity provided by IoT, and IoT is essential to the functions of blockchain exist. Blockchain provides a service layer for integration with standard IoT frameworks. In general, frameworks play three main roles: sensors, miners, and agents. IoT sensors receive data and interact with services using blockchain agents. The sensors are not integrated with the blockchain function [10]. Transactions in the form of sensory information can be interpreted and then transmitted over a network. These agents also provide security through the use of private keys. IoT devices do not have this security. Network miners use the main function of the blockchain to verify transactions and place them in blocks.

The Internet of Things, as shown in Figure 2, is made up of devices that generate, process, and share massive volumes of security and safety-critical data as well as privacy-sensitive data, making them attractive targets for cyberattacks [43]. Many of the new networkable devices that make up the Internet of Things [11] are low-power and lightweight. These devices must concentrate the majority of their available energy and processing to executing core application functions, making it difficult to enable security and privacy in a cost-effective manner. In terms of energy usage and processing overhead, traditional security methods are often too expensive for IoT. Furthermore, because of the difficulty of scale, the many-to-one nature of the traffic, and single point of failure, many state-of-the-art security frameworks are extremely centralized and hence are not necessarily well-suited for IoT.

2.1. IoT Security. Notwithstanding the benefits provided by IoT services, where IoT technology is successfully implemented on lamps, refrigerators, air conditioners, washing machines, wristwatches, mobile phones, etc., managing IoT [12] communications has become a challenge. A large number of IoT devices can be installed anywhere the end-user

Table 1: Entities and methods enforcing security and privacy properties in different tiers.

Properties	Smart home	Overlay network	Cloud storage
Identity and authentication	Ledger of transaction	Signatures	Block-number along with hash
Access control	Policy header and transactions in BC	Multiset transaction	Block-number with hash
Protocol and network	Encryption	Encryption	Encryption
Privacy	Not-private	PK or ID	Block-number along with hash
Trust	Predefined	Verification	Signed hash of data
Nonreputation	Encryption	Signatures	Signed hash of data
Policy enforcement	Policy header	PK lists	Accounting
Authorization	Policy header and transactions	List of keys	Accounting
Fault tolerance	Medium	High	Low

wants, leaving them unattended and being a desirable target for others to attack. In addition, manufacturers do not consider the security of these devices because of the large-scale deployment of IoT devices. For bulk-manufactured devices, default usernames and passwords are the same. Many IoT devices are shipped with a preprogrammed key that cannot be changed. In addition, IoT networks are heterogeneous and dynamic in nature, allowing various (untrusted) devices to indefinitely join the network. In the event of a hack, device intentions may differ during connection time, or malicious devices may masquerade as benign. Data integrity is another issue in IoT security. One of the most important IoT applications is the decision support system [3]. The information gathered by the sensors can be used to make timely decisions. As a result, the system must be protected from injection attacks, which attempt to inject false measures and thus influence decision-making.

2.2. IoT Security Using Blockchain. Moving towards decentralized architectures, blockchain technology has gained tremendous attention in terms of addressing security, anonymity, traceability, and centralization. Entities and methods are enforcing security and privacy properties in different tiers of IoT security using blockchain, as shown in Table 1. The security [13] of this technology stems from the use of hash functions to chain blocks to ensure immutability, as well as the use of encryption and digital signatures to secure data. The distributed nature of the blockchain ensures its availability. Enabling blockchain technology in IoT can help to achieve a properly distributed consensus based IoT system that overcomes security issues. Even if this is an ideal match, it is still a challenging endeavor. Most existing blockchain schemes do not work in the IoT ecosystem and cannot meet the specific needs of the IoT. IoT environments are resource-constrained, computationally, power-intensive, and storage-constrained, resulting in high computational complexity, limited scalability, high bandwidth overhead, and high latency blockchain. There are some devices that are not recommended to be use with IoT. This is due to how the Block name manages device identities [14]. The author uses an open source implementation of the Kademlia Distributed Hash Table (DHT) which provides the secure encrypted communication, thus define how devices are used with smart contracts. Fakhri and Mutijarsa built IoT systems with and without blockchain and compared the two approaches. MQTT is a communication protocol used in IoT systems that do not use blockchain. Ethereum was used as a blockchain platform, along with a smart contract, in the other system. The security levels of both IoT systems were evaluated by simulating attacks and observing their security features. The results of the tests showed that the IoT system based on blockchain technology had a higher level of security than the IoT system that did not use blockchain technology. Mik presented a novel hybrid blockchain architecture for IoT, referred to as Hybrid IoT. In Hybrid IoT [15], subgroups of IoT devices, referred to as PoW (proof of work) subblockchains, were created. The connection between the PoW subblockchains was then made using a Byzantine Fault Tolerance (BFT) interconnector framework, such as Cosmos or Polkadot. The authors' work focused on the formation of PoW subblockchains that are guided by a set of metrics, dimensions, and bounds. The performance evaluation validated the PoW subblockchain design according to the guidelines of the sweet-spot. The results showed that the guidelines of sweet-spot help to prevent security vulnerabilities. To provide an IoT network with a scalable and dynamic communication architecture, a dynamic blockchain-based trust system was proposed in. The proposed architecture practically labelled all IoT devices and mapped them as full nodes and lightweight nodes. If the attacker pretends to be a full node, high-level security verification will either catch him or make the attack extremely costly [4]. It is also difficult if the attacker just wants to pretend to be a lightweight node because all history is recorded and the attacker must fake everything all over again each time they try to attack. However, IoT with blockchain topology should not only manage the ID but also protect the information exchanged in the IoT network.

3. Literature Review

Various problems in IoT despite authentication and best methods for incorporating security such as Zhen Ling, Junzhou Luo et al. (2017), Yiling Xu et al. (2017), Chao Gao et al. (2017), Kui Wu et al. (2017), and Xinwen Fu et al. (2017) found that there are numerous challenges that arise when there is an authentication method (2017). The lack of an authentication mechanism in the IoT is the fundamental

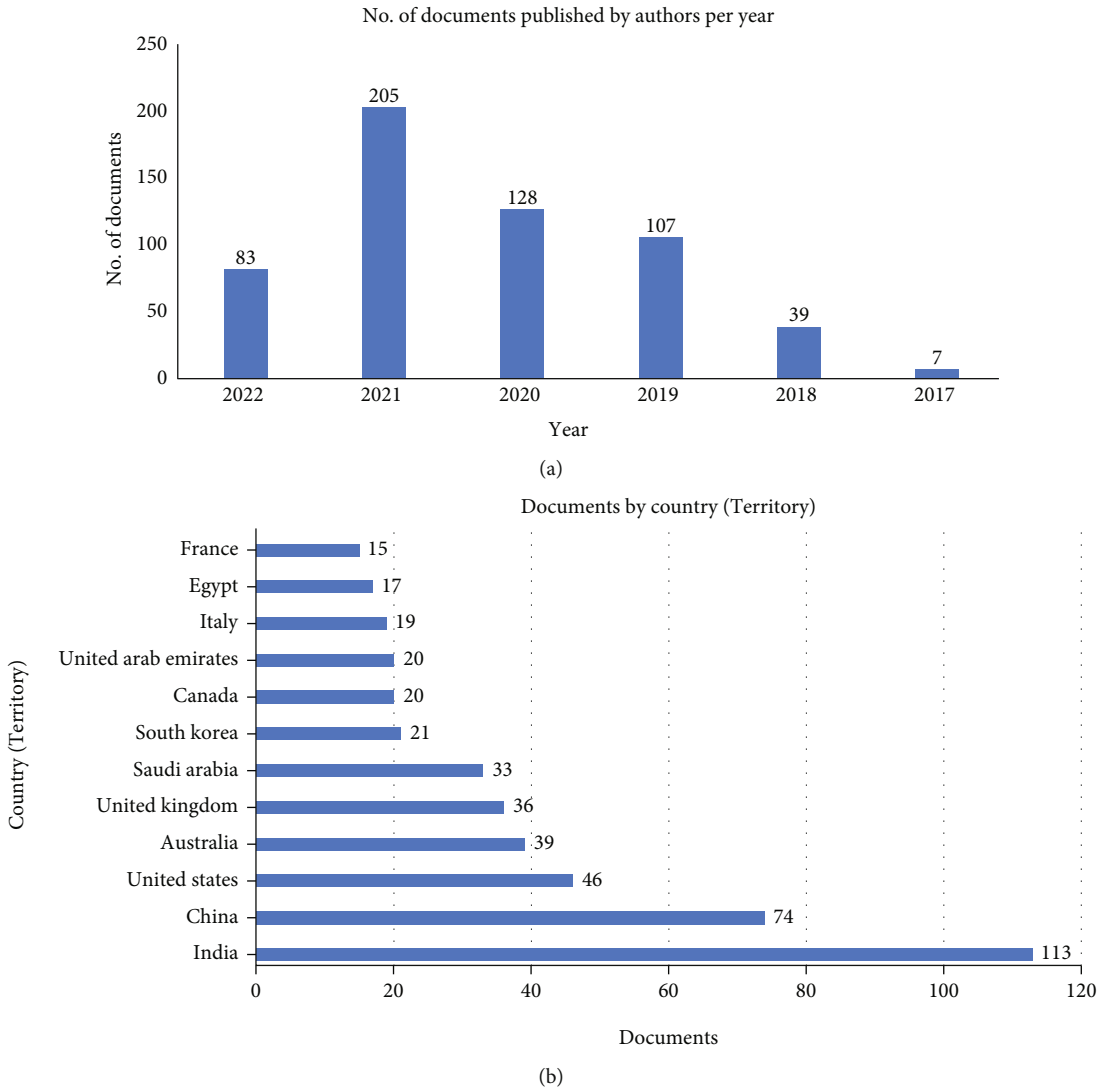
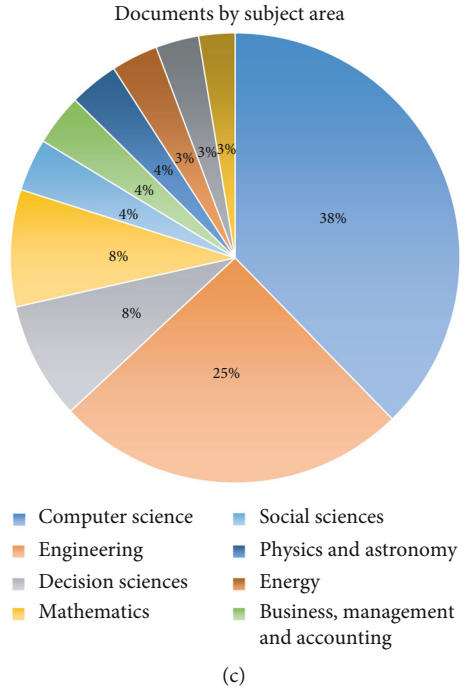


Figure 3: Continued.



(c)

Figure 3: (a) The annual and cumulative numbers of research documents related to blockchain and IoT integration. (b) The country and cumulative numbers of research documents related to blockchain and IoT integration. (c) The subject area and cumulative numbers of research documents related to blockchain and IoT integration.

cause for this. Despite the fact that most IoT [16] apps have authentication enabled, there are security concerns that lead to data loss. Some of the difficulties are as follows. The authors offer a case study on a smart plug system in which they effectively exploit protocols and launch attacks such as brute force, device scanning, firmware assault, and spoofing attack. Their experiments reveal that they are capable of gaining the upper hand.

In the importance of authentication in IoT systems [40], authentication is the cornerstone of providing good security. In IoT systems and m2m applications, a variety of authentication mechanisms are used. These authentication procedures are simple and rely on XOR and hash operations to communicate inside the IoT technology ecosystem [17]. Leakage of critical data is a major concern in many IoT networks Munindar P. Singh et al. (2017) and Muhammad Shahzad et al (2017). The fundamental cause, according to the authors, is that IoT networks lack authentication procedures. The authors suggest alternative approaches for user identification and authorization for IoT networks that lack traditional user interfaces. The authors discuss why authentication is critical in an IoT network. They also [41] provide a solution for overcoming the lack of a traditional user interface for IOT networks.

The search approach should be thorough and objective, as well as simple and repeatable. The search is restricted from 2017 to 2022. The work done on blockchain and Internet of Things integration in the last six years is given below, as shown in Figures 3(a)–3(c).

This investigation is based on publications found in the Scopus electronic database. Searching is an important component of performing a systematic review. In our search, we employed terms such as keywords, title, authors, abstract, references, and index/subject terms, as shown in Figures 4(a) and 4(b). And historiography and average citation per year are shown in Tables 2 and 3. Authors have worked on various next generation IoT and Blockchain Integration concepts for the last seven years, as shown in Table 4.

Table 2 presented historiography based on clustering in Figure 4(b).

Blockchain is an ever-growing list of records that are linked and protected using cryptographic methods. It also offers its users the flexibility to conduct transactions with lower costs and faster speeds. This is presented in Table 3 in the form of citations.

4. Blockchain and IoT Integration

IoT is transforming and optimizing manual workflows to become part of the digital age. By receiving a large amount of information that provides a level of knowledge that has never been heard before, this knowledge facilitates the development of intelligent applications, such as improving the management and quality of people's lives through the digitization of city services. In the past few years [2], Cloud computing technology has contributed to the IoT's essential functions for analysing and processing data and turn them into real-time actions and knowledge. Unprecedented growth in the IoT [18] has opened up new opportunities for communities, such as mechanisms for accessing and sharing information. The open data paradigm is the primary guide to these initiatives. However, one of the most important vulnerabilities of these initiatives which happened in many the situation is lack of confidence. A centralized

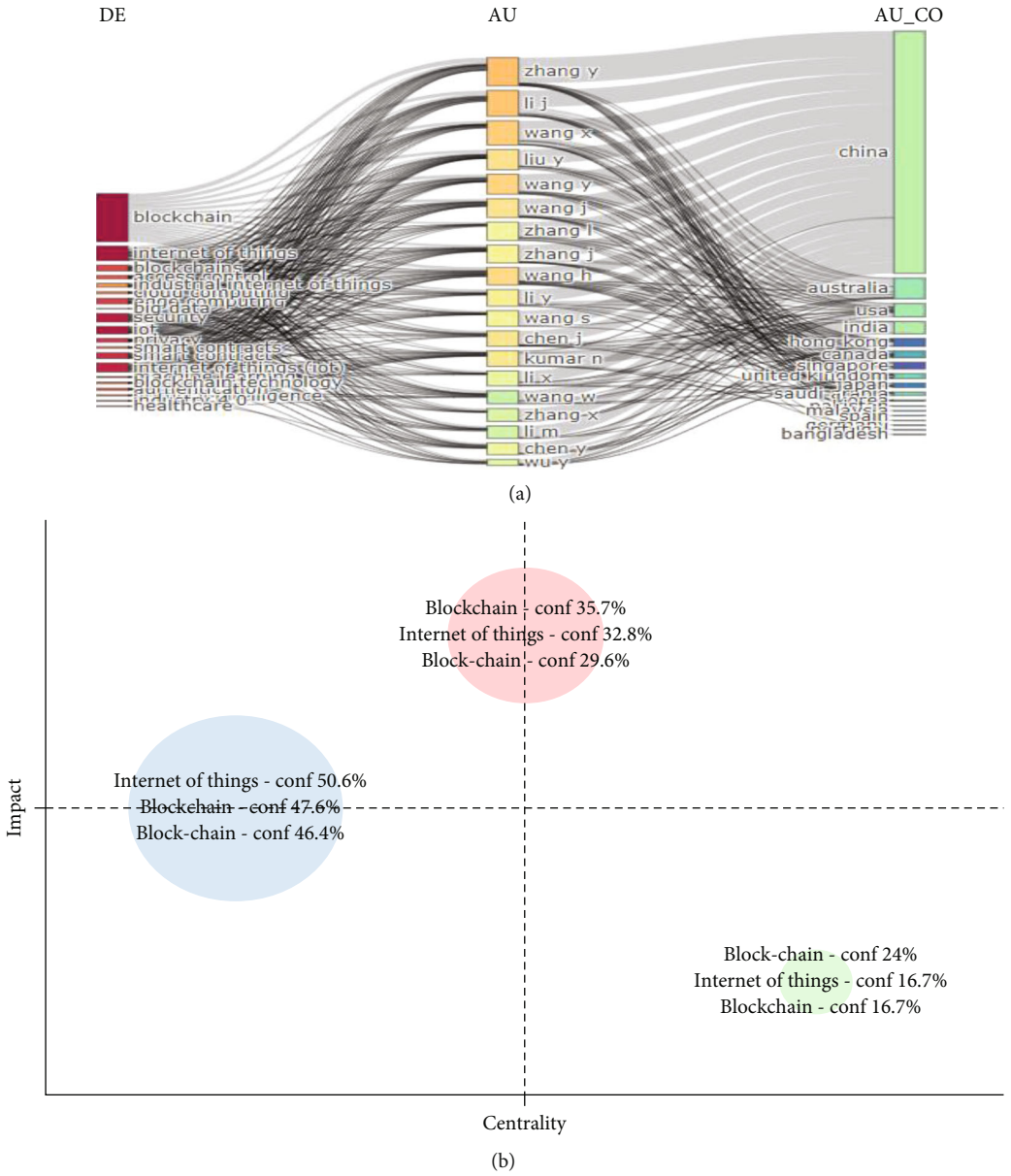


Figure 4: (a) A screenshot of the three fields plot in bibliometric analysis created based on keywords, authors with author's country. (b) Clustering by coupling map.

architecture like the one used in cloud computing is crucial to the development of IoT. They act as a black box, and network participants do not have a clear vision of where and how to use the information they provide.

The integration of promising technologies such as IoT and cloud computing has proven invaluable. In the same way, we recognize the enormous potential of blockchain in revolutionizing the IoT [19]. Blockchain can empower the IoT by providing reliable sharing services. The information is reliable and traceable. The source of information can be identified at any time. And the data will remain unchanged over time. Improve safety where IoT data should be shared securely between large numbers of participants. This integration represents a major revolution. For example, thorough traceability in many food products is a key factor in ensuring food safety. Food traceability may require the participation of a large number of participants: production, feeding, treatment, distribution, etc. A leak in any part of the chain could lead to a breach and slows down the process of finding infections. This can have a devastating impact on citizens' lives and cause enormous economic costs to companies, sectors, and countries. In the event of a food-borne outbreak, better controls in these areas would increase food safety [6, 20], improved sharing of information between participants, reduce search time in case of foodborne outbreaks and saving human lives. In addition, in other areas such as smart cities and smart cars, trusted sharing of information can be beneficial to include new participants in the ecosystem and contribute to improving service and acceptance. Therefore, the use of blockchain can complement the IoT with reliable and secure data. This became known, as mentioned, where blockchain technology was identified as the

Table 2: Historiography.

Paper	Title	DOI	Year	Cluster
Bodkhe, 2020, Trans emerg telecommun technol	Blockchain for precision irrigation: opportunities and challenges	10.1002/ett.4059	2020	1
Li, 2022, Trans emerg telecommun technol	Blockchain as a service models in the internet of things management: systematic review	10.1002/ett.4139	2022	1
Khan, 2021, Electronics (Switzerland)	Reliable Internet of Things: challenges and future trends	10.3390/electronics10192377	2021	2
Guru, 2021, Electronics (Switzerland)	Approaches towards blockchain innovation: a survey and future directions	10.3390/electronics10101219	2021	2
Sadawi, 2021, IEEE access	A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges	10.1109/ACCESS.2021.3070555	2021	2
Tran, 2021, J network comput appl	Integrating blockchain and Internet of Things systems: a systematic review on objectives and designs	10.1016/j.jnca.2020.102844	2021	3
Alkhateeb, 2022, Sensors	Hybrid blockchain platforms for the Internet of Things (IoT): a systematic literature review	10.3390/s22041304	2022	3

Table 3: Average citation per year.

Year	*N*	MeanTCperArt	MeanTCperYear	CitableYears
2018	18	35.78	8.94	4
2019	35	37.71	12.57	3
2020	40	18.07	9.04	2
2021	63	6.27	6.27	1
2022	42	0.74		0

key to solving scalability problems, privacy and reliability associated with the IoT paradigm, increased security, trust and lowering costs were all cited as top benefits of Blockchain/IoT, as shown in Table 5.

From our perspective, IoT can benefit greatly from blockchain functionality and will help to develop the current IoT technology in the future. It is worth noting that there are still a number of research challenges and open issues that need to be explored in order to seamlessly integrate these two technologies, and this research topic is still in its preliminary stages, especially improvements that this integration can bring (but not limited to):

Decentralization and scalability: the transition from a centralized architecture to a distributed P2P removes the center of failure and bottlenecks [21]. It also prevents situations where few powerful companies control the processing and storage of many people. Other benefits along with the decentralization of the architecture is to improve the system's fault tolerance and scalability, and it reduces IoT silos and contributes to further improvements in IoT scalability.

Identity: using common blockchain participants can identify every device. The data provided and entered into the system are immutable and uniquely identifies the actual data provided by the device. Additionally, the blockchain can provide distributed authentication and device authorization for IoT applications. It will represent improvements in IoT and participants.

Autonomy: Blockchain technology powers next-generation application features [22]. This makes it possible to develop intelligent automated assets and hardware as a service. With blockchain, devices can interact without servers involved. IoT applications may benefit from this functionality in application procurement.

Reliability: IoT data remains immutable and distributed over time in the blockchain. System participants can verify the accuracy of the information and ensure that it has not been tampered with. In addition, this technology allows the collection and monitoring of sensor data. Trust is an important part of the blockchain brought by the IoT.

Security: data and communications can be secured by storing blockchain transactions. Blockchains can be used to translate device messages into transactions [23]. Validated by smart contract, in this way, communication between devices is secure. Today's secure standard protocols used in the IoT can be extended with blockchain applications.

Services market: Blockchain can accelerate the creation of the IoT ecosystem of services and data markets. There, transactions between colleagues can be done without employees, and microservices can easily implement and make micropayments. It can be done safely in an unreliable environment. This will improve IoT connectivity and access to IoT data on the blockchain.

Secure code alignment: uses secure, unmodified blockchain storage. The code can be secured and securely inserted into the device [24]. Manufacturers can track status and update with confidence. IoT middleware can take advantage of this capability to securely update their IoT devices.

4.1. Blockchain Technology Solution to IoT. The challenges that IoT systems confront might be solved more effectively with blockchain technology. The number of interacting items or devices in IoT systems is likely to expand in the future. As the number of gadgets increases, they will attempt to communicate with one another, resulting in the internet becoming a medium. Because most acquired data in IoT devices is stored on central servers, this would provide a number of challenges. If devices wish to access data, they must communicate via a centralized network, [8] with data flowing through a central server. Decentralized or dispersed networks with peer-to-

Table 4: Authors have worked on various IoT and Blockchain Integration concepts for the last seven years.

References	Year	Objectives	Future scope
[16]	2016	IoT middleware, cloud platforms, and cloud infrastructures are all surveyed as integration components. Additionally, certain integration ideas and data analytics methods are reviewed, along with various difficulties and unresolved research problems.	Users can choose the essential components depending on their own needs in order to achieve a smooth integration based on the comparisons performed and the aspects examined.
[29]	2017	A test bed is described to compare central and local data processing and highlight benefits of distributing data across multiple locations in a network.	Using test bed, this system offers network saving, real-time processing, intelligent local data processing, and potential local processing mechanisms within the smart grid.
[30]	2018	It discusses several application areas, groups the literature that is now available into these categories, introduces two usage patterns—device manipulation and data management, and provides information on the stage of development of some of the solutions currently available.	The machine economy was created as a result of attempts to commercialise data due to the prevalence of IoT devices and rising data creation. The use of BC to address the issue of data trading and interchange is an example of how this could be applied in the real world.
[34]	2019	Implementation of five privacy-preserving techniques, including privacy protection, encoding, private enterprises, combining, and discrepancy secrecy, in blockchain-based IoT systems.	Before being put into use, blockchain-based IoT devices need to be protected against a number of privacy issues.
[36]	2020	A case study is implemented in a smart IoT system utilizing the Ethereum-based Blockchain technology.	The IoT smart environment is created using sensor devices, and on the Ethereum platform, devices are authorised using the Dec AUTH protocol.
[40]	2021	The suggested BaaU-based framework for trustworthiness in the HIoT systems of the future.	Next-generation healthcare IoT (HIoT) applications may be one of the industries that the blockchain network will likely revolutionize as a technical improvement.
[41]	2022	A cooperative data sharing system where numerous data sources and consumers work together to complete data sharing tasks using cloud-edge computing and blockchain technology.	The outcomes demonstrated that it can be helpful in examining the effectiveness of any blockchain-enabled data sharing system. This will facilitate the successful implementation of efficient data exchange systems.

Table 5: Benefit of implementing integrated IoT with Blockchain networks.

Benefits	1St choice	2nd choice	Sum
Increased security and trust in shared multiparty transactions and data	33%	30%	63%
Increase in business efficiency and lowering costs	27%	29%	56%
Increase in revenue and business opportunities	21%	22%	43%
Improved constituent or participant experiences	19%	17%	37%

peer networking (PPN), distributed file sharing (DFS), and autonomous device coordination (ADC) capabilities are one of the best ways to tackle this [25]. These three roles may be carried out by blockchain, allowing IoT systems to track a large number of linked and networked devices. BC enables IoT systems to coordinate the processing of transactions between devices. BC will improve the security and dependability of IoT systems, making them more resilient. With the support of a distributed ledger, BC enables for speedier peer-to-peer communications.

4.2. Blockchain Scalability in IoT. Blockchain has gained popularity as a result of the use of Bitcoin for online transactions that do not require third-party security. However, the most difficult challenge for blockchain providers is the scalability. Scalability issues must be addressed to integrate IoT and blockchain. On the one hand, because of their sheer number, IoT devices will generate transactions at a rate that current blockchain [10] solutions will not be able to handle. However, owing to resource constraints, it is impossible to implement blockchain peers on IoT devices. Both technologies cannot directly be integrated in their current state [26]. To address the issue of scalability, various techniques such as Segwit, Sharding, block size increase, POS, and off-chain state have been proposed. Segwit, or segregated witness, is a scalability solution that increases the number of transactions in a block while keeping the block size constant. By removing the signature data from the Bitcoin transaction, a segregated witness creates room for new transactions.

Biswas et al. proposed a framework that enables the blockchain ledger to scale across all peers by establishing a local peer network. It limited the number of transactions that enter the global blockchain by implementing a scalable local ledger while maintaining peer validation of transactions at both the local and global levels. The results of the implementation testbed showed that significant improvements in the

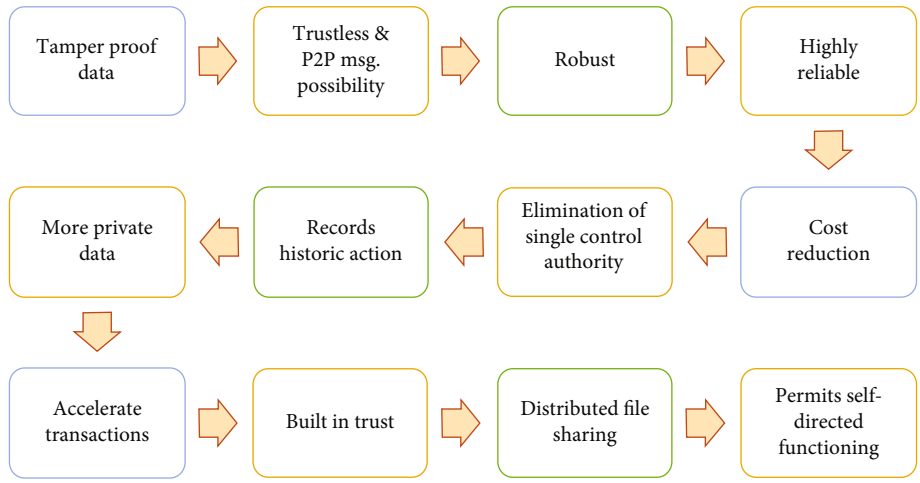


Figure 5: Blockchain technology have the following advantages for large scale IoT systems.

transaction rate and ledger weight were possible. This would improve the scalability of large-scale business transactions in IoT [27] and address the issue of memory requirements for storing blocks. However, the current implementation and evaluation have been carried out in part on virtual machines, with the application written in Node-red.

There are several fields that deploy IoT systems for all the advantage that it provides such as the ability to capture the data and communicate with its peer devices without any human or machine intervention. During these interactions, there is a high possibility of the data leakage. In order to overcome this, there are various methods that are employed to address this area of security.

4.3. Importance of Combining IoT with Blockchain. For industries, IIoT (Industrial Internet of Things) [14] [28] is an inseparable part. Here, people are made mandate for delivering IIoT systems that are secure, general, and scalable. Due to problems like malicious attacks and single point of failure, the existing IIoT systems are unstable in providing services. Although blockchain is a technology that has qualities like security promise and recovery combing IoT, and blockchain is interesting. Most of the IoT devices are power constrained and are not suitable for blockchain though it has low-throughput and less power-intensive. For the purpose of protecting the sensitive data confidentiality, authors came up with a method that regulates the access to sensor data.

In a centralized architecture, there are problems associated with obstacles and the center of failure. Moving to a peer-to-peer architecture solves this problem. Because the storage space is decentralized, small businesses can control and process the data, unlike a centralized architecture where large businesses can control the data [22]. This allows for better fault tolerance and system scalability. The identity of the connected device is important because it can lead to security and reliability issues. All connected devices can be uniquely identified through a single blockchain system. Credentials are also required to identify the data that devices receive. Blockchain also provides authentication for IoT devices.

Many standalone smart devices can be made using blockchain technology, which enables advanced functions to be integrated into smart hardware. Smart devices can also interact with each other without an IoT server. It can be used for modular applications. The system is also reliable as there is no risk of data loss from the blockchain. Users can verify data integrity, and data will remain intact. The system can track and account for data, so reliability is an important factor in integration considerations [15]. The system is also secure as the data is stored as blockchain transactions. This allows you to change the type of transactions monitored by smart contracts. A secure key can be provided to be securely embedded into IoT devices, allowing organizations to secretly track and update devices. It can also create an environment conducive to market exploitation [29]. Transactions between different actors can be done without an agency, and micropayments can be made instantly even if there is no trust between different people. It can improve IoT by providing more blockchain insights.

When integrating a blockchain, it is important to consider whether the devices in the system can interact with each other. A new layer known as fog computing has been added between IoT devices and cloud computing for better integration. Blockchain technology has the following advantages for large scale IoT systems, as shown in Figure 5.

Communication between two IoT devices is fast and secure. They can also work offline and have the ability to communicate with each other using routing techniques, so they do not need a blockchain to communicate. Only a small amount of data is stored in the blockchain. It is used in applications that require minimal delay [30], on the other hand, for communication between the IoT and the blockchain, all data recording all interactions that occur must pass through the blockchain. This ensures that all interactions can be tracked and recorded. In effect, this increases bandwidth usage. Therefore, this can be considered as a major limitation of blockchain. When communicating with hybrid technologies, small units of information are shared with the blockchain. Although the IoT [31] connection is direct, it is difficult to choose which interventions must be carried out during operation by the blockchain. Fog computing, which

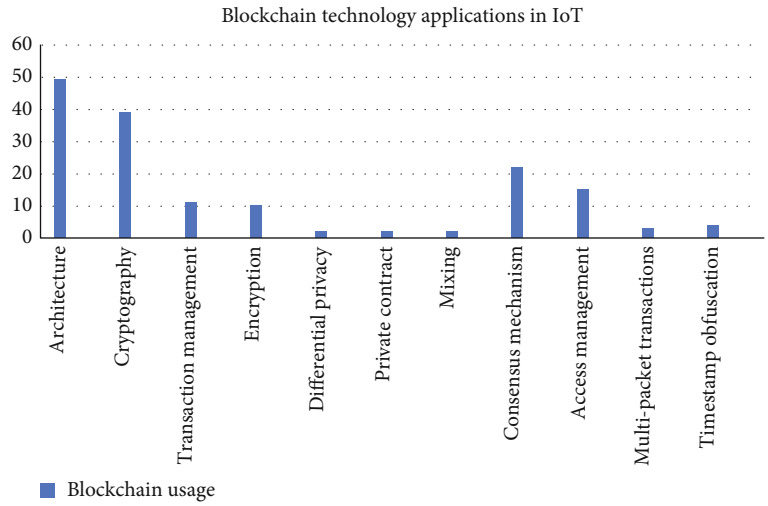


Figure 6: Application types.

uses gateways and other devices for mining, has overcome these limitations, but the use of this technology is growing rapidly. But it is not necessary to use it everywhere. It should only be used for required applications. In general, private use of blockchain may not be suitable for applications that require high performance. However, hybrid techniques may be required to increase efficiency. Wust and Gervais introduced a process that identifies blockchain requirements based on their application.

To facilitate the integration of IoT and blockchain, major companies are teaming up and selling off-the-shelf devices [32]. Some IoT devices are sold with built-in functionality to connect to the EthEmbeddedblockchain, and the company responsible for Ethereum allows nodes to be installed on devices such as Odroid, Beaglebone, and Raspberry Pi. Configure Bitcoins, Litecoins, and Ethereum nodes in the Raspberry PI a. The RaspnodeWiFi Router also supports wallet support for Litecoin and Bitcoin. The R-LTC Anrouter can also mine Litecoin, which makes this router easy to set up. It is still in its infancy and requires extensive research for further integration. Some IoT devices also have mining capabilities. Not all IoT devices have this capability. Since it requires high-quality hardware and is not valid on IoT devices, you will generally not find mining with IoT.

There are other ways to integrate blockchain with the IoT, including integration with cloud computing. Devices have been integrated in this way for many years to address IoT shortcomings such as storage, access, and compute, but cloud computing operates in a centralized framework. It is therefore unreliable and secure when information is shared with specific recipients. Therefore, blockchain is preferred over cloud computing to solve this problem.

4.4. Blockchain Used Because of Its Decentralized Nature in Various Applications. The scattered nature of IoT networks and their huge scale, according to several academics, is a big concern, as shown in Figure 6. Even though, the Decentralized nature of blockchain techniques provide privacy and security, they are not ideal for devices with limited resources due to delays, considerable energy use, and computational overhead. These elements define the smart home tier's different key functions and components [33]. A component called miner is used to handle the home writers' internal and external communications. This component is a high-resource gadget that is always online. Auditing and managing communications are two more responsibilities of the miner. Blockchains retain security goals such as integrity, availability, and secrecy. Because of the different security threats that have been put on the global IoT network, the advantages that may be derived from IoT networks may exceed the risks. Data stored on the central server is subject to DDoS and Sybil attacks, as well as single point failure, which reduces the availability of services and exposes the sensor data stored in the data center.

4.4.1. Potential of Smart Contracts (SC) in Blockchain. SC are well suited for business activities that involve purchase or exchange of goods, services, and rights, especially when frequent transactions occur among a network of parties and manual tasks are performed by counterparties for each transaction [2]. This application is a match for many financial services transactions (e.g., simplifying automatic dividend payments, stock splits and cryptographic signatures on stock certificates, and streamlining over-the-counter agreements). It also [41] describes many supply chain, manufacturing, and retail transactions. However, the technology is still in its infancy, so most use cases of smart contracts today consist of the transfer of cryptocurrency [34] and recording/changing ownership of land or other assets.

4.4.2. Could Blockchain Technology Can Be a Remedy? Yes. The blockchain technology could be one of the remedies for addressing the security and privacy issues in IoT. This is because, the blockchain technology eliminates the central server concept of IoT and allows the data to flow through the blockchain distributed ledger for each transaction with appropriate authentication.

5. Challenges

Storage capacity and scalability—it is still debatable whether blockchain scalability and storage capacity issues are widespread. And in combination with IoT applications, it becomes even more difficult. However, for this reason, Blockchain technology may seem unsuitable for IoT, but the challenges involved can be avoided or completely minimized: some IoT devices can generate large amounts of data [18] [35]. This makes integration difficult. This is because the ubiquitous blockchain cannot handle such large transactions. Therefore, it is beneficial to address these issues before combining the two technologies. Today, only a small percentage of IoT big data is useful for knowledge extraction and production operations. Therefore, many researchers have proposed filtering methods. Normalize and compress IoT data to reduce it. IoT includes devices such as embedded devices and communication devices. This stores the amount of data that the IoT provides to the blockchain. Data compression can reduce the data we transmit, process, and store from the IoT. Finally, negotiated protocols can be used to increase allocated bandwidth and reduce contract latency. This improves the integration between IoT and blockchain.

Security by insufficient efficiency and a large number of uneven devices—security challenges in IoT applications need to be addressed at different levels. Moreover, IoT environments have various characteristics such as wireless communication, mobility, etc. that compound security challenges. A full security analysis has been performed. It is important to build a highly secure IoT. Due to the increasing number of attacks and their severe impact, blockchain is considered the crucial technology to support much-needed security advancements in IoT, but the integrity of data generated by IoT [9] remains a major challenge. By integrating the two technologies, blockchain can ensure that the data transmitted through the chain remains intact and changes can be detected. Therefore, when the data reaches its destination, the corrupted data stays that way. Apart from suspicious sources, corrupted data in IoT [36] can come from many other sources. Factors such as disturbance, device failure, environment, and type of participant play a role in the integrity of the IoT framework. Sometimes, IoT devices do not perform well and are difficult to detect until they are properly secured. Sometimes, it works fine at first and works due to hardware or software issues. Eavesdropping, throttling, or denial of service (DOS) is a major threat that can have a huge impact on the IoT and therefore needs to be addressed. Test it properly before combining it. They must be properly positioned and packaged to avoid physical damage and include an instant device error detection mechanism.

Cost and energy—Blockchain adoption is hampered by a lack of processing capacity. For example, Bitcoin mining necessitates a significant degree of energy to verify and validate exchanges.

Complexity and inactivity—due to the proprietary nature of blockchain-based trades, it may take several hours for all gatherings to update their corresponding records.

Adoption and mindfulness—the lack of attention and reception is one of the most fundamental challenges in blockchain innovation. Many people, for example, have a limited understanding of how it works.

Limitation of capacity and adaptation—as previously said, the storage limit and adaptability of blockchain are still being debated, however, when it comes to IoT applications, the inherent limit and versatility constraints exacerbate these issues. In this respect, blockchain may appear to be unsuitable for IoT applications [37]; however, there are ways to alleviate or avoid these limitations. This constraint addresses a significant barrier to blockchain integration in the IoT, where devices can continuously generate terabytes (GBs) of data. It has been discovered that several existing blockchain operations can only handle a few transactions per second, which could be a bottleneck for the IoT.

Confidentiality and information security—many IoT applications operate with private information, such as when a device is attached to an individual, as in the e-healthcare situation, thus, it is critical to solve the issue of data security and anonymity. Although Blockchain is touted as the greatest solution for addressing the personalities of IoT [38–41] leaders, there may be applications where anonymity is required, similar to Bitcoin. This is the case with a wearable that can hide an individual's identity when delivering personal information, or with clever cars that preserve the security of customers' schedules.

Brilliant agreements—although brilliant agreements have been identified as the ideal application of blockchain innovation, there are still a few issues to be resolved, as previously said. The use of clever contracts in IoT [42–44] might be beneficial, but the way they integrate into IoT applications is different [45, 46].

6. Conclusion and Future Scope

Blockchain aims to revolutionize the next generation IoT. This review has provided a comprehensive overview of the interaction between blockchain technology and the IoT model. Implementing restrictions is important for integrating blockchain and IoT into government infrastructure. This recognition will accelerate engagement between citizens, governments, and businesses. Consensus will play an important role in integrating IoT as part of the process of mining and distributing more blockchains. Research efforts should be made to ensure the security and privacy of key technologies such as IoT and blockchain. One of the biggest concerns about blockchain is that people are taking advantage of this situation, especially in the context of the instability of digital currency. The paper then also went on to explain and chronologically introduce articles on Internet of Things, IoT security using blockchain, Blockchain scalability in IoT, and new challenges and opportunities in IoT and defense mechanisms, as well as using blockchain to ensure confidentiality, authentication, access control, trust, and reputation. Although enabling IoT data security, blockchain has numerous significant problems. For a successful blockchain and IoT integration, an analysis of the key problems of blockchain and IoT integration should be investigated, considering the issues raised in this study. As future work, we

intend to investigate how blockchain, edge computing, and IoT can complement each other in their integration, as well as how edge computing's many security and data integrity issues may be handled by using blockchain technology. Finally, we intend to launch a variety of blockchain applications in the IoT because of blockchain's autonomy to foster the creation of next generation IoT markets. The whole prospect of working on blockchain to maybe one day create something that has never been done before is the motivation behind trying to make this decentralized app.

Data Availability

No data were used to support this study.

Conflicts of Interest

We declared no competing interest exists.

Acknowledgments

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

References

[1] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: applications, challenges, and future trends," *Peer-to-peer Networking and Applications*, vol. 14, no. 5, pp. 2901–2925, 2021.

[2] C. McPhee and A. Ljutic, "Editorial: Blockchain," *Management Review*, vol. 7, no. 10, pp. 3–5, 2017.

[3] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A case study for Blockchain in manufacturing: "FabRec": a prototype for peer- to-peer network of manufacturing nodes," *Procedia Manufacturing*, vol. 26, pp. 1180–1192, 2018.

[4] T. Justinia, "Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences," *Acta Informatica Medica*, vol. 27, no. 4, pp. 284–291, 2019.

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

[6] M. Alharby and A. Van Moorsel, "Blockchain-based smart contracts: a systematic mapping study," 2017, http://arxiv.org/abs/1710.06372.

[7] M. Iansiti and K. R. Lakhani, "Harvard Business Review," *HBR, R1701J, Jan-Feb*, 2017.

[8] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, "Design of the blockchain smart contract: a use case for real estate," *Journal of Information Security*, vol. 9, no. 3, pp. 177–190, 2018.

[9] S. Nakamoto, "Bitcoin whitepaper," vol. 17, no. 7, p. 2019, 2008, URL: https://bitcoin.org/bitcoin.pdf-.

[10] Z. Wang, H. Jin, W. Dai, K. K. R. Choo, and D. Zou, "Ethereum smart contract security research: survey and future research opportunities," *Frontiers of Computer Science*, vol. 15, no. 2, pp. 1–18, 2021.

[11] A. H. Mohammed, A. A. Abdulateef, and I. A. Abdulateef, "Hyperledger, Ethereum and blockchain technology: a short overview," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–6, Ankara, Turkey, 2021.

[12] H. Xiaoting and N. Li, "Subject information integration of higher education institutions in the context of Web3. 0," in *2010 The 2nd International Conference on Industrial Mechatronics and Automation*, vol. 2, pp. 170–173, Wuhan, China, 2010.

[13] M. Hamilton, "Blockchain distributed ledger technology: an introduction and focus on smart contracts," *Journal of Corporate Accounting & Finance*, vol. 31, no. 2, pp. 7–12, 2020.

[14] W. Metcalfe, *Ethereum, Smart Contracts, DApps*, Blockchain and Crypt Currency, 2020.

[15] E. Mik, "Smart contracts: terminology, technical limitations and real world complexity," *Law, Innovation and Technology*, vol. 9, no. 2, pp. 269–300, 2017.

[16] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing," *Journal of Network and Computer Applications*, vol. 67, pp. 99–117, 2016.

[17] J. Rivera and R. Van Der Meulen, "Gartner," *Forecast Alert: Internet of Things—Endpoints and Associated Services, Worldwide*, Gartner, Ed., 2016.

[18] K. Zīle and R. Strazdiņa, "Blockchain use cases and their feasibility," *Applied Computer Systems*, vol. 23, no. 1, pp. 12–20, 2018.

[19] M. A. Engelhardt, "Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector," *Technology Innovation Management Review*, vol. 7, no. 10, pp. 22–34, 2017.

[20] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[21] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, Inc., 2014.

[22] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. WangBlockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[23] N. Radziwill, "Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world," *The Quality Management Journal*, vol. 25, no. 1, pp. 64-65, 2018.

[24] E. Androulaki, A. Barger, V. Bortnikov et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, pp. 1–15, 2018.

[25] J. Kennedy, "$1.4 bn investment in blockchain start-ups in last 9 months, says PwC expert," *Silicon.com*, vol. 4, 2016.

[26] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "{Bitcoin-NG}: a scalable blockchain protocol," in *13th USENIX symposium on networked systems design and implementation (NSDI 16)*, pp. 45–59, 2016.

[27] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.

[28] J. Bhosale and S. Mavale, "Volatility of select crypto-currencies: a comparison of Bitcoin, Ethereum and Litecoin," *Annual Research Journal of SCMS Pune*, vol. 6, 2018.

[29] U. Ahsan and A. Bais, "Distributed big data management in smart grid," in *2017 26th Wireless and Optical Communication Conference (WOCC)*, pp. 1–6, Newark, NJ, USA, 2017.

[30] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: a systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[31] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[32] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in internet of things and AI," *Big Data and Cognitive Computing*, vol. 4, no. 4, p. 28, 2020.

[33] C. Nartey, E. T. Tchao, J. D. Gadze et al., "On blockchain and IoT integration platforms: current implementation challenges and future perspectives," *Wireless Communications and Mobile Computing*, vol. 2021, 25 pages, 2021.

[34] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[35] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021.

[36] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT using blockchain technology," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 881–888, 2021.

[37] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A survey of IoT and blockchain integration: security perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021.

[38] S. K. Lo, Y. Liu, S. Y. Chia et al., "Analysis of blockchain solutions for IoT: a systematic literature review," *IEEE Access*, vol. 7, pp. 58822–58835, 2019.

[39] T. Alam, "Blockchain and its role in the internet of things (IoT)," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 5, no. 1, pp. 151–157, 2019.

[40] A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati, and T. Khurshaid, "Blockchain-as-a-utility for next-generation healthcare internet of things," *CMC-Computers Materials & Continua*, vol. 68, no. 1, pp. 359–376, 2021.

[41] M. M. Mijwil, K. Aggarwal, D. S. Mutar, N. Mansour, and R. S. Singh, "The position of artificial intelligence in the future of education: an overview," *Journal of Applied Sciences*, vol. 10, no. 2, 2022.

[42] S. D. Okegbile, J. Cai, and A. S. Alfa, "Performance analysis of blockchain-enabled data sharing scheme in cloud-edge computing-based IoT networks," *IEEE Internet of Things Journal*, 2022.

[43] A. Alsharef, K. Aggarwal, M. Kumar, and A. Mishra, "Review of ML and AutoML solutions to forecast time-series data," *Archives of Computational Methods in Engineering*, pp. 1–15, 2022.

[44] L. Kakkar, D. Gupta, S. Saxena, and S. Tanwar, "IoT architectures and its security: a review," in *Proceedings of the Second International Conference on Information Management and Machine Intelligence*, pp. 87–94, Springer, Singapore, 2021.

[45] M. M. Mijwil, D. S. Mutar, Y. Filali, K. Aggarwal, and H. Al-Shahwani, "Comparison between expert systems, machine learning, and big data: an overview," *Journal of Applied Sciences*, vol. 10, no. 1, 2022.

[46] S. Tanwar, T. Paul, K. Singh, M. Joshi, and A. Rana, "Classification and imapct of cyber threats in India: a review," in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(I-CRITO)*, pp. 129–135, Noida, India, 2020.