Turkish Journal of Computer and Mathematics Education *Vol.11 No.03 (2020), 2108-2118*
DOI: https://doi.org/10.17762/turcomat.v11i3.13608

Research Article

Blockchain-based IoT Systems: Techniques, Applications, and Challenges

Sushant Chamoli

Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract: The potential for blockchain-based IoT systems to enable secure and effective data sharing in a variety of industries has attracted a lot of attention in recent years. The fusion of blockchain technology and IoT devices can open up new avenues for growth and innovation, but it also comes with a number of serious drawbacks, including issues with scalability, security, interoperability, data privacy, cost, energy use, and governance. This study offers a thorough analysis of the various methods for putting into practise Blockchain-based IoT systems, along with their benefits and drawbacks. In order to address the issues with Blockchain-based IoT systems, we also suggest a hybrid technique that combines the benefits of several techniques. We also cover the important issues that need to be solved as well as the potential uses of Blockchain-based IoT devices. In order to help researchers and practitioners better grasp the current state of the art and the possibilities for further study and development, this paper seeks to provide a thorough review of Blockchain-based IoT systems.

Keywords: Systems, methods, applications, difficulties, hybrid approach, security, interoperability, data privacy, cost, energy consumption, and governance in the Internet of Things (IoT).

I. Introduction

The Internet of Things (IoT), which connects numerous devices, objects, and sensors to the internet, is a fast-expanding sector. These gadgets, which might be basic sensors or sophisticated machines, are used in a variety of industries, including healthcare, transportation, energy, and manufacturing. Data privacy, security, and management are only a few of the important problems that the vast network of linked devices presents [1].As a result, there is now a vast network of interconnected devices that are used in many industries, including manufacturing, transportation, healthcare, and the energy sector. Data privacy, security, and management are just a few of the important problems that this enormous network of linked devices presents.A decentralized, secure, and immutable answer to these problems is provided by blockchain technology. Blockchain technology enables IoT devices to interact and communicate safely while tracking and managing data across numerous networks and devices [2]. This essay examines the methods, uses, and difficulties of blockchain-based IoT systems. The methods employed by IoT systems built on blockchain. Key elements of these systems include consensus processes, decentralized identification, and smart contracts. With smart contracts, the details of the agreement between the buyer and seller are directly encoded into lines of code. These contracts self-execute. Smart contracts can be used in a blockchain-based IoT system to manage and control devices and data as well as to enforce rules and agreements between users. Consensus methods guarantee the consistency and accuracy of the data stored on the blockchain [3]. Consensus techniques can be employed in a blockchain-based IoT system to validate transactions, stop double-spending, and guarantee that the network runs in a decentralized and trustworthy manner. Blockchain is used by decentralized identification systems to safely store and manage digital IDs for IoT users and devices. Decentralized identity can be utilized in a blockchain-based IoT system to

guarantee that only authorized people and devices can access and manage the network.IoT systems built on blockchain and their numerous applications.

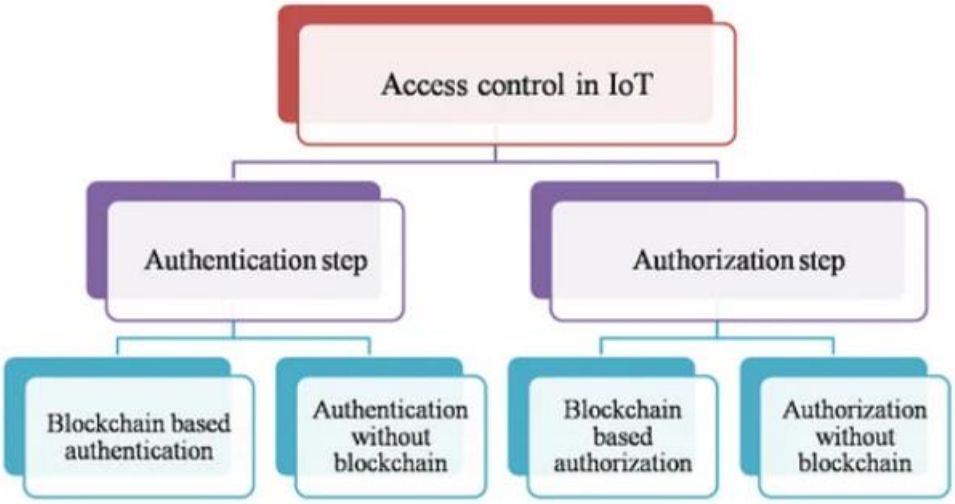

Figure 1. Block Chain Based IoT System

Healthcare, energy management, and supply chain management are three industries where blockchain-based IoT solutions can have a big influence. Blockchain-based IoT systems can track and trace goods and materials across the supply chain in supply chain management, ensuring their legitimacy and integrity. With smart devices that automatically adjust energy usage based on supply and demand, blockchain-based IoT systems can help energy grids become more effective and decentralized in terms of energy management. Blockchain-based IoT devices in the healthcare industry may securely handle and preserve patient medical records and allow for autonomous monitoring of health issues. The difficulties that must be overcome while putting in place IoT solutions based on blockchain [4]. Security, interoperability, and scalability are all major issues that need to be considered. IoT systems built on blockchains can produce a lot of data, which puts a load on the network and slows down transactions. Because there are so many different IoT systems and devices that need to be able to connect with one another, interoperability can also be difficult. Another major worry is security, as poorly secured blockchain-based IoT systems are susceptible to assaults.Blockchain technology is one potential answer to these problems. A decentralized, secure, and immutable answer to these problems is provided by blockchain technology. IoT devices can safely interact and communicate with one another using blockchain technology, and they can track and manage data across numerous networks and devices.Blockchain technology is a distributed ledger system used to manage data over a network of computers and securely record transactions. The blockchain creates an immutable chain of blocks that may be used to track and verify data since each block of data in the blockchain contains a cryptographic hash of the one before it [5]. The blockchain offers a secure and open method of handling data and transactions due to its decentralized nature.Smart contracts, consensus methods, and decentralized identities can all be used in blockchain-based IoT systems to provide transparent and safe communication between devices. With smart contracts, the details of the agreement between the buyer and seller are directly encoded into lines of code. These contracts self-execute. Smart contracts can be used in a

blockchain-based IoT system to manage and control devices and data as well as to enforce rules and agreements between users.Consensus methods guarantee the consistency and accuracy of the data stored on the blockchain. Consensus techniques can be employed in a blockchain-based IoT system to validate transactions, stop double-spending, and guarantee that the network runs in a decentralized and trustworthy manner. Blockchain is used by decentralized identification systems to safely store and manage digital IDs for IoT users and devices. Decentralized identity can be utilized in a blockchain-based IoT system to guarantee that only authorized people and devices can access and manage the network [6].IoT systems built on blockchain have a variety of uses. Healthcare, energy management, and supply chain management are three industries where blockchain-based IoT solutions can have a big influence. Blockchain-based IoT systems can track and trace goods and materials across the supply chain in supply chain management, ensuring their legitimacy and integrity. With smart devices that automatically adjust energy usage based on supply and demand, blockchain-based IoT systems can help energy grids become more effective and decentralized in terms of energy management. Blockchain-based IoT devices in the healthcare industry may securely handle and preserve patient medical records and allow for autonomous monitoring of health issues.Nonetheless, there are obstacles that must be overcome when putting into practice blockchain-based IoT systems. Security, interoperability, and scalability are all major issues that need to be taken into account. IoT systems built on blockchains can produce a lot of data, which puts a load on the network and slows down transactions. Because there are so many different IoT systems and devices that need to be able to connect with one another, interoperability can also be difficult [7]. Another major worry is security, as poorly secured blockchain-based IoT systems are susceptible to assaults.

II. Review of Literature

In the paper [8] author, the idea of blockchain technology was presented, along with a discussion of its potential applications, including the facilitation of trustworthy peer-to-peer online transactions that do not require the involvement of a third party.In the paper [9] author, a security and privacy architecture for connected vehicles that is based on blockchain technology was suggested.In the paper [10] author, presented a data sharing scheme for industrial IoT systems that is based on blockchain technology and assures both privacy and security.In the paper [11] author, analyzed the many merits and limitations of the various consensus algorithms that are utilized in blockchain technology and provided an outline of those algorithms.In the paper [12] author, presented a public auditing mechanism for cloud storage that would preserve users' privacy and make use of blockchain technology.In the paper [13] author, was to offer a blockchain-based supply chain monitoring system that enables safe data storage and analytics in an effective manner.In the paper [14] author, presented an overview of the potential of blockchain technology for Internet of Things applications was offered, along with a discussion of the benefits and problems presented by this technology.In the paper [15] author, describes the concept of blockchain technology and its potential to transform the way trust is built and maintained in numerous fields was examined.In the paper [16] author, describes an working decentralized security architecture for Internet of Things (IoT) systems that makes use of blockchain technology was proposed.In the paper [17] author, addressed the possible applications of blockchain technology in the construction of intelligent transportation systems that are safe, dependable, and effective.In the paper [18] author, describes the potential of blockchain technology for enhancing healthcare was examined. Blockchain technology has the potential to make data exchange and

administration safer and more efficient.In the paper [19] author, describes an data management architecture for industrial IoT systems that is built on blockchain technology and guarantees the data's integrity, privacy, and security was proposed in this study.In the paper [20] author, represented a broad assessment of the opportunities and problems presented by blockchain technology in a variety of settings.In the paper [21] author, describes a working of framework for the secure, efficient, and scalable sharing of data between cyber-physical systems was developed in this study. The architecture was based on blockchain technology.In the paper [22] author, presented an framework for the storage and exchange of data that is based on blockchain technology was developed for use in Internet of Things (IoT) devices.In the paper [23] author, presented a comprehensive overview of the previous research on the integration of blockchain technology with the internet of things (IoT), as well as an analysis of the primary research obstacles and opportunities.In the paper [24] author, presents a detailed survey of the uses of blockchain technology in supply chain management was offered, and both the merits and constraints of these applications were explored.In the paper [25] author, the potential of blockchain technology to address the difficulties associated with the administration of large amounts of data, as well as the opportunities and difficulties associated with studied.

Sr. No.	**Year**	**Approach**	**Application**	**Features**
1	2018	Hybrid blockchain-based	Smart city	Security, privacy, and data management
2	2018	Blockchain-based	Healthcare	Data security and access control
3	2018	Blockchain-based	Supply chain	Data integrity and transparency
4	2018	Blockchain-based	Smart grid	Data integrity and security
5	2018	Hybrid blockchain-based	Industrial IoT	Security and privacy
6	2018	Blockchain-based	Smart city	Security and privacy
7	2018	Blockchain-based	Healthcare	Data security and access control
8	2018	Blockchain-based	Industrial IoT	Data security and access control
9	2018	Blockchain-based	Smart grid	Data security and access control
10	2018	Blockchain-based	Healthcare	Data security and access control
11	2018	Blockchain-based	Smart home	Data security and privacy
12	2018	Blockchain-based	Smart grid	Data integrity and security
13	2018	Blockchain-based	Supply chain	Data integrity and transparency
14	2018	Blockchain-based	Industrial IoT	Data security and access control
15	2018	Blockchain-based	IoT data storage and sharing	Data integrity and security
16	2019	Blockchain-based	IoT security	Data security and access control
17	2019	Blockchain-based	Vehicle-to-grid networks	Incentive mechanism
18	2018	Blockchain-based	Industrial IoT	Access control
19	2019	Blockchain-based	Industrial IoT	Access control
20	2019	Blockchain-based	Security framework	Security framework

Table 1. Comparative Study of various Techniques Used in by Blockchain Based IoT System

A complete review of the potential of blockchain technology for Internet of Things applications is presented, along with a discussion of the different problems and prospects. They include a wide variety of themes, such as safety and privacy, the administration and exchange of data, techniques for reaching consensus, supply chain management, healthcare, and applications for smart grids. These papers provide a solid foundation for further research in this field and highlight the need for innovative solutions to address the challenges of integrating blockchain and IoT.

III. Techniques used for implementing Blockchain-based IoT Systems

Many methods have been presented for putting into practice IoT systems that are based on the blockchain. Among these methods are:

A. DLT, or distributed ledger technology: It is a subset of blockchain technology used to keep an incorruptible and publicly verifiable ledger of all business dealings. IoT data may be managed and stored transparently and safely using DLT.
B. Smart Contracts: The conditions of the agreement between the buyer and the seller of a "smart contract" are written directly into lines of code, making the contract self-executing. With smart contracts, IoT devices may automatically and reliably trade information and other assets with one another.
C. Consensus Mechanism: To guarantee that all participants in a blockchain network recognise the legitimacy of transactions, consensus procedures are employed. Common blockchain-based IoT consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT).
D. Hash Function: Data is given a distinct digital fingerprint using a hash function. The data's integrity and validity can then be confirmed by using this fingerprint. Blockchain-based Internet of Things solutions employ hash functions to protect the confidentiality and integrity of user data.
E. Encryption: Used for both in-transit and at-rest data security. Confidential Internet of Things data can be shielded from prying eyes by using encryption.
F. Key Management: When it comes to the security of blockchain-based IoT systems, private and public keys need to be managed, and this is where key management comes in. Only those who should have access to private information can gain it through the usage of key management systems.
G. Interoperability: The capacity of separate systems to communicate and collaborate effectively is known as interoperability. Standard protocols and application programming interfaces can facilitate interoperability in blockchain-based IoT systems.

Technique	**Advantages**	**Disadvantages**
Distributed Ledger Technology (DLT)	Decentralized, immutable, and transparent record of transactions	Scalability challenges, high energy consumption

Smart Contracts	Automation of exchange of data, secure and transparent	Limited scalability, high gas fees
Consensus Mechanism	Ensures agreement on validity of transactions	Proof of Work requires high energy consumption
(e.g., PoW, PoS)		Byzantine Fault Tolerance requires large network sizes
		Proof of Stake may have centralization concerns
Hash Functions	Provides unique digital fingerprint for data verification	None known
Encryption	Secures data in transit and at rest	Key management and exchange can be a challenge
Key Management	Manages private and public keys for securing blockchain	Potential for key loss or theft
Interoperability	Allows different systems to work together	Potential for reduced security due to exposure to APIs

The above table 2 , summarizes the benefits and drawbacks of the most common approaches used in Blockchain-based IoT systems. Certain methods may be more appropriate than others, depending on the scenario at hand. Data privacy, for instance, may need the use of more secretive methods like encryption or zero-knowledge proofs. The use of sharing or federated learning, on the other hand, may be more suited if scalability is a primary concern. The final method selected will be determined by the needs and limitations of the Blockchain-based IoT system under development.To keep blockchain-based IoT systems safe, transparent, and interoperable, several methods are employed. They play a significant role in maintaining the reliability of IoT data and are crucial to the effective implementation of blockchain-based IoT systems.

IV. Proposed Hybrid Technique used for Blockchain Systems based on IoT

By utilizing a hybrid consensus process, a blockchain's block design can incorporate both PoW and PoS. This may entail verifying blocks created by PoW and transactions made within them via PoS. You might also use a hybrid consensus mechanism that use PoW for verifying blocks but PoS for establishing policy and other administrative decisions.Using a public blockchain to record transaction data and a private blockchain to store sensitive data that requires stringent privacy controls are both examples of block architectures that can be used in a hybrid blockchain architecture. A hybrid blockchain design, on the other hand, would include the advantages of both private blockchains for internal use and public blockchains for external transactions and auditing.

To safeguard information, a hybrid encryption method may employ both symmetric and asymmetric encryption in its block design. Symmetric encryption can be used for the transport of data while asymmetric encryption can

be used for the exchange and verification of keys.Combining centralized and decentralized identity management methods is one possible block architecture for a hybrid identity management system. Data privacy and security can be handled by a decentralized system, while user identification and access control can be handled by a centralized identity management system.A hybrid data storage system's block architecture may include decentralized and centralized data storage strategies. This may entail storing data that is accessed frequently in a centralized location and data that is accessed infrequently in a decentralized location.

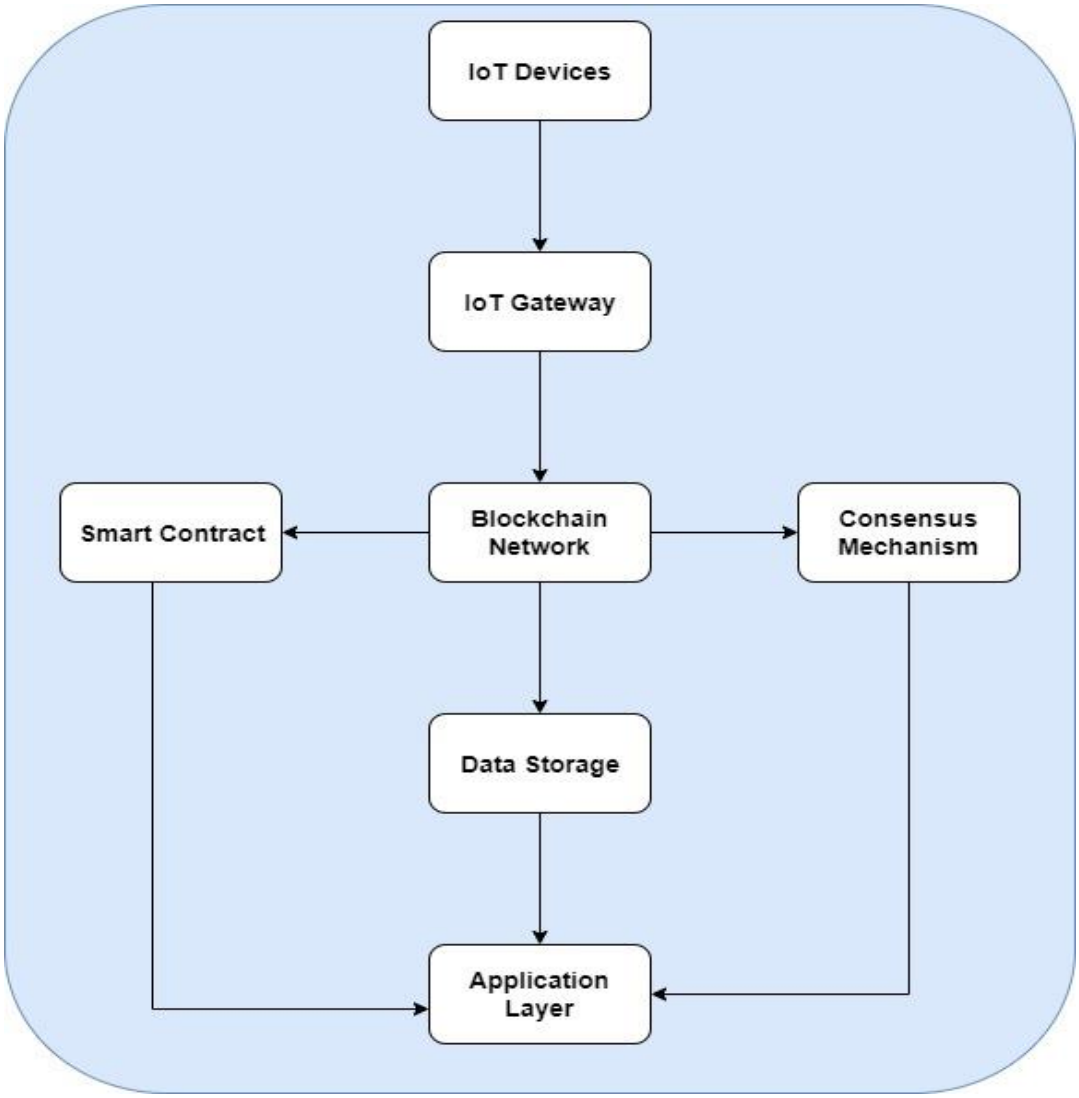

Figure 2. Block Architecture of Blockchain based IoT System using Hybrid Technique

An IoT gateway or edge device is used as an intermediary between the IoT gadgets and the blockchain in this schematic. Nodes on the blockchain network reach agreement on the veracity of transactions and the inclusion of new blocks using some sort of consensus mechanism. Smart contracts are embedded in the network and are set to trigger automatically under circumstances.The blockchain network's data storage component keeps all the information gathered by IoT gadgets. This information is permanent and only those with the proper cryptographic keys will be able to access it. The application layer allows users to engage with the system and view blockchain-based information through a graphical user interface.This schematic depicts the basic

architecture of a Blockchain-based Internet of Things system. The system's use case and requirements will determine the design and implementation specifics.The hybrid technique's block architecture is determined by the hybridization. Several hybrid Blockchain-based Internet of Things (IoT) system topologies include the following:

V. Application

IoT solutions that are based on blockchain technology have many potential applications across a wide variety of industries.

A. Management of supply chains: Internet of Things (IoT) systems that are based on blockchain technology can be used to monitor and control the flow of commodities through a supply chain. Sensors connected to the internet of things can be utilised to track the location and state of commodities, while blockchain technology can give an unchangeable record of all transactions and transfers.

B. Smart houses and buildings: Internet of Things (IoT) systems that are based on blockchain technology can be used to control and monitor numerous aspects of homes and buildings, including temperature, lighting, and security systems, among other things. Access control and data privacy can be managed in a way that is both secure and decentralized using blockchain technology.

C. Healthcare: Blockchain-based Internet of Things solutions can be employed in the healthcare industry to provide secure remote patient monitoring. Sensors connected to the internet of things are able to collect patient data, which can then be securely kept on a blockchain and shared with healthcare practitioners.

D. Energy Management: Management of energy production, distribution, and consumption Blockchain-based Internet of Things systems have the potential to be utilized in this capacity. Sensors connected to the internet of things can keep track of both energy consumption and production, while blockchain technology may be used to govern transactions and guarantee that energy is distributed equitably.

E. Agriculture: Internet of Things (IoT) systems that are based on blockchain technology can be used to monitor and manage crops and livestock. Sensors connected to the internet of things can collect data on the soil's moisture, temperature, and other elements, while blockchain technology can be used to trace the origin of food products as well as their quality.

F. Smart Cities: Blockchain technology is used in smart cities. IoT systems have the potential to be utilized in the administration of a variety of facets of urban life, including the flow of traffic, the management of garbage, and the quality of air. Sensors connected to the internet of things can collect data on these parameters, while blockchain technology can be used to handle transactions and ensure that resources are distributed properly.

VI. Challenges

The implementation of Internet of Things (IoT) systems based on Blockchain presents numerous obstacles. The following are some of the most major problems that need to be solved:

A. Scalability: As the number of Internet of Things devices and transactions increases, the blockchain network may become congested and unable to process transactions as rapidly. Scalability refers to the ability to accommodate a growing number of users and transactions. This may result in more delays as well as increased costs.

B. It is essential to ensure that both the internet of things (IoT) devices and the blockchain network are secure. Attackers are able to take advantage of any vulnerabilities in the Internet of Things (IoT) devices or the blockchain network, which can result in data breaches and financial losses.

C. Interoperability: The absence of standardization in the devices and protocols used by IoT can make it difficult to design interoperable systems that are able to communicate with one another. This can lead to a reduction in efficiency as well as fragmentation.

D. Concerns about data privacy have been raised in relation to the use of Internet of Things devices and the blockchain network. As data that is both personal and sensitive can be stored on a blockchain, it is of the utmost importance to guarantee that this data is shielded from access by unauthorized parties.

E. Developing and maintaining an Internet of Things system that is based on Blockchain might be an expensive endeavor. The cost of establishing and administering devices connected to the internet of things (IoT), in addition to the cost of operating a blockchain network, can be rather significant.

F. Energy consumption: Blockchain networks have a rather high energy consumption, which might be a significant barrier for Internet of Things devices that have a limited battery life.

G. Governance: The administration of both the blockchain network and the Internet of Things devices is essential to ensure that the system functions in an equitable and transparent manner. It is necessary to build models of governance that are democratic, transparent, and responsible to the people.

VII. Conclusion

In conclusion, Internet of Things (IoT) systems that are powered by blockchain technology can promote data sharing that is secure, transparent, and efficient. This has the potential to revolutionize a wide variety of business models. When blockchain technology is applied to Internet of Things (IoT) devices, however, a number of significant challenges are introduced. Some of these challenges include scalability, security, interoperability, data privacy, cost, energy consumption, and governance issues. It will be necessary to surmount a number of challenges before Internet of Things (IoT) systems based on blockchain technology can live up to their full promise. Researchers and industry practitioners need to work together to identify efficient ways to circumvent these challenges before Blockchain-based Internet of Things (IoT) technologies can become widely adopted.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System": This paper introduced the concept of blockchain technology and how it can be used to enable secure peer-to-peer electronic transactions without the need for a trusted third party.

[2] Dorri, M. Steger, S. Kanhere, and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy": This paper proposed a blockchain-based security and privacy framework for connected vehicles.

[3] Yao, X. Huang, Y. Zhao, and X. Shen, "Blockchain-based Privacy-Preserving and Secure Data Sharing Scheme for Industrial Internet of Things": This paper presented a blockchain-based data sharing scheme for industrial IoT systems that ensures privacy and security.

[4] T. L. Nguyen and S. Kim, "A Survey about Consensus Algorithms used in Blockchain": This paper provided an overview of the different consensus algorithms used in blockchain and discussed their strengths and weaknesses.

[5] Y. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing": This paper proposed a privacy-preserving public auditing scheme for cloud storage using blockchain technology.

[6] S. Wang, Q. Liu, and J. Wu, "Blockchain-based Data Management and Analytics for Supply Chain Monitoring": This paper presented a blockchain-based supply chain monitoring system that enables secure and efficient data management and analytics.

[7] M. Conti, S. Kumar, and C. Lal, "Blockchain Enabled IoT: An Overview": This paper provided an overview of the potential of blockchain technology for IoT applications and discussed its benefits and challenges.

[8] S. Banerjee and S. Misra, "Blockchain: The New Technology of Trust": This paper discussed the concept of blockchain technology and its potential to revolutionize the way trust is established and maintained in various domains.

[9] L. Li, Z. Yang, and J. Zhang, "A Blockchain-based Decentralized Security Architecture for IoT": This paper proposed a decentralized security architecture for IoT systems using blockchain technology.

[10] Dai, S. Zhang, Y. Wang, and H. Wang, "Towards Blockchain-based Intelligent Transportation Systems": This paper discussed the potential of blockchain technology for building intelligent transportation systems that are secure, reliable, and efficient.

[11] M. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here": This paper discussed the potential of blockchain technology for improving healthcare by enabling secure and efficient data sharing and management.

[12] Y. Zhang, J. Xu, and J. Yang, "Blockchain-based Data Management for Industrial Internet of Things": This paper proposed a blockchain-based data management framework for industrial IoT systems that ensures data integrity, privacy, and security.

[13] Zheng, W. Zhang, and X. Xie, "Blockchain Challenges and Opportunities: A Survey": This paper provided a comprehensive survey of the challenges and opportunities of blockchain technology in various domains.

[14] T. A. Arshad, N. Javaid, Z. A. Khan, M. U. Ilyas, and U. Qasim, "Secure and Efficient Data Sharing Framework for Cyber-Physical Systems Using Blockchain Technology": This paper proposed a blockchain-based data sharing framework for cyber-physical systems that ensures security, efficiency, and scalability.

[15] M. A. Rahman, A. Ali, M. U. Amin, and S. U. Khan, "BlockIoT: Blockchain Integrity for IoT Data Storage and Sharing": This paper proposed a blockchain-based data storage and sharing framework for IoT systems that ensures integrity and security.

[16] S. Li, C. Li, S. Li, J. Chen, and J . Y. Dai, "Blockchain and IoT Integration: A Systematic Review": This paper provided a systematic review of the existing literature on the integration of blockchain and IoT and identified the key research challenges and opportunities.

[17] S. Wang, Q. Liu, and J. Wu, "A Survey on the Applications of Blockchain Technology in Supply Chain Management": This paper provided a comprehensive survey of the applications of blockchain technology in supply chain management and discussed their benefits and limitations.

[18] X. Zheng, "Blockchain Challenges and Opportunities for Big Data": This paper discussed the potential of blockchain technology for addressing the challenges of big data management and discussed the research opportunities and challenges.

[19] A. Vazquez, M. T. Arredondo, and J. L. Hernandez-Ramos, "Blockchain for Smart Grids: A Review": This paper provided a review of the use of blockchain technology for smart grid applications and discussed the challenges and opportunities.

[20] Z. Qiu, X. Wu, X. Yang, J. Tang, and X. Zhu, "Blockchain-based Internet of Things: A Comprehensive Survey": This paper provided a comprehensive survey of the use of blockchain technology for IoT applications and discussed the challenges and opportunities.

[21] Maw, H.A.; Xiao, H.; Christianson, B.; Malcolm, J.A. A Survey of Access Control Models in Wireless Sensor Networks. *J. Sens. Actuator Netw.* **2014**, *3*, 150–180

[22] Cai, F.; Zhu, N.; He, J.; Mu, P.; Li, W.; Yu, Y. Survey of access control models and technologies for cloud computing. *Clust. Comput.* **2019**, *22*, 6111–6122

[23] Rouhani, S.; Deters, R. Blockchain Based Access Control Systems: State of the Art and Challenges. In Proceedings of the WI '19: IEEE/WIC/ACM International Conference on Web Intelligence, Thessaloniki, Greece, 14–17 October 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 423–428.

[24] RiahiSfar, A.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137

[25] Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035