FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Review Article | Volume 10, Issue 2 | Pages 74-79 | e-ISSN: 2347-470X

Blockchain Technology to Handle Security and Privacy for IoT Systems: Analytical Review

Chen Zhonghua[1,2] and S. B. Goyal[2]

[1]BaiCheng Normal University, BaiCheng, China
[2]City University, Petaling Jaya, Malaysia

***Correspondence:** Dr. S. B. Goyal; Email: drsbgoyal@gmail.com

ABSTRACT: With a large number of mobile terminals accessing IoT for information exchange and communication, security issues such as identity authentication, data transmission, and device failure are becoming more and more serious. Most of the traditional security technologies are based on centralized systems, and due to the limitation of IoT topology, traditional security technologies can only be applied to specific industries. Blockchain technology has the features of decentralization, data encryption, and tamper-proof, which are especially suitable for application in complex heterogeneous networks. This paper discusses for the first time the use of the block chain in many fields, providing an opportunity to address IoT security issues. Second, it discussed the IoT acceptance on various domains and the privacy issues IoT faces on limited resources. Finally, this paper investigates many of the problems facing the integrated process of block chain-based and IoT-based applications. The purpose of this article is to provide an overview of block chain based policies for privacy protection in IoT. After analyzing related solutions, blockchain technology can work better in the area of IoT security and privacy protection.

General Terms: Blockchain, IoT.
Keywords: BIoT (Blockchain+IoT), Internet of Things (IoT), Blockchain, Security and privacy.

ARTICLE INFORMATION
Author(s): Chen Zhonghua and S. B. Goyal;
Special Issue Editor: Dr. Sandeep Kautish
Received: 10/04/2022; **Accepted:** 20/04/2022; **Published:** 13/05/2022;
E- ISSN; 2347-470X
Paper Id; 0222SI-IJEER-2022-01;
Citation: 10.37391/IJEER.100204
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100204.html

This article belongs to the Special Issue on **Novel Architectures and Methods in Industrial IoT and Wireless Sensor Networks for Sustainable Computing**

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Bitcoin has brought together many community groups and has gradually evolved into a technical foundation for transforming productive relationships and building a trusting society. Blockchain is a distributed and distributed technology with trackable and consistent data that can establish trust relationships in participating nodes in a network environment without a trust center. Smart contract technologies in the next generation of blockchain, such as Ether and Hyperledger Fabric, extend blockchain from a distributed database for storing critical data to a decentralized, distributed computing platform. Blockchain technically solves the security issues of access control methods that use centralized authorized decision-making entities. Access control of blockchain-based can reduce the dependence of access control on a single trusted entity and improve the reliability of access control and data security. Meanwhile, Devices of IoT can use blockchain as the underlying network architecture to form the IoT, thus strengthening the IoT's ability to resist external cyber-attacks [1].

This article provided an overview of the use of blockchain technology in related fields and the challenges IoT faces in terms of security and privacy. This article provided an overview of the use of blockchain technology in related fields and the challenges IoT faces in terms of security and privacy. This article fully introduces the use of blockchain technology in related fields and the challenges IoT faces in terms of security and privacy. This thesis has the following parts. Introduce the origins of blockchain technology, technology principles and blockchain industry development and applications; reveals the basic concepts of IoT technology and summarizes the security and privacy issues as well as the major security threats IoT faces in the first phase. The second section briefly introduced the combination of blockchain and IoT security and privacy, focusing on a detailed discussion of the existing challenges and issues facing BIoT applications. The third section discussed the whole article and summarizes the risks and challenges faced by IoT in the security and privacy. The fourth section summarizes future research applications and guidelines on blockchain technology in the IoT security sector.

1.1 Blockchain

1.1.1 The Overview of Blockchain

1.1.1.1 Blockchain Definitions

A blockchain is essentially a continually increasing distributed database maintained by numerous participants. The Distributed Shared Ledger (DSL) blockchain maintains a growing and ordered chain of data through smart contracts that allow any number of nodes participating in the system to put together a time system of all nodes through cryptographic algorithms that can Encryption algorithms calculate and record all information exchanged in the system to a data block and generate a data block thumbprint that can be used to chain the following data blocks and verify it. The core of the system also lies in the development from information connectivity to value connectivity by establishing trust between the two parties of a transaction through a distributed network, a time-series tamper-proof cryptographic ledger and a decentralized consensus mechanism, and by programming and manipulating data with smart contracts consisting of automation scripts [2]. Typically, the structure of the blockchain data is shown in Figure 1.

1.1.2 The technical characteristics of blockchain

Blockchain is an integrated innovation of many existing technologies and is mainly used to achieve multi-party trust and university cooperation. In general, mature blockchain systems have four characteristics: transparency, tamper-proof traceability, privacy security, and high reliability of the system [3].

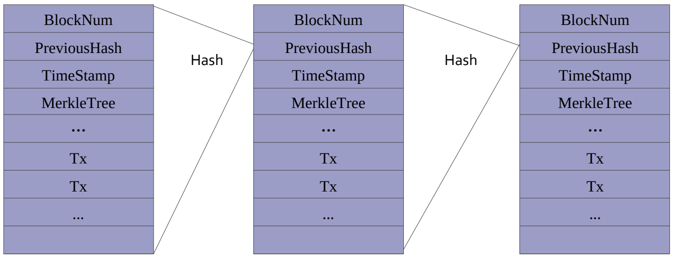

Figure 1: Data structure of blockchain

1.1.2.1 Transparency

In a decentralized system, all nodes in the network are peer-to-peer and they send and receive information in the network equally. Therefore, each node in the system has full observation of all actions in the network and maintains a local ledger of these actions in each node and the whole system is transparent to each node.

1.1.2.2 Tamper-proof-traceability

Tamper-proof means that once a transaction is verified across the network and added to the blockchain, it is difficult to modify or delete it. Traceability signifies that every exchange on the blockchain is fully tracked. We can track all historical transactions associated with a certain state on the blockchain.

1.1.2.3 Privacy security

As any node in the blockchain system contains the complete blockchain authentication logic, no node needs to depend on any other node to accomplish the verification process of transactions in the blockchain. The de-trust features make it unnecessary for nodes to reveal their identities to each other, as no node needs to judge the validity of a transaction based on the identity of other nodes, which provides the basis for the blockchain system to protect user privacy.

1.1.2.4 High reliability of the system

First, each node has a ledger and participates in all system syncing, which means that even if one node fails, it does not affect the normal operation of the entire system. Second, blockchain systems support Byzantine fault tolerance. Traditional distributed systems, while highly reliable, usually tolerate only node crashes or network partitions in the system; once the system is broken, or the information processing logic of the nodes is modified, the whole system will work properly and will not become distributed [4]. Generally, a blockchain network includes a data storage layer, a network communication layer, a data security layer, a consensus layer, an incentive layer, and an applications layer. The blockchain infrastructure model is shown in Figure 2.

1.1.3 *Blockchain technology principle*

The key technologies of blockchain mainly include: cryptography, consensus algorithms, smart contracts, and peer-to-peer networks [5], as shown in Figure 3.

1.1.3.1 Encryption Algorithm

Cryptography technology gives blockchain many capabilities and features, such as immutability, authentication, communication security, storage security, and privacy protection. From the technical point of view, the following cryptographic techniques are used in mainstream blockchain systems: hashing algorithms, asymmetric encryption algorithms, digital signature algorithms, digital certificates, and symmetric encryption algorithms. For some advanced usage scenarios, technologies such as Trusted Execution Environment (TEE), homomorphic encryption, and zero-knowledge proof are also adopted [6].

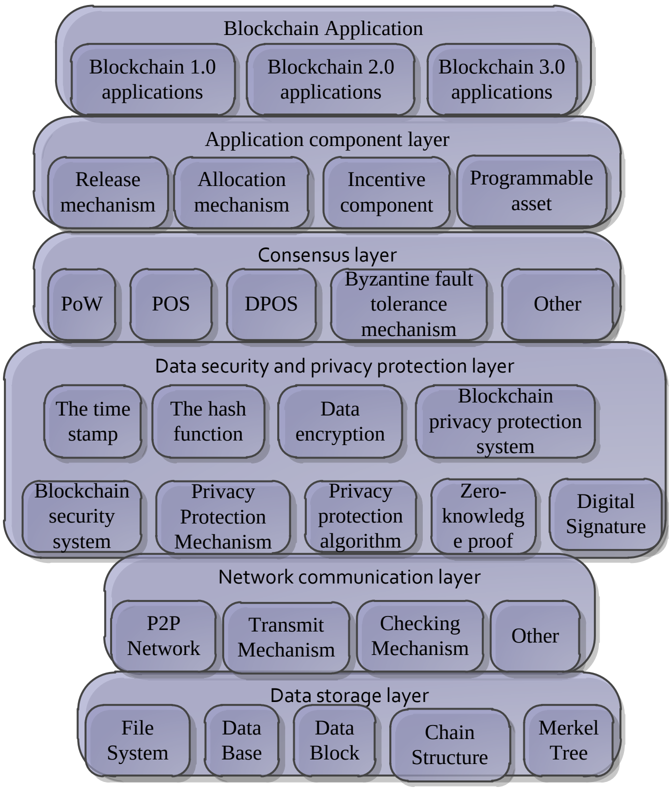

Figure 2: Data structure of blockchain

1.1.3.2 Consensus Mechanism

First, the consensus algorithm is the foundation and core of blockchain technology, which determines how to agree on the execution order and content of transactions among cluster nodes and ensures the consistency of node ledger data. The development of consensus theory laid a solid foundation for the proposal of consensus protocols, in which the correct model, fault model, and network model are far-reaching [7].

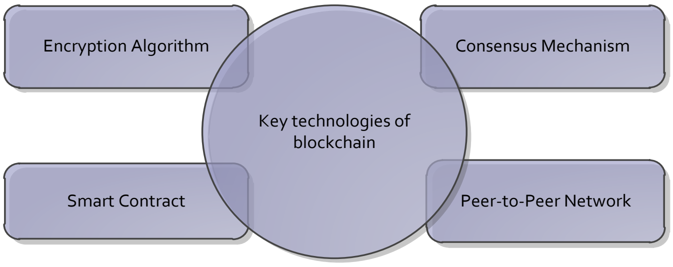

Figure 3: Blockchain key technology

1.1.3.3 Smart Contract

In short, a smart contract is an automated system where some of the conditions are met. The introduction of smart contracts is an important milestone in the development of blockchain. From the original blockchain's single cryptocurrency application to its integration into all areas of social production and life today, the role of smart contracts cannot be underestimated. Almost all of these applications - finance, government services, supply chain, gaming - run on different blockchain platforms in the form of smart contracts [8].

1.1.3.4 Peer-to-peer network

This networking (P2P) is a decentralized way of exchanging information over the Internet. It eliminates centralized service nodes and treats all network participants as peers and distributes tasks and workloads among them. The P2P architecture breaks the traditional C/S model by eliminating central servers and is a network structure that relies on collective maintenance by users. The P2P network is highly reliable because data transfer between nodes does not depend on a central service node. In blockchain systems, all nodes need to jointly maintain the ledger data, which means that each transaction needs to be sent to all nodes in the network [9].

1.1.4 Applications of blockchain

Blockchain is used in many areas of our daily lives [10] in Figure 4.

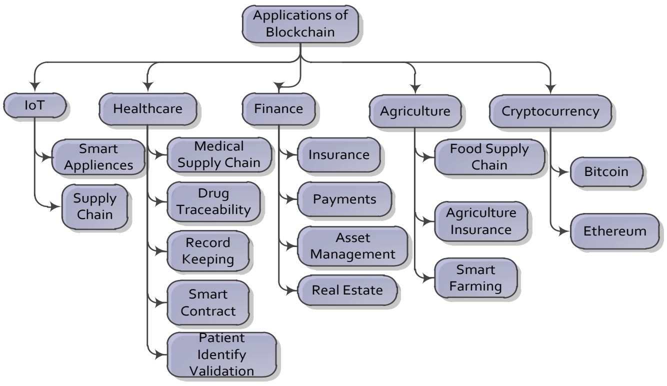

Figure 4: Applications of Blockchain

1.1.4.1 Finance

Blockchain assures the secure storage and immutability, taking advantage of his integration in commercial banking, as it makes the exchange of funds more secure. With blockchain, the transactions become visible and confidential [11].

1.1.4.2 Medical care

Blockchain has been widely used in the healthcare industry [12]. For example, it can store patient case information, treatment records, etc. Blockchain can be used online in Medical Devices to improve the safety of smart medical devices used by patients and the privacy of sensitive data [13].

1.1.4.3 Supply chain

Since blockchain has the property of immutability, it is applied in the supply chain system, which can trace the purchase and sale records of the supply chain system, making it impossible for buyers and sellers to deny, and the researchers have proposed the blockchain technology-based supply chain model with multiple ledger tracking in the simplification of the supply chain management process [14].

1.1.4.4 Electronic Voting

The transparency and immutability of blockchain make its application in election voting effective in preventing fraud such as vote tampering. If the vote is successful, a new block is built and connected to the series. This way also has some drawbacks, such as the poor scalability of the voting system and the problem of voters being coerced to vote [15].

1.1.4.5 Smart City

Blockchain has greater application potential in many areas of new smart cities [16]. In terms of infrastructure, it can be combined with the construction of new smart cities to explore empowerment in areas such as information architecture, intelligent transportation, energy and electricity to improve the intelligentization and precision of city management. In terms of data sources, blockchain is promising to destroy the existing barriers to data circulation and sharing, offer high-quality data sharing assurance, improve data quality control, and enhance data security to ensure protection [17].

1.2 Internet of Things

1.2.1 *Overview and applications of IoT*

IoT is an Internet-based network, traditional communication networks and other information carriers that connect all common physical objects that can be dealt with independently [18]. It has three key features: shared device devices, independent end point connectivity, and universal service understanding [19], the applications of IoT was showed in Figure 5.

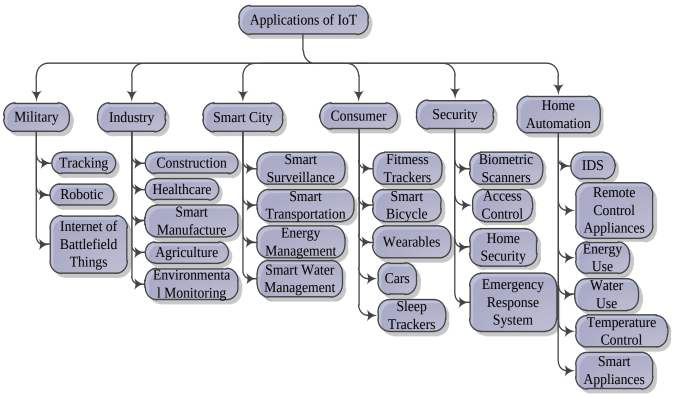

Figure 5: Applications of IoT

1.2.2 Systems Security and Privacy Challenges in IoT

1.2.2.1 Limitations of IoT devices

As an increasing number of enterprises adopt IoT technologies, a new set of security challenges and vulnerabilities have surfaced [20]. The complexity of IoT communication is largely due to the large number of devices connected to the global Internet and the large amount of data generated by these devices. The devices of IoT sysytem are an easy target for cyber attackers to compromise, and thus IoT attacks are more likely to occur. Learn about the main security challenges of the IoT ecosystem below [21].

1.2.2.2 Inadequate risk measures for IoT device updates

The IoT will bring about a high degree of developed capabilities for connection, customization and automation [22]. Yet, IoT devices are also faced with a large number of problems and challenges, especially in terms of comprehensive updates, and a large number of IoT devices are not updated with security, and these devices are directly exposed to potential threats or attacks.

1.2.2.3 Cryptocurrencies attract more and more hackers

The increasing number of cryptocurrencies has proven to be very tempting and attractive to cyber hackers. There is no doubt that the frequency of cyberattacks is on the rise, but the essential problem is not in the blockchain itself. Blockchain technology itself is not particularly risky, but the process of developing its applications is.In fact, blockchain technology itself is not particularly risky, but the process of developing its applications is. Attacks on blockchain technology continue to climb as numerous blockchain companies attempt to improve security to counter hacking attacks [23].

1.2.2.4 Ransomware and malware extortion and attacks on the IoT

As the number of IoT devices grows, ransomware cyberattacks can directly cripple or limit device functionality and steal sensitive data information from customers. Ransomware and malware are being organized with the aim of merging various attacks [24]. Flimsy login passwords and credentials put nearly all IoT devices at risk of password cracking and brute force attacks. IoT devices are susceptible to cyber assaults when they are attached to the global Internet. The industry companies and network security researchers are trying to provide secure products to users, and there is much more to be done now [25].

2. MATERIALS AND METHODS

2.1 Blockchain and IoT convergence

2.1.1 Blockchain and IoT fusion theoretical architecture

IoT devices are connected to networks, generating large amounts of data and integrating powerful data analytics capabilities that are expected to change the way people produce and live [26]. However, while providing development opportunities, there are still many problems in scalability, compatibility, and security in the IoT industry at this stage, which seriously limit the space for the integration and development of IoT with various industry sectors and hinder the realization of its potential value. Blockchain, as an emerging technology fused with IoT, can be an effective solution to the problems of trust, data management, security, and privacy problems in the IoT growth [27].

2.1.1.1 The Imperative Need for Blockchain and IoT Integration and Innovation

As an emerging technology, the IoT is more widely used. At this stage, there are still many problems in the IoT industry [28]. The industry chain in IoT is long, involving a wide range of technical fields, and the value conduction effect of the market channel is slow [29]. The trust system and value system among all parties in the IoT system such as devices, various users, and service platforms are not clear yet, which makes it difficult to integrate IoT into other industries [30]. The centralized IoT platforms built by manufacturers or service providers mostly have the authority to collect and analyze user data and control user devices without user authorization, which poses a great danger to device security and user privacy [31]. The integration of blockchain and IoT can effectively solve a series of problems faced in the development of IoT and help scalable devices to build efficient, trusted, and secure distributed IoT networks and deploy massive data-intensive applications, while providing valid safeguards for user privacy [32].

2.1.1.2 Convergence architecture for blockchain and IoT

The IoT architecture developed by integrating blockchain technology is a “limited” service framework (as shown in Figure 6). The blockchain IoT strategy can be broken down into a user-centered application background, service and support layer， network public chain layer, and device awareness layer. In this regard, the device sensing layer is linked to physical objects and supports the collaboration of IoT entities in a "decentralized" mode and is able to collect information through sensors [33].

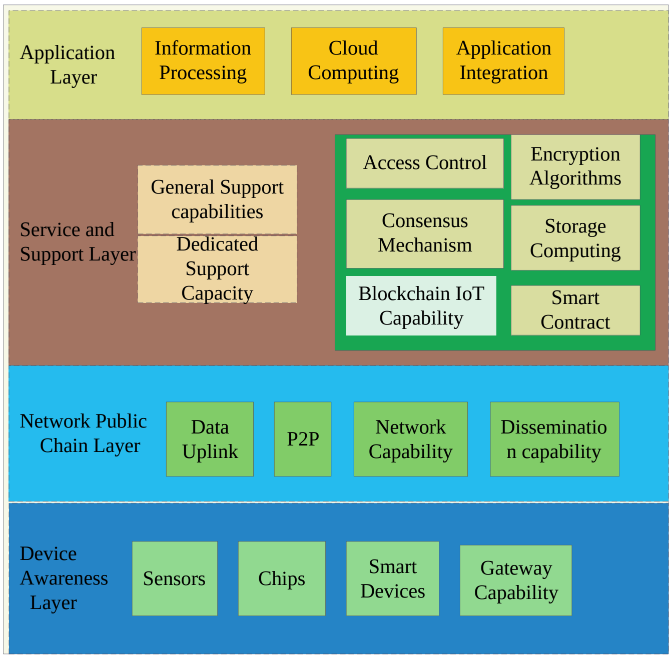

Figure 6: Applications of Blockchain

2.1.2 Challenges for BIoT applications

Although the interconnection of blockchain and IoT can provide a lot of benefits, some challenges still need to be addressed in the development [35].

2.1.2.1 Scalability, processing power, and storage issues

In the era where every chip or sensor is an IoT device, the scalability of the IoT blockchain is bound to be important. This is because of the need to collect and load a huge amount of data. In addition, the required amount of processing power and time to encrypt all IoT devices in a blockchain-based ecosystem is not ideal and is not feasible on the latency-sensitive industrial Internet. Storage, on the other hand, is another major problem in blockchain systems, which is a data storage technology that can only be appended and cannot be deleted [36].

2.1.2.2 *Technology Development*

At present, industries are still skeptical about the comprehensive application of "blockchain + Internet of Things". How blockchain works with IoT is still not understood by most end users. And this may limit firms from investment in this developing technology as it remains and lack of regulated status [37].

2.1.2.3 Stability

When blockchain is applied to real life, the requirement for stability is very high. Imagine applying the blockchain of IoT concept to smart city, if something goes wrong with the blockchain, it will affect the lives of countless people [38], [40].

2.1.2.4 Legal and Compliance Issues

Some stakeholders in the industry have raised the issue of responsibility when a device takes an action that is based on rules that are automatically executed by a blockchain application and activated by another blockchain-based application. But it is never a simple matter to operate in the smart contract space, and reaching a contract, such as outside of this IoT and blockchain, is far from easy [39], [41]. The current challenges and issues that BIoT applications have faced were listed in Table 2 below.

Table 1. Challenges and Issue of BIoT Applications

No.	Challenges	Issue for BIoT Applications
1	Scalability, processing power, and storage issues	IoT device scalability, small storage, and blockchain latency
2	Technology Development	Enterprises still have doubts about the integrated application of BIoT
3	Stability	Lack of high stability of IoT devices
4	Legal and Compliance Issues	Lack of legal supervision of smart contracts

3. DISCUSSION

The natural pan-centric distributed and trusted nature of blockchain provides new ideas for designing frameworks and architectures for the convergence of blockchain and IoT. In a smart IoT computer, a few IoT devices use intelligent algorithms scattered across a network, and these devices need constant communication to participate in AI computer operations or to make smart team decisions together. However, both the tool itself and the interaction between machines are exposed to various cyber threats, such as the possibility of the transmitted information being corrupted or altered when the device malfunctions or is maliciously attacked. Blockchain can be used for intelligent Iot computer programs, such as confidential, authenticated, authentic documents that can ensure secure interoperability in an independent, reliable, shared record system and distributed compliance regarding the legitimacy of processed records. At the same time, the chain block and the consensus of intelligent contract mechanism and incentive mechanism of a natural fit for building a market economy, an effective incentive IoT calculation of information sharing and interaction.

4. CONCLUSION & FUTURE WORK

According to the forecast of related organizations, the amount of global IoT devices are going to reach tens of billions by 2023. As the number of devices in the IoT rises dramatically, the demand for services continues to increase, the cost of data center infrastructure construction and maintenance investment rises significantly, and the security risks and performance bottlenecks of related IoT business platforms are increasing day by day. Designing new IoT service models has become a strategic focus for enterprise and organizational innovation, and combining blockchain technologies to build a "decentralized" IoT structure has become one of the key models.

FUNDINGS

This paper was funded by Jilin Provincial Department of Education, China, grant number JJKH20210005KJ.

REFERENCES

[1] Shangrong. Jiang and YuzeLi, J. 2022. Blockchain competition: The tradeoff between platform stability and efficiency. European Journal of Operational Research, Volume 296, Issue 3, Pages 1084-1097.

[2] Ali Alferaidi, Kusum Yadav, Yasser Alharbi, Navid Razmjooy, Wattana Viriyasitavat, Kamal Gulati, Sandeep Kautish, Gaurav Dhiman, "Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles", Mathematical Problems in Engineering, vol. 2022, Article ID 3424819, 8 pages.

[3] Lei. Wang and Yichao. Ma, J. 2022. Design of integrated energy market cloud service platform based on blockchain smart contract. International Journal of Electrical Power & Energy Systems, Volume 135, 107515.

[4] Tonghe. Wang and Haochen. Hua, J. 2022. Challenges of blockchain in new generation energy systems and future outlooks. International Journal of Electrical Power & Energy Systems, Volume 135, 107499.

[5] Shangrong. Jiang and Yuze. Li, J. 2022. Blockchain competition: The tradeoff between platform stability and efficiency. European Journal of Operational Research, Volume 296, Issue 3, Pages 1084-1097.

[6] Maxat. Kassen, J. 2022. Blockchain and e-government innovation: Automation of public information processes. Information Systems 103, 101862.

[7] Ghonimy and Mohamed. Eid Helmy, J. 2021. Factors Influencing the Decision to Adopt Blockchain Technology. Capella University ProQuest Dissertations Publishing, 28547645.

[8] Saurabh. Shukla and Subhasis. Thakur, J. 2021. Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model. Internet of Things, 100422.

[9] Christian F. Durach, Till Blesik. J. 2021. Blockchain Applications in Supply Chain Transactions [J]. Journal of Business Logistics 42(1), 7–24.

[10] Josepha. Witt, J. 2021. When is Blockchain Technology Valuable? –A State-of-the-Art Analysis. UK Academy for Information Systems (UKAIS).

[11] Christian. F. Durach and Till, J. 2021. Blesik. Blockchain Applications in Supply Chain Transactions. Journal of Business Logistics, 42(1): 7–24.

[12] Huawei Huang and Wei Kong, J. 2021. A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools. ACM Comput. Surv, 42-54 pages.

[13] Mahtab.Kouhizadeh, J. 2021. Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. International Journal of Production Economics, Volume 231, 107831.

[14] Iftikhar Zainab and Yasir. Javed. Syed Y.A, J. 2021. Zaidi. Munam A. Privacy Preservation in Resource-Constrained IoT Devices Using Blockchain—A Survey. Electronics 10, no. 14: 1732.

[15] Aparna Kumari and Rajesh Gupta, J. 2021. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. Computer Communications, Volume 172, Pages 102-118.

[16] Shantanu. Pal. and Ali. Dorri, J. 2021. Blockchain for IoT Access Control: Recent Trends and Future Research Directions. arXiv, 2106.04808.

[17] Algarni and Sultan. Fathy Eassa, J. 2021. Blockchain-Based Secured Access Control in an IoT System. Applied Sciences, 11, no. 4: 1772.

[18] Laphou. Lao and Zecheng, J. 2021. A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling. ACM Computing SurveysVolume, 53 Issue 1 Article No.18pp 1–32.

[19] Marco. Picone and Simone. Cirani, J. 2021. Blockchain Security and Privacy for the Internet of Things. Sensors (Basel), 21(3): 892.

[20] S. Sun. and R Du, J. 2021. Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. IEEE Access, vol. 9, pp. 36868-36878.

[21] Pavithran. D. and Shaalan. K, J. 2020. Towards building a blockchain framework for IoT. Cluster Comput, 2089–2103.

[22] Fei. Chen and Zhe. Xiao, J. 2020. Blockchain for Internet of things applications: A review and open issues. Journal of Network and Computer Applications, Volume 172, 102839.

[23] A.Subhadra, R.Ganesh, K.Maheshbabu, K.Sai Sandeep, J. 2020. Iot Based Real Time Weather Monitoring System, International Journal of Engineering Applied Sciences and Technology , Vol.4, Issue 11, ISSN No 2455-2143, Pages 384-392.

[24] M. Pradhan and J. Noll, J. 2020. Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems. IEEE Communications Magazine, vol. 58, no. 8, pp. 14-20.

[25] J. K. Solomon Doss and S. Kamalakkannan, J. 2020. IoT System Accomplishment using BlockChain in Validating and Data Security with Cloud. 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 60-64.

[26] Smetanin. Sergey and Aleksandr. Ometov, J. 2020. Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective, Sensors 20, no. 12: 3358.

[27] D. Torres and J. P. Dias, J.2020. Real-time Feedback in Node-RED for IoT Development: An Empirical Study. IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT).

[28] V. Sharma. I. and You, K. Andersson. J. 2020. Security, Privacy and Trust for Smart Mobile- Internet of Things (M-IoT): A Survey. IEEE Access, vol. 8, pp. 167123-167163.

[29] Yan. Zhang.and Bing. Li, J. 2020. An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices. Electronics, 9(2), 285.

[30] Md. Sadek. Ferdous and Mohammad, Jabed Morshed Chowdhury, J. 2020. Blockchain Consensus Algorithms: A Survey. arXiv: 2001, 07091 [cs.DC].

[31] Rui. Zhang.and Rui. Xue. J. 2019. Security and Privacy on Blockchain. ACM Comput. Surv, Vol. 52, No. 3.

[32] Malak. Alamri and NZ. Jhanjhi, J. 2019. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. International Journal of Computer Science and Network Security International, Vol.19 No.5.

[33] Bhabendu. KumarMohanta.and Debasish. Jena, J. 2019. Blockchain technology: A survey on applications and security privacy Challenges. Internet of Things, Volume 8, 100107.

[34] Erdem, A. and Yildirim, S.Ö, J. 2019. Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art. Security, Privacy and Trust in the IoT Environment, pp 97–122.

[35] R. Henry. And A. Herzberg, G. 2018. Blockchain Access Privacy: Challenges and Directions. IEEE Security & Privacy, vol. 16, no. 4.

[36] Francesco Restuccia and Salvatore D'Oro, J. Blockchain for the Internet of Things: Present and Future. IEEE INTERNET OF THINGS JOURNAL, Vol. 1, NO. 1.

[37] Dylan, Yaga and Peter, Mell, J. 2018. Blockchain Technology Overview. National Institute of Standards and Technology Internal Report, 8202 66 pages.

[38] G. Karame and S. Capkun, J. 2018. Blockchain Security and Privacy. IEEE Security & Privacy, vol. 16, no. 04, pp.

[39] O. Novo, J. 2018. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195.

[40] Z, Zheng, S. and Xie. H, J. 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data (BigData Congress) 557-564.

[41] Harald. Sundmaeker, J. 2010. Vision and challenges for realising the Internet of Things. Luxembourg: Publications Office of the European Union.

[42] Chandrajeet Yadav, Vikash Yadav and Jasvant Kumar (2021), Secure and Reliable Data sharing scheme using Attribute-based Encryption with weighted attribute-based Encryption in Cloud Environment. IJEER 9(3), 48-56. DOI: 10.37391/IJEER.090305.