Systematic Review of Blockchain integrated Internet of Things: Architecture, Benefits, Security and Privacy concerns

Bharati B Pannyagol[1*], Dr. Santosh Deshpande[2†], and Dr. Rohit Kaliwal[3†]

[1*] *Research Scholar,* [2†] *Professor,*[3†] *Assistant Professor,*
Department of Computer Science and Engineering , Visvesvaraya Technological University, Belagavi, Karnataka, India.

Abstract
The proliferation of smart devices and related technologies has made the Internet of Things(IoT) the most rapidly emerging technology of the past ten years, both in terms of industrial applications and research opportunities. Security problems are being caused by the IoT by use of unstable fixed and mobile devices. One potential solution to the security issues with IoT is to use Blockchain technology. This paper delves into safety hazards and problems that affect the IoT and cause system performance degradation. It presents a layered architecture of IoT with Blockchain. In addtional the paper also outlines the solutions provided by the Blockchain ,recent trends and different hazards in using Blockchain with IoT that will helpful for future reseach.

Keywords
Internet of Things,Blockchain,Security,Hazards,Privacy.

1. Introduction

The importance of the Internet of Things in creating intelligent applications has grown recently. With the integration of cutting-edge and complex technologies, IoT turns traditional applications into intelligent applications. This study highlights the use of Blockchain technology to protect IoT data privacy and security.

1.1. Internet of Things (IoT)

The potentially ground-breaking IoT technology will link everything and everyone to the Internet. It is rapidly emerging as a pervasive global computing network [1]. Nowadays, IoT becoming the most growing up technology, and it is decisive in human life to survive in a better way. The things [2] which have the facility to data transfer via a network without

ComSIA'24: Computing & Communication Systems for Industrial Applications, May 10–11, 2024, New Delhi, INDIA
*Corresponding author.
† These authors contributed equally.
* bharati.p@vtu.ac.in (B. B Pannyagol); † sldeshpande@gmail.com(S.L.Deshpande);
†rohit.kaliwal@gmail.com(R. Kaliwal)
0000-0003-0998-7182 (B.B. Pannyagol); 0000-0001-5152-0952 (S.L.Deshpande); 0000-0001-8342-2126 (R. Kaliwal)

demanding human to human or human to computer interaction are labeled as IoT [3]. It expands the dependency of the human allowing them to interrelate, contribute, and collaborate in constructing a framework that is simple, secure, and time-saving [4]. It refers to node, device or sensors that measure the physical quantity and convert it into the digital or understanding quantity [5], [6]. The fundamental concept behind the IoT is to enable the independent sharing of valuable data amongst various discretely embedded, individually identifiable real-world devices in our surroundings [1]. There has been an exponential growth in the IoT-based services in the world, especially in Tele health, Manufacturing and in urban areas to form Smart cities [7].

The IoTs has significantly changed the communication industry, a relatively new technological development. Its implementation in a variety of industries [8], including weather monitoring [9], agriculture [10], [11], and healthcare [12] etc. The general impression of IoT environments and applicable [13], [14] scenarios layer wise are represented in Figure 1.

Figure 1: Top IoT applications

1.2. IoT Enabling Technologies

IoT enabling technologies provide the foundation for edifice and deploying IoT solutions. These technologies encompass various H/W and S/W components that enable connectivity, data processing, and interaction between IoT devices and applications. Figure 2 explains some key IoT enabling technologies.

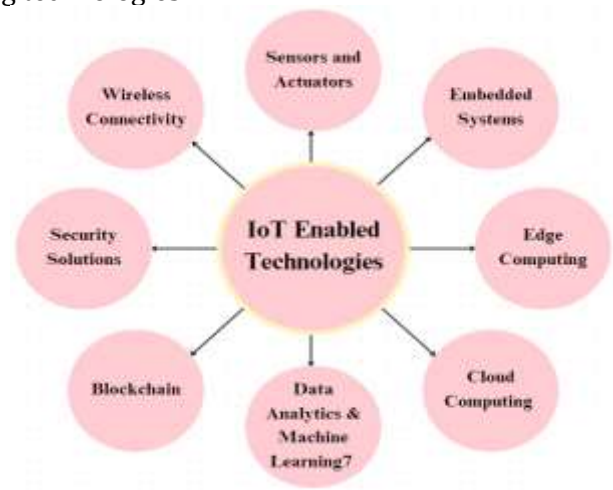

Figure 2: IoT Enabled Technologies

- **Wireless Connectivity:** These have different characteristics, such as battery life, connectivity, and spectrum, allowing them to be suitable for various applications [15].
- **Sensors and Actuators:** Sensors accumulate information from the atmosphere around them, while actuators enable devices to perform actions based on received data.
- **Embedded Systems:** Embedded systems are specialized computing devices designed to perform specific functions within IoT devices. These systems typically include microcontrollers or microprocessors, memory, input/output interfaces, and firmware/software for device operation.
- **Edge Computing**: It involves processing data locally on IoT devices or within proximity to them, instead of sending all data to a centralized cloud server for processing. This reduces latency, bandwidth usage, and reliance on cloud infrastructure, making it suitable for real-time IoT applications.
- **Cloud Computing:** Cloud platforms provide scalable storage, computing, and analytics capabilities for managing and analyzing large volumes of IoT data. Cloud services such as data storage, data processing, ML, and application hosting support IoT deployments and enable advanced data-driven insights and applications [16].
- **Data Analytics and Machine Learning:** Data analytics techniques, including descriptive, diagnostic, predictive, and prescriptive analytics, extract meaningful insights from IoT data. ML algorithms can identify patterns, anomalies, and trends in IoT data to optimize operations, predict failures, and enable autonomous decision-making.
- **Blockchain:** Blockchain technology offers decentralized, transparent, and immutable ledger capabilities for secure data storage, transactions, and smart contracts in IoT applications. It enhances data integrity, security, and trust among IoT stakeholders, particularly in applications requiring secure data exchange and transactional integrity [17].
- **Security Solutions:** This technology protects IoT devices, networks, and data from virtual threats and unauthorized access. These technologies include encryption, authentication, access control, IDS, and secure bootstrapping.

1.3. Basics of BC Technology

The BC is now regarded as the second-most important invention after the Internet. The BC technology is based on the suitability of the tertiary platform [18]. It is a form of database loading that is non-centralized, reliable, and grim to use for fraudulent purposes [19]. The main advantage of BC, it is unbearable to initiate an attack in the network because it must compromise 51% of its systems to the target network. The major characteristics of BC are audibility, persistency, anonymity, and decentralization, thereby efficiency is increased and the cost is saved [20]. BC is a point-to-point distributed ledger based on steganography and a network-sharing system characterized by its disintermediation, transparency, and openness [21]. The BC technology and distributed ledgers are attracting massive attention

and trigger multiple projects in different industries. However, the financial industry is seen as a primary user of the BC concept [22]. It is recognized as a key enabling technology that brings/connects all distributed sensors and smart devices together, to gather and switch the information within smart city infrastructure using an open channel [23].

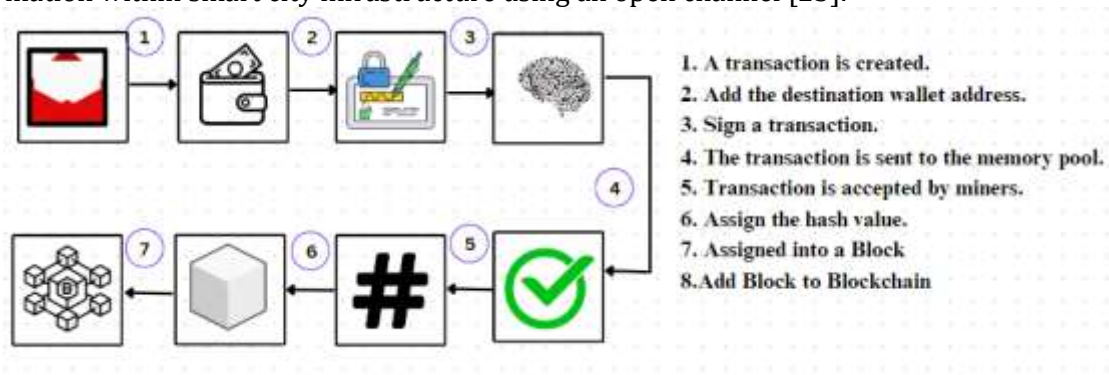

Figure 3: Transaction processing in BC

The BC may be developed as a sequential data structure composed of interconnected blocks, each of which encapsulates an assortment of systematically arranged transactions. Figure 3 shows the how the BC process the transaction. The Merkle tree is a binary tree structure that employs hash codes. Every block on the BC has a Merkle root hash along with many bits of information, comprising the block versions, timestamp, nonce, hash of the previous block, and difficulty level at that moment. Merkle trees, the practice of cryptography and methods for consensus are essential components that underpin distributed ledger technology. The entire tree network may be utilized when root hashing is applied. Every block comprises a comprehensive record of several transactions that have occurred subsequent to the previous transaction. When these transactions are recorded, the root hashing reflects the current state of the BC.

2. Blockchain –IoT Layered Architecture

Incorporation of BC technology into the IoT architecture [24],[25] to improve overall security and IoT system functionality is explained in this segment. To connecting to the BC network, IoT devices use gateways. The IoT devices can undergo basic authentication and security checks through these gateways before being allowed to connect to the network. Figure 4 illustrate the layered architecture of BC integrated IoT.

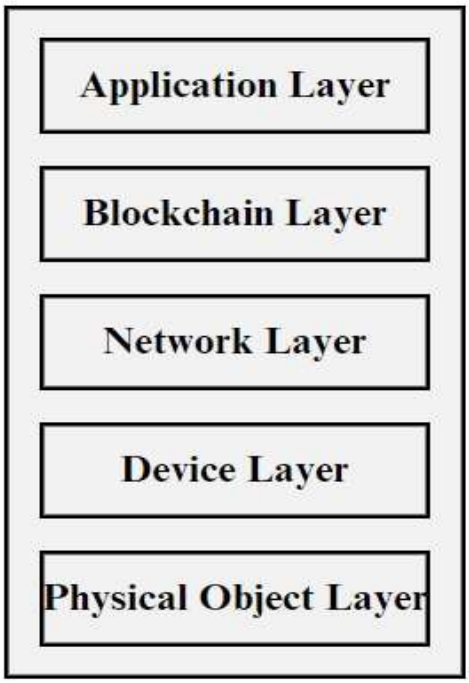

Figure 4: Layered architecture of BC-IoT

- **Application Layer:** Apps developed using BC technology and chain code are included in this layer. Through interfaces to this layer, the applications which comprise software, web-based applications, user interfaces, and protocols often communicate with the BC system.
- **BC Layer:** The establishment of consensus is a basic and essential aspect within the context of BC technology. This layer provides environment for the implementation of the smart contract and consensus methods for preserving the block chain's consistency in order, integrity, security, transaction validation, and prevention of double spending
- **Network Layer:** This layer oversees transaction identification and distribution, besides the distribution of blocks, inside the IoT ecosystem. This implies that the nodes will autonomously identify one another and establish connections, facilitating the exchange and sending of data to enhance the existing situation of the BC system.
- **Device Layer:** Here, the raw facts will be fetched. This layer comprises the radio frequency identification tags (RFIDs), sensors, transducers, actuators, smart phones, and other devices that make up the IoTs.
- **Physical Object Layer:** This layer will include any physical real-world object that is able to link to the IoTs, including people, animals, vehicles, trees, refrigerators, trains, factories, residences, and anything else that must be controlled and observed.

3. Security and Privacy concerns in IoT

The IoT presents a myriad of privacy and security concerns stemming from the interconnectedness of devices and the vast quantities of data they collect, process, and transmit. Inadequate data encryption exacerbates these risks, leaving transmitted data vulnerable to interception and manipulation. Moreover, weak authentication mechanisms

and default passwords in many IoT devices facilitate unauthorized access, potentially allowing malicious actors to take control of devices or access sensitive data. Ongoing security monitoring and updates are crucial to adapt to evolving threats and ensure the security and confidentiality of IoT ecosystems. Table 1 shows the comparative evaluation of BC use and IoT security requirements.

Table 1: The literature's comparative examination of BC in IoT security

Security Requirements	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	[34]	[35]
Integrity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓	✓	✓	✓	x	✓	✓
Authentication	✓	✓	✓	✓	x	✓	x	✓	✓	✓
Access control	x	x	✓	✓	✓	x	✓	✓	✓	✓
Privacy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Non repudiation	x	✓	✓	✓	✓	✓	✓	✓	x	x

3.1. Blockchain Solution to IoT

To address the above security and privacy concerns requires a multifaceted approach, encompassing robust encryption techniques; secure smart contract development practices, scalable BC architectures, and compliance with regulatory requirements. Table 2 summarize BC feature and its solution to IoT.

Table 2: BC technology offers several mechanisms that can enhance security and privacy in IoT deployments:

Feature	**Solution**
Immutable Data Storage	The decentralized ledger improves security by guaranteeing data integrity and preventing unauthorized tampering with IoT data.
Secure Data Sharing	IoT devices can practice smart contracts, which automatically enforce predefined rules and conditions, to securely exchange data with external systems or with each other.
Identity Management	Each IoT device can have a distinct digital identity stored on the BC. This improves privacy by blocking unauthorized devices from connecting to the link and enabling secure authentication and access control.
Data Encryption	Using cryptographic techniques, BC can enable end-to-end encryption of IoT data.
Audit ability and Transparency	BC transparent and auditable nature enables real-time monitoring and auditing of IoT transactions and data exchanges.
Consensus Mechanisms	BC consensus mechanisms guarantee all transactions are approved and verified by network users.
Decentralization	The decentralized architecture of BC removes potential points of failure and lowers the likelihood of cyber-attacks or data breaches.
Smart Contracts	Smart contracts automate and uphold agreements between IoT devices, guaranteeing that data exchanges and transactions take place safely and in accordance with predetermined guidelines.

4. Recent Trends in BC Enabled IoT

The BC technology has engrossed extensive attention because to its safe method of conducting transactions between several organizations without relying on a trusted intermediary, additionally to its ability to confirm the accuracy of information. BC

technology is becoming prevalent throughout many professional sectors, including retail, healthcare, and scientific domains. Following are the recent trends of BC in IoT.

- ✓ **Tokenization of IoT Assets**: Bringing the physical objects to the digital tokens stored in BC or programmable money. Today's most significant platform for token generation is the Ethereum BC. Tokens serve as a digital representation of a physical object, enabling algorithms and Smart Contracts to access objects and rendering the actual realm "tangible" for the digital world.
- ✓ **NFTs in IoT**: Non-Fungible Tokens are distinct, non-transferable tokens that permit the tracking of tangible or intangible assets (like collectible artwork or notaries instruments). With in the framework of IoTs, the ability to access resources or services is an example of a non-physical possession.
- ✓ **Cross-Chain Integration**: Creating tools that make it easier for various BC networks to exchange information and data, allowing an IoT ecosystem that is more interconnected and compatible.
- ✓ **BC as a Service (BaaS)**: Using BaaS platforms to accomplish it easier for enterprises without an abundance of BC experience to develop and implement BC-enabled IoTs applications.
- ✓ **Consortium BC Adoption**: Creation of sector-specific consortia that use BC technology to solve shared problems in manufacturing, logistics, and healthcare, encouraging cooperation between various stakeholders.
- ✓ **Integration with AI and Machine Learning**: Exploring how BC, IoT and AI/ML can work together to enable more intelligent automation and decision-making in IoT system.

5. Hazards in using BC with IoT

Together, BC and IoT technology have the potential to address a no. of issues, including storing and monitoring data, providing services, and determining the location of devices. But in the process of implementing an integrated plan, some of the following things could go wrong. A few of the difficulties encountered in implementing the BC-IoT architecture were itemized in Table 3.

Table 3. Different Hazards in BC-IoT

Hazards in BC-IoT	Description of each Hazard
Scalability	Because there are so many devices in the IoT that are connected, scaling authentication and security using BC is difficult.
Privacy	BC technology offers openness and immutability, yet privacy concerns arise. IoT device data on a BC may reveal critical information to all network participants. Privacy and secrecy of IoT data while using BC technology is difficult.
Security	BC networks are very young and need security improvements. Sybil attacks, when attackers create numerous phony identities to take control of BC networks, are one example.
Resource Constraints	IoT devices might not be capable to run computationally intensive BC due to resource limits

Energy Consumption	Limited resource IoT devices might not be able to use BC for network security due to its energy requirements.
Compatibility & Interoperability	Integration of IoT devices and BC systems may be problematic. A BC-based authentication and different protocols or operating systems may cause an IoT device's security system to malfunction.
Regulatory & Legal Constraints	BC in IoT security may raise legal and regulatory concerns.
Reliance on centralized components	BC technology aims to decentralize and spread security; however, IoT security systems may still employ authentication servers or smart contracts.
User acceptance and usability	BC technology is sophisticated, which may hinder end-user usability.
Lack of Standardization	Unstandardized frameworks and protocols for BC and in IoT security can hinder implementation.

6. Conclusion

Subsequently there are more IoT devices than ever before, security has grown to be a critical concern. This paper presents a comprehensive analysis of security and privacy threads in IoT. Further this review focuses on discussing the integration of Blockchain with IoT. From this review, BC technology is one of the most promising fields with a lot of potential for improving the security and privacy of IoT data which helpful for future research. This review also identifies the some of the difficulties faced while integrating BC with IoT.

References

[1] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)."

[2] "A Study on the Basics of IoT and its Essential Needs to Develop Real World Applications," 2019. [Online]. Available: https://www.researchgate.net/publication/353886847

[3] S. R. Jino Ramson, S. Vishnu, and M. Shanmugam, "Applications of Internet of Things (IoT)-An Overview," in ICDCS 2020 - 2020 5th International Conference on Devices, Circuits and Systems, Institute of Electrical and Electronics Engineers Inc., Mar. 2020, pp. 92–95. doi: 10.1109/ICDCS48716.2020.243556.

[4] S. S. Chouhan, U. P. Singh, and S. Jain, "Automated Plant Leaf Disease Detection and Classification Using Fuzzy Based Function Network," Wirel Pers Commun, vol. 121, no. 3, pp. 1757–1779, Dec. 2021, doi: 10.1007/s11277-021-08734-3.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey." [Online]. Available: www.elsevier.com/locate/comnet

[6] Institute of Electrical and Electronics Engineers. Kerala Section and Institute of Electrical and Electronics Engineers, 2020 International Conference on Innovative Trends in Information Technology (ICITIIT).

[7] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A Blockchain-Based Framework for Integrity and Privacy-Preserving Data Sharing in Smart Cities." [Online]. Available: https://orcid.org/0000-0002-7154-4561

[8] K. Witkowski, "Internet of Things, Big Data, Industry 4.0 - Innovative Solutions in Logistics and Supply Chains Management," in Procedia Engineering, Elsevier Ltd, 2017, pp. 763–769. doi: 10.1016/j.proeng.2017.03.197.

[9] M. Sreerama Murthy, R. P. Ram Kumar, B. Saikiran, I. Nagaraj, and T. Annavarapu, "Real Time Weather Monitoring System using IoT," in E3S Web of Conferences, EDP Sciences, Jun. 2023. doi: 10.1051/e3sconf/202339101142.

[10] B. Bhandari, R. Patel, A. Tiwari, N. Sharma, and S. Thawait, "Role of IoT in Agriculture in India in Water Irrigation," Int J Res Appl Sci Eng Technol, vol. 11, no. 5, pp. 6520–6524, May 2023, doi: 10.22214/ijraset.2023.53257.

[11] D. V. Gowda, S. M. Prabhu, M. Ramesha, J. M. Kudari, and A. Samal, "Smart Agriculture and Smart Farming using IoT Technology," in Journal of Physics: Conference Series, IOP Publishing Ltd, Nov. 2021. doi: 10.1088/1742-6596/2089/1/012038.

[12] Poorva Sanjay Sabnis and Snehal Shewale, "The use of IoT in Health Care System: A Perspective," COMPUTING TRENDZ, vol. 11, no. 1,2, pp. 30–36, Aug. 2023, doi: 10.21844/cttjetit.v11i1-2.1.13004.

[13] K. Naik and S. Patel, "An open source smart home management system based on IOT," Wireless Networks, vol. 29, no. 3, pp. 989–995, Apr. 2023, doi: 10.1007/s11276-018-1884-z.

[14] G. Wang, A. El Saddik, X. Lai, G. Martinez Perez, and K.-K. R. Choo, Eds., Smart City and Informatization, vol. 1122. in Communications in Computer and Information Science, vol. 1122. Singapore: Springer Singapore, 2019. doi: 10.1007/978-981-15-1301-5.

[15] V. Potdar, A. Sharif, and E. Chang, "Wireless sensor networks: A survey," in Proceedings - International Conference on Advanced Information Networking and Applications, AINA, 2009, pp. 636–641. doi: 10.1109/WAINA.2009.192.

[16] S. P. Sasirekha, A. Priya, T. Anita, and P. Sherubha, "Data Processing and Management in IoT and Wireless Sensor Network," in Journal of Physics: Conference Series, IOP Publishing Ltd, Dec. 2020. doi: 10.1088/1742-6596/1712/1/012002.

[17] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," Journal of Network and Computer Applications, vol. 181. Academic Press, May 01, 2021. doi: 10.1016/j.jnca.2021.103050.

[18] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," in Procedia Computer Science, Elsevier B.V., 2018, pp. 116–121. doi: 10.1016/j.procs.2018.01.019.

[19] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in International Conference on Information Networking, IEEE Computer Society, Apr. 2018, pp. 473–475. doi: 10.1109/ICOIN.2018.8343163.

[20] Vivekanadam B, "Analysis of Recent Trend and Applications in Block Chain Technology," Journal of ISMAC, vol. 2, no. 4, pp. 200–206, Oct. 2020, doi: 10.36548/jismac.2020.4.003.

[21] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He, and K. C. Li, "Data Fusion Approach for Collaborative Anomaly Intrusion Detection in Blockchain-Based Systems," IEEE Internet Things J, vol. 9, no. 16, pp. 14741–14751, Aug. 2022, doi: 10.1109/JIOT.2021.3053842.

[22] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business and Information Systems Engineering, vol. 59, no. 3, pp. 183–187, Jun. 2017, doi: 10.1007/s12599-017-0467-3.

[23] P. Kumar et al., "PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities," IEEE Trans Netw Sci Eng, vol. 8, no. 3, pp. 2326–2341, Jul. 2021, doi: 10.1109/TNSE.2021.3089435.

[24] M. Kumar, Nidhi, S. Tiwari, and S. Kaur, “Blockchain-IoT Layered Architecture, Current Trends, Challenges, and Applications,” in 7th International Conference on Trends in Electronics and Informatics, ICOEI 2023 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 688–694. doi: 10.1109/ICOEI56765.2023.10126036.

[25] B. B. Pannayagol and S. Deshpande, “Security in Internet of Things: An Overview,” in Proceedings - IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 243–248. doi: 10.1109/DICCT56244.2023.10110070.

[26] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” in Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (part of CPS Week), Association for Computing Machinery, Inc, Apr. 2017, pp. 173–178. doi: 10.1145/3054977.3055003.

[27] A. G. Abbasi and Z. Khan, “Veidblock: Verifiable identity using blockchain and ledger in a software defined network,” in UCC 2017 Companion - Companion Proceedings of the 10th International Conference on Utility and Cloud Computing, Association for Computing Machinery, Inc, Dec. 2017, pp. 173–179. doi: 10.1145/3147234.3148088.

[28] IEEE Communications Society. Internet of Things Emerging Technologies Initiatives, IEEE Computational Intelligence Society, Institute of Electrical and Electronics Engineers, and S. Internet of Things Week (2017 : Geneva, GIoTS2017 : Global Internet of Things Summit : 2017 proceedings papers : CICG, Geneva, June 6-9, 2017.

[29] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, “Blockchain Based Data Integrity Service Framework for IoT Data,” in Proceedings - 2017 IEEE 24th International Conference on Web Services, ICWS 2017, Institute of Electrical and Electronics Engineers Inc., Sep. 2017, pp. 468–475. doi: 10.1109/ICWS.2017.54.

[30] Institute of Electrical and Electronics Engineers, 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm) : 25-28 Sept. 2017.

[31] P. N. Astya, Galgotias University. School of Computing Science and Engineering, Institute of Electrical and Electronics Engineers. Uttar Pradesh Section, and Institute of Electrical and Electronics Engineers, IEEE International Conference on Computing, Communication and Automation (ICCCA 2017) : proceeding : on 5th-6th May, 2017.

[32] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, “IoT information sharing security mechanism based on blockchain technology,” Future Generation Computer Systems, vol. 101, pp. 1028–1040, Dec. 2019, doi: 10.1016/j.future.2019.07.036.

[33] S. Rathore, B. Wook Kwon, and J. H. Park, “BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network,” Journal of Network and Computer Applications, vol. 143, pp. 167–177, Oct. 2019, doi: 10.1016/j.jnca.2019.06.019.

[34] Global IT Research Institute, IEEE Communications Society, and Institute of Electrical and Electronics Engineers, The 21st International Conference on Advanced Communications Technology: “ICT for 4th Industrial Revolution!” : ICACT 2019 : Phoenix Park, Pyeongchang, Korea (South), Feb. 17 ~ 20, 2019 : proceeding & journal.

[35] M. Li and Y. Qin, “Scaling the Blockchain-based Access Control Framework for IoT via Sharding,” in IEEE International Conference on Communications, Institute of Electrical and Electronics Engineers Inc., Jun. 2021. doi: 10.1109/ICC42927.2021.9500403.