WSNs USING BLOCKCHAIN TECHNOLOGY

Piyush Raja, Assistant Professor, Department of CSE, College of Engineering Roorkee, Roorkee, Uttarakhand, India
Dr. Santosh Kumar, Assistant Professor, Department of CSE, College of Engineering Roorkee, Roorkee, Uttarakhand, India
Dr. Taresh Singh, Professor, Department of CSE, College of Engineering Roorkee, Roorkee, Uttarakhand, India

Abstract
Wireless sensor networks are now often used in both civil and military purposes, among many other areas of human existence. WSNs may, however, provide a variety of advantages and conveniences. However, because to its centralized server/client approach, the WSNs presents a number of issues when used in the real world, including security and storage. As a result, the distributed model must be used in the WSNs system. Blockchain is one of the most recent distributed systems in use today. Blockchain is a decentralized technology that can improve WSN security, computation, and administration. The advantages and difficulties of integrating Blockchain technology into WSNs are highlighted in this article's review of the topic. We may draw the conclusion that adopting Blockchain technology to address the security and distributed storage issues for WSNs can be a successful strategy. It may open the door for fresh lines of inquiry and distributed applications.

Keywords: Distributed, centralized, wireless sensor networks, security concerns**.**

1. Introduction

Thousands of inexpensive nodes, or sensing devices, make up wireless sensor networks. The physical environment is monitored and recorded by these sensing devices via factors like temperature, sound, pollution levels, etc. WSN serves as a link between the real and virtual worlds. WSN has a variety of uses, including environmental monitoring, healthcare, smart cities, and military applications. These sensors are placed where they will serve the intended purpose. In the conventional WSN-based system, data is sent through insecure public channels between regular sensor nodes and sink nodes. It's possible that the attacker may get access to it [1]. The sink nodes may internally or externally store the gathered data. Both types of storage systems produce a centralized database as a consequence, which raises a number of security concerns including single points of failure and centralized malicious attacks, among others.

Blockchain is a technology that permits safe data transfer based on a very intricate encryption scheme, much like an organization's accounting ledger, where data is carefully regulated and records all transactions on the peer-to-peer network. Each block has a creation time stamp and is connected to the one before it by hash code and transaction information. There is no way to modify data after the network has recorded it [2,3]. Blockchain technology is designed to thwart fraud and data tampering.

In comparison to the current WSN system without the trusted third party, the Blockchain-based WSN system offers improved security and trust. A trustworthy decentralized method for storing sensory data is offered by BWSN [4]. The single-point-of-failure issue is thus unfounded. When sensor nodes communicate information with other nodes or the central server, conditional anonymity is provided. Because several sensor nodes, such as sink nodes, maintain the same copy of the Blockchain, it offers immutable and chronologically ordered blocks as well as transparency in the WSN. Additionally, BWSN offers validation of sensory data by additional sink nodes based on consensus.

2. Problems with WSNs

The following is a quick discussion of the difficulties with wireless sensor networks:

A. Power

Sensors need some energy or power reserves to perform various tasks when necessary. A major problem in WSN is energy management [15, 16]. The associated battery that powers nodes often has a finite capacity. Sensing, gathering, analyzing, and broadcasting data to the sink node use up this energy. Instead of instruction processing, transmission often consumes the majority of energy. On average, processing 3,000 instructions uses the same amount of energy as radio transmission of a single bit across a distance of 100 m. For sink node registration or BSs inquiries, sensors must also be operational. Nodes accomplish nothing useful during this period while wasting the energy that has been used. As a result, transmission, reception, and idle operation use the available energy [17].

B. Routing and Communication

Finding a communication path from each sensor node to the BS is a difficult aspect of the network architecture. Keeping the nodes alive for a long time is often the goal. Since the nodes often only provide limited coverage for communication, intermediate forwarding nodes are used. The WSN's communication profile and general performance are directly impacted by the deployment method and routing protocols [4,7]. Nodes in WSNs function wirelessly, which is distinct from typical routing in other networks in several ways. Due to the absence of a wired infrastructure, wireless media routing is often less dependable than wired media routing. When some type of local organization into cluster cells is used, WSN nodes normally transfer information hop-by-hop to sink, directly to the base station, or through cluster heads.

C. Safety

Another significant WSN concern is security. Data from WSNs are sent wirelessly across the air, and as these wireless signals are public, anybody may see and take part in the conversation even without being invited [19]. Most WSN nodes work in the license-free Independent Side Band (ISB). Security is thus essential in both commercial and military applications to thwart harmful assaults like unauthorized access and DoS attacks. Following are some categories for security demands for WSNs:

1. Information confidentiality refers to the guarantee of authorized access to information. The fact that the radio spectrum is an open channel and may be readily observed by anybody [20, 21] presents a significant security concern in the wirelessly operated network. An attacker may, for example, sniff the sent packet and tamper with it. To protect data secrecy, it is usual practice to only transfer data after it has been encrypted using a secret key that only intended recipients are in possession of.
2. Information authenticity: In addition, if an attacker learns the packet format used by the WSN protocol stack, he may introduce a new, deceptive packet into the connection between nodes. The information carried by the injected packet is thus false or misleading [6,8]. Such implanted false information may be used to hijack monitoring, tracking, and surveillance apps. To get around this, common techniques like message authentication codes, signatures, secret keys, and broadcasting authentication may be used to ensure data authenticity.
3. Information integrity: Because wireless channels are unstable, mistakes are a given in WSNs. Due to signal fading, reflection, diffraction, scattering, and different types of noise, information that is travelling across electromagnetic medium may need to be retransmitted [9, 11]. In the WSN, a large number of re-transmissions may be quite costly in terms of energy use. Message integrity codes may be used to guarantee data integrity.

D. Accessibility

It's crucial for sensor nodes to have a prolonged lifespan, particularly in applications that are crucial. Early battery drain on a sensor node's power supply is caused by using energy for extraneous or unneeded communication and processing. Energy-efficient routing methods and protocols are necessary to ensure node availability [12, 13].

E. OS

The sensor node operating system must offer crucial resource management and memory management since sensor nodes have a finite amount of memory, low power, and compact size. Compared to standard OS, it ought to be simpler. For wireless sensor networks, Mantis OS, Nano-Q, and TinyOS have been configured particularly [15]. To take into account the developments in the WSN design paradigm, improvements are essential.

F. Software and hardware problems

The power and speed of executing program instructions are an issue for WSNs since sensor devices are constrained in size and have finite memory space. The sensor device typically includes a transceiver, microprocessor, power backup, and sensor [16, 18]. The sensor collects data and then transmits it for processing to a microcontroller. The microcontroller carries out software commands and uses the transceiver to transmit the gathered data to the sink device. The WSN communication and processing protocols are managed by the microcontroller. Since flash memory is speedy and affordable, using flash memory devices is advised [17]. The three operating modes of idle, active and sleep must be used by sensor nodes in order to safeguard the microcontroller power.

G. The MAC Layer Problem

Much of the energy loss in a wireless sensor network happens at the MAC layer as a result of collision, empty hearing packet overhead, and busy traffic. Idle nodes need 50 to 100% of their power to receive packets while they are idle. To solve this problem, the Sensor-MAC periodic hearing and rest protocol is suggested [19]. The duty cycle is trimmed in this protocol so that nodes are only active when necessary and nodes are allowed to choose their own listening and rest schedules. If no data is received during a period of time, nodes choose a schedule and transmit synchronization information to the BS. Timeout MAC, Dynamic sensor MAC, and Traffic-Adaptive MAC are three more MAC protocols. Each follows a distinct protocol and has advantages and disadvantages.

H. Synchronization of Time

Field sensor nodes are separately operated. The information detected may be ambiguous or imprecise if their local clocks are not in sync with those of other nodes [19].

3. Model of the system and its benefits

In conventional WSNs, many devices will access data through a centralized network via a centralized server. Figure 1 depicts the procedure for gaining access to this data. However, the need for large-scale network applications and the number of devices connected to the network are growing. As a result, having a centralized server is no longer a viable strategy for WSN systems on a wide scale. The most cutting-edge technology must be included into the WSNs system. One of the best ways to deal with this issue is to employ distributed networks, which may be used for "Peer-to-Peer Networking, Distributed File Sharing, and Autonomous Device Coordination" activities. The usage of Blockchain technology enables the WSNs system to keep track of a sizable number of networked devices, particularly for WSNs that need application growth. The use of Blockchain technology will significantly increase the security and dependability of the WSNs system, which can coordinate the management of connections between devices. In addition, the distributed ledger shown in Figure 1 enables the WSNs system to handle peer-to-peer connections fast.

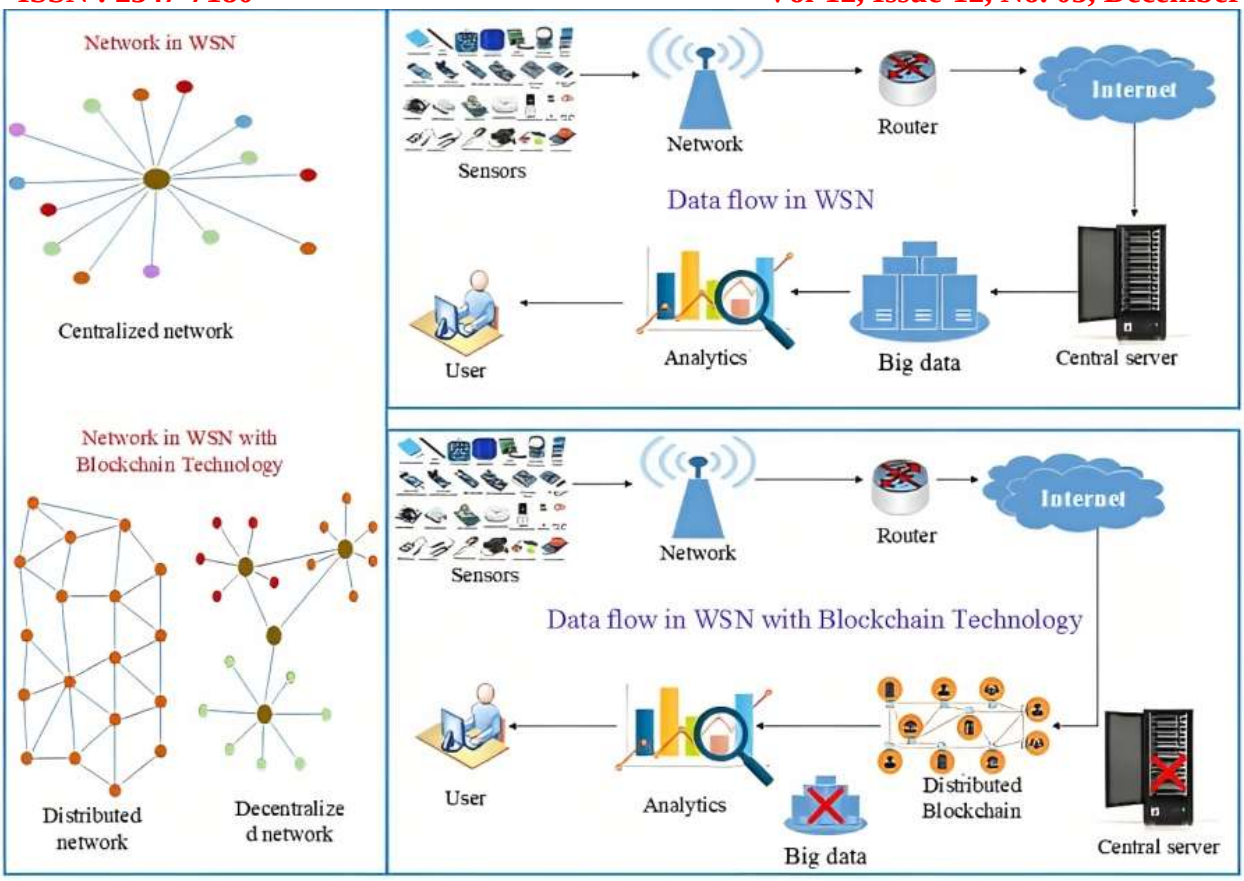

Figure 1: Data flow in WSNs, WSNs network types, and WSNs networks using Blockchain technology.

The two data flow procedures in conventional WSNs and BC-integrated WSNs vary from one another. Blockchain-enabled WSNs do not utilize centralized data centers for their data storage. WSNs with integrated BC employ the same technology as conventional WSNs, but since there is no longer a centralized server, data that is sent to the Internet passes via the distributed Blockchain. The Blockchain's distributed ledger has made data authentication and data manipulation easier to detect. By using BC technology, the data transfer will also become more dependable and secure.

WSNs with Blockchain	**WSNs without Blockchain**
Decentralized	Centralized
Distributed ledger	Client- server architecture
High power consumption	Low power consumption
High security	Low security
Requires a device with a large processing speed and storage capacity	WSNs devices have limited processing speed and storage capacity
More difficult to implement and maintain	Simple to implement and maintain

Table 1 presents a comparison between WSNs systems without Blockchain technology and WSNs systems with integrating Blockchain technology.

The use of Blockchain technology in WSN can bring a lot of benefits such as greatly reducing costs because it does not need to maintain a centralized data storage center, will distribute computing needs, data is stored on all devices in the network.

The outstanding characteristics of Blockchain technology such as decentralization, reliability, and security make it an ideal solution to solve the challenges facing WSNs. Due to the transparency of data

in the Blockchain, users can track the data when they want. In addition, transactions in the network need to use confirmation and participant consent to prevent tampering.

3. Challenges in Research

Everyone recognize that blockchain technology has a lot of advantages. Blockchain, however, is not a flawless technology; it also has its drawbacks and difficulties, and users must make trade-offs when using them. These difficulties may be summed up as follows:

A. Scalability: As the size of the WSNs grows, the distributed nature of the blockchain may be lost. As the number of nodes in WSNs rises, many properties of Blockchain will also. Given the enormous demands for WSN growth, this is seen as one of the major constraints.

B. Power use and processing speed: The criteria for blockchain technology are highly tight in terms of power usage, computing power, and processing speed. The majority of the devices in WSNs, though, are low-power ones. Additionally, there are several devices in WSNs that do not have coordinated power use, computational power, and processing speeds. As a result, implementing blockchain in WSNs is quite challenging.

C. Storage: One of the main benefits of Blockchain is the elimination of the central server paradigm by using a distributed ledger to record transactions and device IDs across the network. These ledgers are, however, kept in each network node, where their size will grow over time. Additionally, when the network has to be expanded, there are more network nodes. WSN devices, on the other hand, offer little computation and storage capabilities. Therefore, substantial modifications to the WSN infrastructure will be needed in order to use Blockchain technology.

D. Lack of knowledge: Because Blockchain technology is still relatively new, there aren't many individuals who are familiar with it. In the meanwhile, many apps demand that users have a firm grasp of how Blockchain works. We use WSNs all around us, thus it is essential that the general public be aware of them before using Blockchain in WSNs.

E. Legal and compliance issues: Since Blockchain technology connects many devices from across the globe without adhering to any norms or rules, manufacturers and service providers face difficulties and many firms are wary of using Blockchain technology.

4. Conclusion

Thanks to the rapid advancement of sensor technology, gathering data from the environment has become simpler. Consequently, thanks to the advantages that wireless sensor networks provide, people's lives will be considerably improved. Although there are still significant restrictions due to the server/client paradigm that the present WSN architecture is built on, particularly in terms of scalability, security, and distributed data storage. This is seen as a practical way to get around the aforementioned restrictions thanks to the excellent benefits brought about by the development of Blockchain technology. We have outlined the advantages and difficulties of using Blockchain technology with WSN in this paper. Finally, we can demonstrate that the inclusion of Blockchain technology will address the WSN's shortcomings. Additionally, it brings about a lot of brand-new difficulties. As a result, additional study is still required to examine the use of Blockchain technology in the WSN network.

References

[1] M. T. Nguyen, Huy Tran Van, Giap Nguyen Trong, Khoi H. Do, "Wireless Communication Technologies and Applications for Wireless Sensor Networks: A Survey," ICSES Transactions on Computer Networks and Communications, vol. 5, no. 1, pp. 1-15, Apr. 2019.

[2] Nguyen, Minh T. “Data collection algorithms in wireless sensor networks employing compressive sensing”, Dissertation Oklahoma State University, 2016.

[3] Minh T. Nguyen, Hien M. Nguyen, Antonino Masaracchia, Cuong V. Nguyen, "Stochastic-Based Power Consumption Analysis for Data Transmission in Wireless Sensor Networks" EAI Transactions on Industrial Networks and Intelligent Systems Issue 19, Vol. 6, June 2019.
[4] Anjum and P. Mouchtaris, Security for wireless ad hoc networks. John Wiley & Sons, 2007.
[5] S. Datema, "A case study of wireless sensor network attacks," Master's Thesis in Computer Science, Parallel and Distributed Systems Group, 'Faculty of Electrical Engineering, Mathematics, and Computer Science', Delft University of Technology, September, 2005.
[6] Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Communications of the ACM, vol. 47, no. 6, pp. 53–57, 2004.
[7] Zia and A. Zomaya, "Security issues in wireless sensor networks," in2006 International Conference on Systems and Networks Communications (ICSNC'06), pp. 40–40, IEEE, 2006.
[8] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, vol. 1, no. 367, p. 6, 2007.
[9] S. Singh and H. K. Verma, "Security for wireless sensor network," International Journal on Computer Science and Engineering, vol. 3, no. 6, pp. 2393–2399, 2011.
[10] A. MANJUNATHAet al., "Review on security in wireless sensor network," Journal of Critical Reviews, vol. 7, no. 11, pp. 3533–3536, 2020.
[11] A. Stanciu, "Blockchain based distributed control system for edge computing," in 2017 21st International Conference on Control Systems and Computer Science (CSCS), pp. 667–671, IEEE, 2017.
[12] A. Banafa, "Iot and blockchain convergence: benefits and challenges," IEEE Internet of Things, 2017.
[13] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in IEEE EUROCON 2017-17th International Conference on Smart Technologies, pp. 763–768, IEEE, 2017.
[14] S.-Y. Wang, Y.-J. Hsu, and S.-J. Hsiao, ''Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innova- tive implementation,'' in Proc. Int. Symp. Comput., Consum. Control (ISC), Dec. 2018, pp. 149–152.
[15] S. A. Imam, M. K. Singh, V. K. Sachan, A. Choudhary, and A. M. Zaidi, ''An energy-efficient data transmission scheme based on DSC-MIMO for wireless sensor network,'' in Proc. 2nd IEEE Int. Conf. Integr. Circuits Microsyst. (ICICM), Nov. 2017, pp. 309–312, doi:10.1109/ICAM.2017.8242191.
[16] J. O. Ogbebor, A. L. Imoize, and A. A.-A. Atayero, ''Energy efficient design techniques in next-generation wireless communication networks: Emerging trends and future directions,'' Wireless Commun. Mobile Comput., vol. 2020, Mar. 2020, Art. no. 7235362, doi: 10.1155/2020/7235362.
[17] O. Alamu, A. Gbenga-Ilori, M. Adelabu, A. Imoize, and O. Ladipo, ''Energy efficiency techniques in ultra-dense wireless heterogeneous networks: An overview and outlook,'' Eng. Sci. Technol., Int. J., vol. 23, no. 6, pp. 1308–1326, Dec. 2020, doi: 10.1016/j.jestch.2020.05.001.
[18] E. Choudhari, K. D. Bodhe, and S. M. Mundada, ''Secure data aggregation in WSN using iterative filtering algorithm,'' in Proc. Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA), Feb. 2017, pp. 1–5, doi: 10.1109/ICIMIA.2017.7975603.
[19] X. Liu, M. Jia, X. Zhang, and W. Lu, ''A novel multichannel Internet of Things based on dynamic spectrum sharing in 5G communication,'' IEEE Internet Things J., vol. 6, no. 4, pp. 5962–5970, Aug. 2019, doi: 10.1109/JIOT.2018.2847731.
[20] J. C. Kwan and A. O. Fapojuwo, ''Radio frequency energy harvesting and data rate optimization in wireless information and power transfer sensor networks,'' IEEE Sensors J., vol. 17, no. 15, pp. 4862–4874, Aug. 2017, doi: 10.1109/JSEN.2017.2714130.
[21] K. Fan, Y. Ren, Z. Yan, S. Wang, H. Li, and Y. Yang, ''Secure time synchronization scheme in IoT based on blockchain,'' in Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData), Jul. 2018, pp. 1063–1068, doi: 10.1109/ Cybermatics_2018.2018.00196.