Blockchain Technology in Wireless Sensor Network: Benefits and Challenges.

Cuong V. Nguyen [a,*], Minh T. Nguyen[b], Trang T.H. Le[b], Thang A. Tran[b], Duy T. Nguyen[b]
[a]Thai Nguyen University of Information and Communication technology
[b] Thai Nguyen University of Technology, Thai Nguyen City, Viet Nam
* Corresponding Author: Cuong V. Nguyen: nvcuong@ictu.edu.vn;

Submitted: August, 10th, 2021 — Accepted: September, 15th, 2021 — Published: December, 2021

Abstract— Nowadays, wireless sensor networks are being widely applied in many fields of human life such as civil and military applications. Although WSNs can bring a lot of benefits and conveniences. However, when applying the WSN in the real world we have to face many challenges such as security, storage due to its centralized server/client model. Therefore, it is necessary to apply the distributed model in the WSNs system. One of the newest distributed systems today is Blockchain (BC). Blockchain is a decentralized technology that can help the computation and management processes as well as security in WSNs. This article provides an overview of Blockchain integration in WSN with highlighting the benefits and challenges of applying this technology to WSN. We can conclude that using Blockchain technology to solve the problem of security and distributed storage for WSN can be an effective approach. It could pave the way for new research directions and distributed applications.

Keywords— Blockchain, Wireless sensor networks, Security issues, Centralized, Distributed.

I. INTRODUCTION

Security is not only a concern of WSNs but also a challenge for any network. In WSN security plays a very important role, it ensures the success or failure of the application. Usually, sensor nodes are deployed randomly or according to a calculated model, they interact closely with the surrounding environment [1, 2, 3]. These sensor nodes operate unattended or without any remote monitoring system. That means they are working in an environment that is vulnerable to hackers and has a great risk of being tampered with. Hackers can attack sensor networks using physical methods. In addition. In addition, taking advantage of some mistakes in the network deployment process and hackers can attack the network as described in paper [4-7]. Besides, because WSN is limited in terms of resources such as low storage power, due to very low power consumption, computing power for complex algorithms is limited, so it depends on different applications that have different security requirements leading to difficulties in synchronization. The requirements for some security features to be achieved when designing a WSN were presented in [8-10].

Blockchain is a technology that allows the transmission of data securely based on an extremely complex encryption system, similar to a company's accounting ledger, where data is closely monitored and record all transactions on the peer-to-peer network. Each block contains information about its creation time and is linked to the previous block by hash code and transaction data. Once the data is recorded by the network, there is no way to change it. Blockchain is designed to resist fraud and alteration of data [11].

Integrating blockchain technology into WSNs will bring a lot of benefits. A large number of connections between sensor devices will be handled thanks to the distributed nature of blockchain. This will significantly decrease the costs associated with installing and maintaining large centralized data centers. At the same time, computing and storage needs are distributed to all devices in the network. In addition, when blockchain technology is integrated into WSNs, it will eliminate the centralized architecture of WSNs [12]. Furthermore, the Centralized Server and Client Model will be eliminated when peer-to-peer messaging, file distribution, and automatic coordination between devices in the network [13, 14].

II. THE SYSTEM MODEL AND BENEFITS

In traditional WSNs, data will be accessed using a centralized network by different devices through a central server. The process of accessing this data is shown in Figure 1. However, the number of devices participating in the network and the demand for large-scale network applications are increasing. Therefore, using a centralized server is no longer an effective approach for large-scale WSN systems. The WSNs system requires the integration of the most advanced technologies. The use of distributed networks will be one of the effective solutions to solve this problem where "Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC)" functions could be capable. The use of Blockchain (BC) technology allows the WSNs system to monitor a large number of devices in the network, especially in the case of WSNs with application expansion needs. The WSNs system can coordinate the handling of connections between devices, and the security and

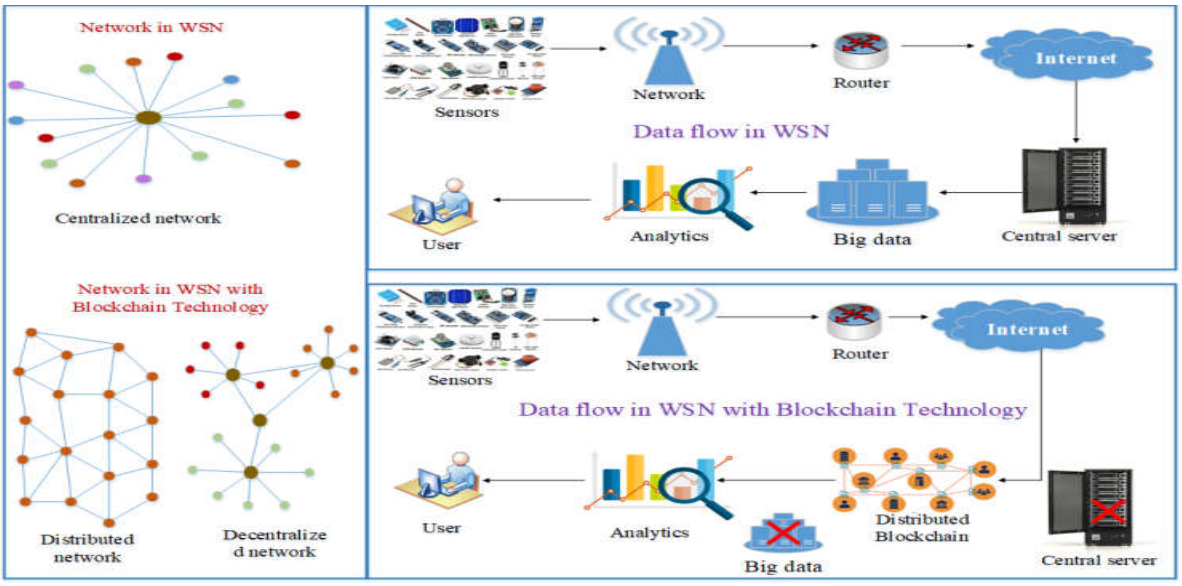

Figure 1. WSN network types, data flow in WSN, data flow in WSN with Blockchain technology.

reliability of the system will be greatly enhanced by integrating BC technology. In addition, the WSNs system can handle peer-to-peer connections quickly with the help of a distributed ledger as shown in Figure 1.

We can see the difference between the two data flow processes in BC-integrated WSNs and traditional WSNs. The data in WSNs with Blockchain does not use centralized data centers. In WSNs integrated BC technology is the same as traditional WSNs but when the data goes to the Internet the data will go through the distributed Blockchain because the centralized server has been eliminated. Thanks to the distributed ledger in the blockchain, data authentication, and data tampering have become better. The data flow will also become more reliable and secure with the application of BC technology.

TABLE I
COMPARISION BETWEEN TYPES OF WSNs

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	WSN 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.

III. RESEARCH CHALLENGES

We can see a lot of benefits that Blockchain can bring. However, Blockchain is not a perfect technology, it also has its flaws and challenges, when applying them users also need to trade-off some characteristics. These challenges can be summarized as follow:

Scalability: Blockchain's distributed character may be lost as the scale of the WSNs expands. Many characteristics of Blockchain will decrease as the number of nodes in WSNs increases. This is considered as one of the significant limitations because the expansion needs of WSNs are huge.

Power consumption and processing time: Blockchain requirements on power consumption, computing power as well as processing time are very strict. Meanwhile, the devices in WSNs are mostly low-power devices. In addition, in WSNs there are many different devices that are not synchronized in terms of power consumption, computing power, and processing speed. Therefore, the application of Blockchain in WSNs faces many difficulties.

Storage: Using a distributed ledger to store transactions and device IDs in the network and eliminating the central server model is one of the key advantages of Blockchain. However, these ledgers are stored in each network node, the size of which will increase over time. Moreover, the number of

Manuscript ID = 0396 — ISSN: 2588-5847
Website: www.i-cses.com — E-mail: info@i-cses.com

network nodes is increasing due to the need to expand the network. Meanwhile, devices in WSNs have low computing power and storage capacity. Therefore, the application of Blockchain technology will require significant changes to the infrastructure of WSNs.

Lack of skills: The number of people who know about Blockchain technology is still limited because it is a quite new technology. Meanwhile, many applications require users to have a clear understanding of how Blockchain works. WSNs are applied everywhere around us, so in order to apply Blockchain in WSNs, it is necessary to have public awareness about Blockchain.

Legal and Compliance issues: Blockchain technology can connect different devices from all over the world without following any standards or laws, which are challenges for manufacturers and service providers and make many businesses afraid to use Blockchain technology.

IV. CONCLUSIONS

Collecting data from the surrounding environment becomes easier thanks to the strong development of sensor technology. Thus, greatly improving people's lives due to the benefits that wireless sensor networks bring. However, the current WSN architecture is based on the server/client model, so there are still many limitations, especially scalability, security, and distributed data storage. With outstanding advantages in the emergence of Blockchain technology, this is considered an effective solution to overcome the above limitations. In this article, we have provided an overview of the benefits and challenges of applying Blockchain technology to WSN. Finally, we can show, the participation of Blockchain technology will solve the limitations of WSN. At the same time, it also creates quite many new challenges. Therefore, we still need more research to investigate the implementation of Blockchain technology in the WSN network

ACKNOWLEDGMENTS

The authors would like to thank Thai Nguyen University of Technology, Viet Nam for the support.

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.

Cuong V. Nguyen was born in 1987 in Thai Nguyen, Viet Nam. He received his B.S. degree in Electronic and Telecommunication Engineering from Thai Nguyen University of technology and M.S degrees in Electrical Engineering from Hanoi University of Science and Technology. His research interests are in Wireless Sensor Network (WSN), Wireless Power Transfer (WPT), Internet of Thing (IoTs). He is currently a member of the Advanced Wireless Communication Networks (AWCN) Lab at Thai Nguyen University of Technology.

Dr. Minh Nguyen is currently the director of international training and Cooperation center at Thai Nguyen University of Technology, Vietnam, and also the director of Advanced Wireless Communication Networks (AWCN) Lab. He has interest and expertise in a variety of research topics in the communications, networking, and signal processing areas, especially compressive sensing, and wireless/mobile sensor networks. He serves as technical reviewers for several prestigious journals and international conferences. He also serves as Editors for Wireless Communication and Mobile Computing journal and Associated Editor for ICSES Transactions on Computer Networks and Communications.

Trang TH. Le is currently a full time lecturer at Electronics Engineering faculty, Thai Nguyen University of Technology, Viet Nam. Her research interests include wireless communication networks, telecommunication

technologies, data processing and wireless sensor networks.

Dr. Thang Tran is currently the Head of Electronics and Telecommunication Department - Electronics Faculty at Thai Nguyen University of Technology, Viet Nam. His main areas of research are Digital communication, Wireless Communication and signal processing areas, especially coding and decoding in Telecommunication fields. He also serves as reviewers for ICSES Transactions on Computer Networks and Communications and other journals, conferences.

Dr. Duy T. Nguyen received his MSc degree in information technology from Thainguyen University, Vietnam, in 2007. In 2017 he received PhD degree from Graduate University of Science and Technology, Vietnam Academy of Science and Technology, Vietnam, on Applied Mathematics. He is currently a lecturer at Thainguyen University of Technology, Thainguyen University, Vietnam. His research interests include Artificial Intelligence, Fuzzy logics, Hedge-Algebras, Engineering controls, Computing.

Manuscript ID = 0396 — ISSN: 2588-5847
Website: www.i-cses.com — E-mail: info@i-cses.com