Big Data and Computing Visions

www.bidacv.com

Big. Data. Comp. Vis. Vol. 3, No. 2 (2023) 70–75.

Paper Type: Original Article

Blockchain-Powered Wireless Sensor Networks: Enhancing Security and Privacy in the IoT Era

Ibrahim Mekawy*

Department of Mathematics, College of Science and Arts, Qassim University, Ar Rass, Saudi Arabia; im.mekawy@qu.edu.sa.

Citation:

Mekawy, I. (2023). Blockchain-powered wireless sensor networks: enhancing security and privacy in the IoT era. *Big data and computing visions, 3*(2), 70-75.

Received: 23/11/2022 Reviewed: 22/12/2022 Revised: 11/01/2023 Accept: 18/02/2023

Abstract

Nowadays, we know that Wireless Sensor Networks (WSNs) are being widely applied in many fields of human life such as civil and military applications. WSNs are broadly applied for various applications in tracking and surveillance due to their ease of use and other distinctive characteristics compelled by real-time cooperation among the Sensor Nodes (SNs). When applying the WSN in the real world we have to face many challenges such as security, and storage due to its centralized server/client models. Although WSNs can bring a lot of benefits and conveniences. This paper discusses an in-depth survey of a blockchain-based approach for malicious node detection, an exhaustive examination of the integration of blockchain techniques with WSNs (BWSN), and insights into this novel concept.

Keywords: Wireless sensor networks, Blockchain technology, Malicious node detection, Security issues, Centralized, Distributed.

1 | Introduction

Wireless Sensor Networks (WSNs) are generally composed of dispersed micro-devices (termed sensors), which may be embedded and possess simple or various sensing capabilities [1]. These networks are widely used in various areas such as smart homes, military and industrial applications due to their wide range of coverage areas support, massive precision monitoring, remote monitoring, fast stabilization, high fault tolerance and ease of use and unique characteristics including self-organization [2]. Usually, Sensor Nodes (SNs) are deployed randomly or according to a calculated model, they interact closely with the surrounding environment [3]. These SNs 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 [4]. In addition, taking advantage of some mistakes in the network deployment process and hackers can attack the network. 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 [5]. Each block contains information about its creation time and is linked to the

Corresponding Author: im.mekawy@qu.edu.sa

https://doi.org/10.22105/bdcv.2022.371381.1084

previous block by hash code and transaction data [6]. 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 [7].

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 [8]. This will significantly decrease the costs associated with installing and maintaining large centralized data centres [9]. At the same time, computing and storage needs are distributed to all devices in the network [10]. In addition, when blockchain technology is integrated into WSNs, it will eliminate the centralized architecture of WSNs [11]. They found the weighted trust approach to be more rapid in the latter scenario [12]. While similar malicious node detection approaches offer a practical resolution to the malicious node detection problem in WSN, none provides a mechanism to store the execution process of malicious no detection or to store the original node data for accurate traceability in the future [13]. The emergence of smart contracts and blockchain techniques gives a novel route for detecting malicious devices in WSNs [14].

2 | Literature Review

Wireless Sensor Networks

Modern-day sensors are ubiquitous; our daily lives are consumed with sensor-based applications in cars, cell phones, computers, electrical gadgets, factories, machines, wristwatches, and even in the human body [2]. WSNs are generally summarized as a network of nodes that sense information jointly and, in general, allow interactions with remote computing devices, persons, and the nearby environment [15]. In WSNs, all nodes are equipped with sensors to sense physical phenomena, such as temperature, light, pressure, humidity, and so on to process information and then send them to a sink or base station for more processing and analysis [16]. WSNs can be heterogeneous and may have thousands of tiny SNs. A single node usually contains extremely low processing, storage, and broadcasting capability [17].

Maintaining the integrity of the specifications

The so far listed security requirements of WSN are data confidentiality, data integrity, data freshness, and data authentication and availability [18]. With the introduction of blockchain, authentication and identification of devices will be secured over distributed database technology. Each IoT node can be registered and authenticated in the blockchain and will have a unique ID and address [19]. Thus, it will help in the unique identification of the device. 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 *Fig. 1*. However, the number of devices participating in the network and the demand for large-scale network applications are increasing [20]. 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 [21].

3 | Wireless Sensor Networks and Blockchain Techniques

This section explains the overview of WSN, classifications of wireless sensor nodes, WSN challenges, overview of blockchain techniques, important blockchain features, and blockchain security analysis [22]. Complete all content and organizational editing before formatting. Please note section A-D below for more information on proofreading, spelling, and grammar. An encryption and trust evaluation model is proposed on the basis of blockchain in which the identities of the Aggregator Nodes (ANs) and SNs are stored. The authentication of ANs and SNs is performed in public and private blockchains, respectively. However, inauthentic nodes utilize the network's resources and perform malicious activities. Moreover, the SNs have limited energy, transmission range, and computational capabilities, and are attacked by malicious nodes. Afterward, the malicious nodes transmit wrong information about the route and increase the number of retransmissions due to which SN's energy is rapidly consumed [19]. The lifespan of the WSN is reduced due to the rapid energy dissipation of the SNS. Furthermore, the throughput increases, and packet loss

increase with the presence of malicious nodes in the network. The trust values of SNs are computed to eradicate the malicious nodes from the network. Secure routing in the network is performed considering residual energy and trust values of the SNS. Moreover, the Rivest-Shamir-Adleman (RSA), a cryptosystem that provides an asymmetric key, is used for securing data transmission. The simulation results show the effectiveness of the proposed model in terms of a high packet delivery ratio.

For numerous applications, the location data of the nodes must be known. Since this data is not necessarily obtainable, there is great interest in methods for assessing the locations of individual nodes. The accuracy and computational complexity of such "localization" algorithms are still a major problem. But, there are cases where the nodes are located in one of some pre-determined conditions. In those cases, calculating the relative positions of the nodes relative to each other may be enough to decide their true positions.

I. Blockchain is a protected and distributed ledger that eases storing and tracing resources independent of centralized third party authority.
II. Input: cmndb, third-party, sn, η, δ, QM, cmndb – BDS.
III. Output: detected malicious nodes.

Using the computed η, SN utilizes the function (Vote) to choose the malicious node ID. The function is separated into three segments: first, along with the real scene, set a suitable Threshold of Voting (TV), followed by, SN decide the η range of everything in the coverage region sensors.

if η > TV then

node is malicious

else

node is normal

Lastly, the malicious node ID cast:

I. The word "data" is plural, not singular.
II. The malicious SNs discovery blockchain smart.
III. Contract (cmndb−SC) proposed in this survey includes the following relations.
IV. Cmndb-SC D (NC, sensor,sn,η, δ, QM,Cmndb-BDS).

Here,

I. NC is the Cmndb−SC publisher.
II. Sn is the node of aggregation, which the NC authorizes to vote.
III. η is the node's reputation.
IV. δ is the indicator of malicious node assessment, which has FR, DT, and RT.
V. QM is the positioning technique of WSNs.
VI. Cmndb−BDS is the Cmndb information structure.

Some common mistakes

I. It involves massive energy expenditure as each transaction needs powerful hardware resources.
II. Scalability is a key limitation of BWSN. It is because authentication of transactions by most nodes takes some time for verification.
III. Privacy protection is another major challenge ahead of Blockchain Wireless Sensor Network (BWSN).

4 | Blockchain-Based WSN Solutions for Data Management

Although scalability and latency remain a direct challenge for information storage with blockchains, information management frameworks for WSN using blockchains have the advantages of widely imposed information credibility and non-reliance on semantics to logging WSN information formation actions. With distributed storage methods, like InterPlanetary File Systems (IPFS), executed along with blockchains, the WSN bulk information can be saved off-chain while keeping immutable logs and linked to the information inside the blockchain. Blockchain-based solutions are visualized to be at least partly distributed. The WSN information of the user is maintained safe and private, exclusive of third-party interference for service provision. Olivera proposed a structure for saving medical records using blockchain exclusively for keeping reports and inquiries while employing available WSN information storage methods for hosting WSN information. The author's proposed solution is built in three stages:

I. Off-chain-based cloud information storage on Decentralized Hash Tables (DHT).
II. Blockchain-based method for the WSN information access control saved in the DHT.
III. The WSN edge devices.

Off-chain storage widely related solutions have shown promise for a distributed information management method in the WSN. For instance, a cloud blockchain with a multitiered structure was proposed to store WSN information.

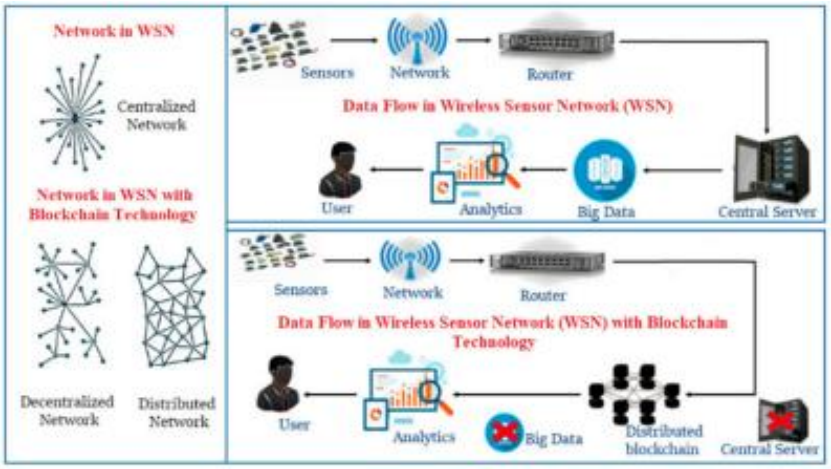

Fig. 1. Centralized, decentralized, and distributed WSN and WSN data flow and BWSN data flow.

Table I. Comparision between types of WSNs.

WSNs with Blockchain	WSN off-Chain-based Chain
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

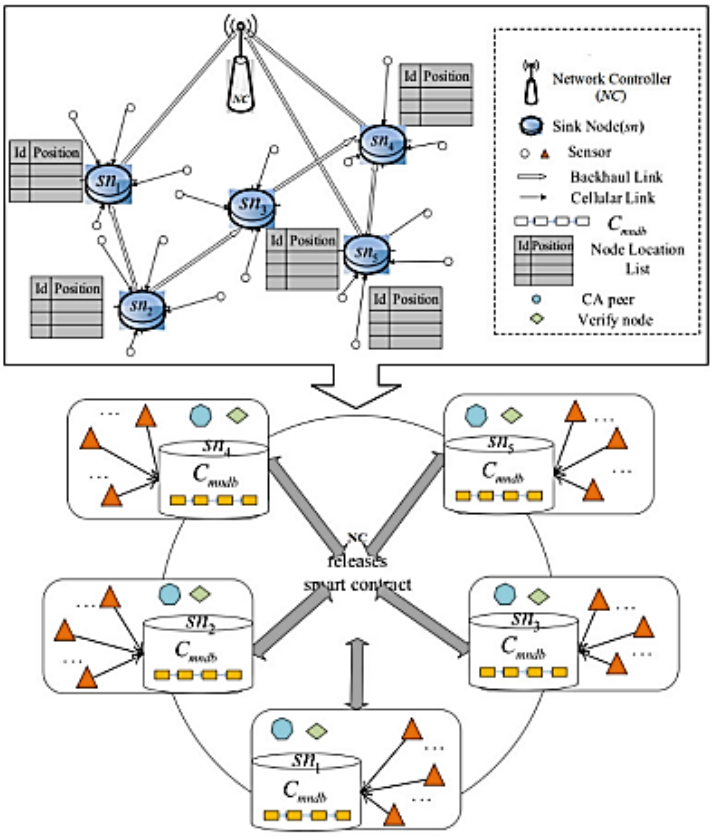

Fig. 2. Blockchain-based wireless sensor network structure for malicious nodes detection.

5 | Conclusion

This paper discussed recent trends in blockchain technology, focusing on recent studies on Blockchain-based Wireless Sensor Networks (BWSNs). 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 WSNs 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.

References

[1] Alharbi, F., Zakariah, M., Alshahrani, R., Albakri, A., Viriyasitavat, W., & Alghamdi, A. A. (2023). Intelligent transportation using wireless sensor networks blockchain and license plate recognition. *Sensors*, *23*(5), 2670. DOI:10.3390/s23052670

[2] Algarni, A. (2022). Smart fire detection using wireless sensors and networks for forest. *Big data and computing visions*, *2*(4), 154–158.

[3] Ramasamy, L. K., Khan K. P., F., Imoize, A. L., Ogbebor, J. O., Kadry, S., & Rho, S. (2021). Blockchain-based wireless sensor networks for malicious node detection: a survey. *IEEE access*, *9*, 128765–128785. DOI:10.1109/ACCESS.2021.3111923

[4] Patil, P., Sangeetha, M., & Bhaskar, V. (2021). Blockchain for IoT access control, security and privacy: a review. *Wireless personal communications*, *117*(3), 1815–1834. DOI:10.1007/s11277-020-07947-2

[5] Gebremariam, G. G., Panda, J., & Indu, S. (2023). Blockchain-Based secure localization against malicious nodes in IoT-based wireless sensor networks using federated learning. *Wireless communications and mobile computing*, *2023*. DOI:10.1155/2023/8068038

[6] Sharma, P., Namasudra, S., Gonzalez Crespo, R., Parra-Fuente, J., & Chandra Trivedi, M. (2023). EHDHE: enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Information sciences*, *629*, 703–718. DOI:10.1016/j.ins.2023.01.148

[7] Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE access*, *7*, 61656–61669. DOI:10.1109/ACCESS.2019.2916503

[8] Salama, R., Altrjman, C., & Al-Turjman, F. (2023). A survey of the architectures and protocols for wireless sensor networks and wireless multimedia sensor networks. *NEU journal for artificial intelligence and internet of things*, *2*(3). https://dergi.neu.edu.tr/index.php/aiit/article/download/725/320

[9] Mao, B., Liu, J., Wu, Y., & Kato, N. (2023). Security and privacy on 6G network edge: a survey. *IEEE communications surveys and tutorials*, *25*(2), 1095–1127. DOI:10.1109/COMST.2023.3244674

[10] Mohapatra, H., & Kumar Rath, A. (2020). Easychair preprint social distancing alarming through proximity sensors for COVID-19 social distancing alarming through proximity sensors for COVID-19. *Easy chair*, *18*. https://wvvw.easychair.org/publications/preprint_download/dMGk

[11] Mohapatra, H., & Rath, A. K. (2020). Nub less sensor based smart water tap for preventing water loss at public stand posts [presentation]. *2020 IEEE microwave theory and techniques in wireless communications* (MTTW) (Vol. 1, pp. 145–150).

[12] Rathore, S., Park, J. H., & Chang, H. (2021). Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. *IEEE access*, *9*, 90075–90083.

[13] Viriyasitavat, W., Xu, L. Da, Bi, Z., & Pungpapong, V. (2019). Blockchain and internet of things for modern business process in digital economy-the state of the art. *IEEE transactions on computational social systems*, *6*(6), 1420–1432. DOI:10.1109/TCSS.2019.2919325

[14] Wu, B., Xu, K., Li, Q., Ren, S., Liu, Z., & Zhang, Z. (2020). Toward blockchain-powered trusted collaborative services for edge-centric networks. *IEEE network*, *34*(2), 30–36. DOI:10.1109/MNET.001.1900153

[15] Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2020). Security and privacy in iot using machine learning and blockchain: threats and countermeasures. *ACM computing surveys (csur)*, *53*(6), 1–37.

[16] Mohapatra, H., & Rath, A. K. (2022). IoE based framework for smart agriculture: networking among all agricultural attributes. *Journal of ambient intelligence and humanized computing*, *13*(1), 407–424. DOI:10.1007/s12652-021-02908-4

[17] Mohapatra, H., & Rath, A. K. (2021). A fault tolerant routing scheme for advanced metering infrastructure: an approach towards smart grid. *Cluster computing*, *24*(3), 2193–2211. DOI:10.1007/s10586-021-03255-x

[18] Mohapatra, H., & Rath, A. K. (2021). An IoT based efficient multi-objective real-time smart parking system. *International journal of sensor networks*, *37*(4), 219–232. DOI:10.1504/IJSNET.2021.119483

[19] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance through energy balanced cluster formation (EBCF) in WSN. *Smart innovations in communication and computational sciences: proceedings of ICSICCS-2018* (pp. 313-321). Springer Singapore.

[20] Kumar, A., Bhushan, B., Shristi, S., Kalita, S., Chaganti, R., & Obaid, A. J. (2023). Blockchain embedded security and privacy preserving in healthcare systems. In *Blockchain technology solutions for the security of IoT-based healthcare systems* (pp. 241-261). Academic Press. https://doi.org/10.1016/B978-0-323-99199-5.00005-7

[21] Goyat, R., Kumar, G., Alazab, M., Conti, M., Rai, M. K., Thomas, R., … & Kim, T.-H. (2020). Blockchain-based data storage with privacy and authentication in internet of things. *IEEE internet of things journal*, *9*(16), 14203–14215.

[22] Alladi, T., Chamola, V., Rodrigues, J. J., & Kozlov, S. A. (2019). Blockchain in smart grids: a review on different use cases. *Sensors*, *19*(22), 4862. https://doi.org/10.3390/s19224862