International Journal of Research in Advent Technology, Vol. 7, No. 5, May 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Applications of Blockchain Technology in Wireless Sensor Networks

Dr. P. S. Gawande
Associate Professor, Rajarshi Shahu College of Engineering, Buldana, India

Abstract— The Internet of Things relies on wireless sensor networks to gather data from particular locations. In a WSN, a large number of low-cost sensor nodes with limited energy, weak computing, and storage capacity form a self-organizing network. By addressing the shortcomings of sensor nodes, blockchain technology improves the functionality of WSNs. In this paper, we look back at the current state of the art and the research that has gone into using blockchain technology in WSNs. Enhancing WSNs' security, dependability, data storage, node recovery, and energy efficiency has been the primary emphasis of most prior research. So far, no other paper has focused on this topic and reviewed all the relevant literature. Researchers interested in using blockchain technology in WSNs might use this review as a starting point.

Index Terms— WSN; blockchain technology; security; data security; energy efficiency

I. INTRODUCTION

Wireless sensor networks (WSNs) have the same security challenges as any other network. The success or failure of an application is dependent on WSN security. Sensor nodes often engage in close environmental interaction after being deployed at random or in accordance with a computed model [1, 2, 3]. These sensor nodes do not require human intervention or a central monitoring system to function. That leaves them working in a very susceptible and potentially tampered-with environment, making them susceptible to hackers. Physical approaches are available to hackers who want to compromise sensor networks. In addition. Also, as mentioned in the study, hackers can exploit vulnerabilities in the network deployment process to launch attacks [4-7]. On top of that, WSN has its limitations when it comes to resources like storage power and computational power for sophisticated algorithms; as a result, synchronization becomes a challenge depending on the application, which in turn depends on the security needs. In order to construct a WSN with certain security features, the requirements were laid out in [8-10]. Similar to an organization's accounting ledger, blockchain technology enables the secure transmission of data through an exceedingly complicated encryption scheme, which records all transactions on the decentralised network. Hash codes and transaction data connect each block to the one before it, and each block also includes information about when it was created. There is no going back after the data has been recorded by the network. Data fraud and tampering are two of blockchain's main design goals [11]. There will be several advantages to incorporating blockchain technology into WSNs. Because blockchain is decentralized, it can manage a high volume of connections between sensor devices. The expenses linked with setting up and running massive central data centers will go down as a result of this. Meanwhile, all nodes in the network share the load of processing and storing data. Also, WSNs' centralized design will be rendered obsolete with the integration of blockchain technology [12]. When devices in a network can automatically coordinate with one another, share files, and communicate with one another, the centralized server and client model will become obsolete [13, 14].

In this paper, we look back at the current state of the art and the research that has gone into using blockchain technology in WSNs. Researchers interested in using blockchain technology in WSNs might use this review as a starting point.

This paper aims to answer the following two questions:

1- What are the advantages of using blockchain in WSNs?
2- What are the limitations of using blockchain in WSNs?

II. BLOCKCHAIN-BASED WIRELESS SENSOR NETWORK

Improvements in data security, data management and storage, node recovery, and WSN energy efficiency have been the primary goals of blockchain research into its application to WSN.

A. Blockchain for Data Security and Reliability

Cloud servers or a BS are usually used to maintain WSNs, verify them, and connect them. This is where data processing and storage are usually done. There are a lot of major problems with this style of device interaction that compromise data accuracy and network security:

1) It's possible for any one node to become a bottleneck or a single point of failure in the network. Domain name system (DDoS) assaults, hacking, data theft, and remote management capture are especially dangerous for Internet of Things (IoT) devices. The BS is vulnerable to hacking, and it

doi: 10.32622/ijrat.752019127

is against the law to access or utilize its data. Everything linked to it could be at risk. For instance, in "smart" water meters, which gather data and send leak alerts to customers' smartphones, hackers can learn when homeowners aren't there since they have access to water consumption data.
2) It is easy to manipulate the centralized model. There is no assurance that the data collected in real-time will be utilized for its intended purpose. It is possible for municipal authorities or utility suppliers to alter the data and analytical information gathered by wireless sensor nodes equipped with air and water pollution sensors if they fear legal action or excessive expenditures. In the Russian Federation, such sensors could avoid the notorious Volokolamsk landfill scandal, in which city officials misled residents for months into believing that the air was safe and that the concentrations of the pollutants did not exceed legal limits [15].
After reviewing the existing WSN system's security flaws, Feng et al. (2018) suggested a platform for processing sensed data that uses a collocation storage architecture based on blockchain technology. An asymmetric signature scheme and a hierarchical Byzantine Fault Tolerant (BFT) consensus mechanism are the building blocks of the suggested WSN blockchain. Experiments and simulations confirmed that the suggested architecture and scheme achieves great output performance while maintaining good security. They made sure that blockchain can function as a service solution for WSN's distributed storage system using the suggested scheme [16].
Buldin et al. (2018) propose WSNs based on blockchain technology as the next generation of industrial networks. Data transmission and storage in such networks is based on the blockchain's decentralized paradigm. Built on top of the EDNCP routing protocol, the model is validated in real time with Onion Omega2+. Among the ways in which the experimental results demonstrate that the suggested approach can improve network security are:

1) All received transactions are protected from spoofing and phantom device injection by utilizing a unique digital signature.

2) Prevent tampering with the original code and data storage on nodes by controlling information distortion caused by hacking devices.

3) Ensure data privacy by encrypting traffic coding. All information is securely stored and is accessible solely to those users who are directly involved in a specific transaction.

4) Prevent data destruction by using a decentralized data storage system. Decentralized public key infrastructure is used by the model to authenticate users. Also, this model can serve as warranty proof if the network nodes input data about the electronic device manufacturer.

Utilizing the blockchain concept and smart contracts to guarantee data stability, the created model offers control over data integrity and safe data transport. Because the firmware hash is compared to its value in the previous blocks when a new block is added to the blockchain, this architecture has the limitation of not being able to upgrade the software.
A system architecture for dam site surveillance was proposed by Youssef et al. (2019). It comprises a sensor cloud and a cloud of unmanned aerial vehicles (UAVs). Dam monitoring center (DMC) data is collected and sent by the UAV cloud, while the sensor cloud is in charge of sensing. Blockchain technology, which the proposed system relies on, allows for the storage, verification, integrity, and traceability of data as well as the payment of entities involved in sensing and delivery. A simulation is run and the data delivery delay ratio is determined to assess the proposed system. There is a negative correlation between the amount of time that passes between alert generations and the delay ratio; as this correlation grows, less data is generated and the delivery delay falls [17].
Internet of Things (IoT) monitoring can provide useful data for assessing mussel quality when in cold storage, as demonstrated by Moinet et al. (2017). However, this data storage is vulnerable because it depends on a centralized architecture [18]. In order to enhance trust and transparency in cold storage, they suggested a blockchain-based multi-sensors (WSN) monitoring system. This technique would collect and validate data on quality metrics.
In order to forecast and categorize the quality loss of frozen shellfish, quality evaluation apps utilized SVM algorithms and K-means. The results demonstrate that WSN monitoring based on blockchain technology can continually monitor dynamic indicators while ensuring the confidentiality and reliability of data. There is an accuracy of 88.89% in the training set and an accuracy of 87.17% in the test set. The SVM model achieved an RMSE of 0.1502 on the training set and 0.1793 on the test set. Both the K-means and SVM models outperform the neural network model in terms of accuracy. By using the suggested system, food loss can be reduced and the quality and safety of cold-stored frozen shellfish can be better managed.
It has been demonstrated by Casado-Vara (2018) that WSN sensors have the potential to provide inaccurate data. If the inaccuracy of the sensors is unknown, this leads to poor data quality and a high maintenance cost for the WSN. In order to anticipate when the accuracy of the sensors would begin to decline, the author suggests using a stochastic model built on the Blockchain. In order to carry out necessary maintenance and preserve data quality, the results anticipated that the very accurate prediction would reveal sensors that will be inaccurate in the near future [19].

B. Blockchain for Data Management and Storage

Managing data storage is crucial for a WSN since the network is data-centric. Data, not the network or sensor node, is what matters to WSN consumers. Despite WSNs' ability to facilitate efficient and dependable data access and storage even in environments that are inherently unpredictable or heterogeneous, the energy and storage capacity available to individual nodes remain finite. The subject of how to make the most efficient use of limited storage space for data has been the subject of multiple studies. Collaboration amongst network nodes is an integral part of any WSN's typical operation. Unfortunately, some nodes in the network may act

doi: 10.32622/ijrat.752019127

selfishly since they don't have enough resources. The entire network will malfunction if a large number of nodes in the network act selfishly and fail to relay packets. One of the key goals of research in WSNs is to find ways to motivate selfish nodes to work together for the benefit of the network [20].

The initial blockchain-based node incentive mechanisms for data storage in WSN were developed by Ren et al. (2018). According to the suggested setup, every node's data storage is like a blockchain block. The node that stores the data will receive the digital money reward; as the data saved grows, so does the reward for the node's implementation. Two blockchains are also constructed. Two databases exist: one to hold information about each node and another to manage who can access the data. Furthermore, they take the role of the proof of work (PoW) in the main bitcoin network, which is responsible for mining and storing the new data block. In contrast to the PoW approach, it drastically reduces the amount of processing power needed. The new data is saved in the node that is closest to the existing data to use the preserving hash functions. Additionally, only distinct sub-blocks are stored. The suggested solution can significantly reduce node storage requirements as a result [20].

Novel approaches are required to address the data storage and management challenge in distributed heterogeneous WSNs. A nonlinear cooperative control algorithm was suggested by Casado-Vara (2019) that combines elements of blockchain technology with game theory. The author introduced a novel approach to the autonomous administration and processing of dispersed WSNs that exhibit heterogeneity. Indoor surface temperature data quality is improved using the proposed technique. In order to ensure the dependability and robustness of the data acquired, the researcher utilized an algorithm. The WSN gathers the information and records it on a blockchain. The information held in a blockchain is subsequently subjected to game theory (GT). The game's distributed and self-organizing nature means it can function on any WSN, regardless of the network's design, sensor count, or sensor type [21].

C. Blockchain for Node Recovery

In a WSN, the storage, energy, and processing power of the network nodes are constrained. Environmental factors, depleting battery power, adversary attacks, and other similar events are likely to cause nodes to fail. In the event of a node failure, a robust recovery mechanism is required. A Blockchain-based Node Recovery (BNR) mechanism for WSNs was proposed by Noshad et al. (2019). The BNR technique uses the node degree to determine how to recover from failed nodes. Using the active or inactive state of cluster heads, the scheme's algorithm identifies the nodes that have failed. After then, the dormant nodes are restored using the recovery method. Recovering the failed cluster heads is the primary goal of this step, which aims to return the cluster nodes to an active state. The goal of writing a node recovery smart contract is to do this. In order to guarantee the safety of the proposed method, the researchers conduct a security study and a cost analysis for node recovery. We can see how well the suggested model works in the simulations [23].

D. Blockchain for Energy Efficiency

The scientific community is interested in studying smart buildings because they see them as an improvement over conventional building management system. In addition, regulatory bodies enact legislation to promote the use of smart buildings. Because technology increases the value of their assets and makes buildings more energy efficient, construction contractors have started to adopt a technology-driven approach [24]. In order to facilitate the remote control, automation, and management of a building's numerous sensors, objects, and functions, a collection of technologies referred to as a "smart building" has been developed [24].

III. DISCUSSION

For a variety of reasons, researchers have suggested implementing blockchain technology in WSNs; nonetheless, most of these studies have focused on enhancing the trustworthiness and security of WSN data. They take advantage of blockchain's decentralized format, which is more trustworthy and secure than WSNs' centralized form, to transmit and store data. Due to the finite resources of each node—energy and storage space—many researchers employ blockchain to manage and store sensor data. Each node's stored data is viewed as a block in the blockchain. Additionally, numerous researchers have used blockchain to enhance WSN energy efficiency. Blockchain technology has the potential to increase the energy efficiency of smart buildings and WSNs based on monitoring systems, according to researchers.

IV. CONCLUSION

Because it integrates many sensor, computer, and wireless communication technologies it has broad practical uses. Communication, microelectronics, networks, databases, etc., have all made wireless sensor networks a popular area of study. They are a component of the long-term goals for the expansion of the Internet of Things. A network's overall performance is impacted by sensors' energy, storage, and security restrictions. We can improve the WSNs' performance by using blockchain, which is a strong distributed peer-to-peer technology. In order to increase the network's longevity, security, and stability, this article offers new methods for WSNs that are based on the blockchain.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

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.

doi: 10.32622/ijrat.752019127

[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] Ferrag, M. A., Maglaras, L., & Ahmim, A. (2017). Privacy-preserving schemes for ad hoc social networks: A survey. IEEE Communications Surveys & Tutorials, 19(4), 3015-3045.
[16] Feng, L., Zhang, H., Lou, L., & Chen, Y. (2018, May). A Blockchain-Based Collocation Storage Architecture for Data Security Process Platform of WSN. In 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)) (pp. 75-80). IEEE.
[17] Youssef, S. B. H., Rekhis, S., & Boudriga, N. (2019, April). A Blockchain based Secure IoT Solution for the Dam Surveillance. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.
[18] Moinet, A., Darties, B., & Baril, J. L. (2017). Blockchain based trust & authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730.
[19] Casado-Vara, R. (2018, June). Stochastic approach for prediction of WSN accuracy degradation with blockchain technology. In International Symposium on Distributed Computing and Artificial Intelligence (pp. 422-425). Springer, Cham.
[20] Ren, Y., Liu, Y., Ji, S., Sangaiah, A. K., & Wang, J. (2018). Incentive mechanism of data storage based on blockchain for wireless sensor networks. Mobile Information Systems, 2018.
[21] Casado Vara, R. C. (2019). Adaptive model for monitoring and control of dynamic IoT networks.
[22] Noshad, Z., Javaid, A., Zahid, M., Ali, I., & Javaid, N. (2019, November). Node Recovery in Wireless Sensor Networks via Blockchain. In International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 94- 105). Springer, Cham.
[23] Alaayed, I., El Bahja, H., and Vega, P. (2013). A sliding mode based on fuzzy logic control for photovoltaic power system using dc-dc boost converter. In 3rd International Conference on Systems and Control, pages 320–325. IEEE.
[24] Afsar, M. (2015). Energy-Efficient Coalition Formation in Sensor Networks: a GameTheoretic Approach.

doi: 10.32622/ijrat.752019127