Journal of Theoretical and Applied Information Technology
15th December 2020. Vol.98. No 23
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A REVIEW ON USING BLOCKCHAIN IN WIRELESS SENSOR NETWORKS

[1]SHURUG ALSAEDY, [2]SHOUQ ALRADDADI, [3]ALI OWAIS

[1]Master Student, Umm Al-Qura University, College of Computer and Information Systems, Computer Science, Saudi Arabia
[2]Master Student, Umm Al-Qura University, College of Computer and Information Systems, Computer Science, Saudi Arabia
[3]Bachelor Student, Umm Al-Qura University, College of Computer and Information Systems, Computer Science, Saudi Arabia

E-mail: [1]S44180584@st.uqu.edu.sa, [2]S44180476@st.uqu.edu.sa, [3]s435004507@st.uqu.edu.sa

ABSTRACT

Wireless Sensor Networks are important parts of Internet of Things, which are used to collect information from specific areas. A WSN is a self-organizing network built by a large number of cheap, limited energy, weak computing and low storage capacity sensor nodes. The blockchain technology is utilized to solve the limitations of sensor nodes and enhances the performance of WSNs. This paper reviews the most recent proposed approaches of employing blockchain in WSNs and their research outcomes. Most of the previous studies focus on improving the security, reliability, data storage, and node recovery and energy efficiency of WSNs. This is the first paper that highlights this subject and discusses all the related works. This review can be used as a basis for researchers who are interested in employing blockchain technology in WSNs.

Keywords: *Wireless Sensor Networks; Blockchain; Internet of Things; Security; Reliability; Energy Efficiency*

1. INTRODUCTION

The Wireless Sensor Network (WSN) has appealed wide attention of researchers in recent years. It consists of large number of sensor nodes working cooperatively to detect the environmental conditions: humidity, temperature, pollution level, sound level, etc. Then, the collected data is stored at a central place, which is termed as a base station or a sink. Such nodes have a microcontroller, transceiver, wireless devices and a battery as an energy source. The nodes have limited energy, computational power and low storage capacity. Therefore, WSNs have limitations of low computational capability, small memory, limited energy resources and accordingly a less security and reliability [1].

WSNs mainly consist of distributed and centralized architectures [3]. In the distributed architecture, user terminals and other network devices can get data directly from sensor nodes. In the centralized architecture, sensor nodes gather data and send to base stations through network routing for processing and analysis. Most of the traditional IoT security authentication protocols use centralized authentication techniques. The adopted authentication protocols [4-6] depend on a reliable third party, such as, authentication server, certificate authorization center and so on, this makes the network vulnerable to a single-point failure. For WSN, it is necessary to create a decentralized model of data transmission and storage which would allow to make networks as much as possible protected from hacking (isolating the hacked nodes from the whole network) and resistant to changes in software and data. These opportunities can be realized through the technology of blockchain.

Blockchain is currently discussed in the news around the globe. It is proposed in 2008 by Satoshi Nakamoto [2]. It is simply an arrangement of blocks contains data structures to allow users to create digital log of all their transactions protected from unauthorized changes. Transactions carried out between the parties are signed using public key encryption and entered into the registry, consisting of cryptographically linked to each other in a chain of transaction blocks — the blockchain. It is impossible or extremely difficult to modify or delete blocks listed in such a registry [2].

Blockchain is a new decentralized distributed technology, can work efficiently with the distributed topology of the WSN, to enhance the performance of the IoT [7], [8]. In blockchain-based WSNs, the terminal sensors perform a reliable connection avoiding threats such as ack-flooding, spoofed routing information, or malicious attack. Figure 1 shows a comparison between traditional and blockchain-based of WSN process. As seen in Figure 1 (a), the collected data is passed to the server through the sink node and internet. Then, the data is collected and stored in a server which can be attacked and be the point of failure. In Figure 1 (b), a decentralized distributed blockchain storage system is presented instead of the centralized server. Through Internet the sensor data can sent to the blockchain system. Transactions and nodes are secured using the node signatures and public key. A node Id is used as a public key to transmit and validate the transaction or sensed data to the blockchain system [9].

This paper reviews the most recent proposed approaches of employing blockchain in WSNs and their research outcomes. This review can be used as a basis for researchers who are interested in employing blockchain technology in WSNs.

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?

2. BLOCKCHAIN-BASED WIRELESS SENSOR NETWOR

For using blockchain in WSN, the major focus of researchers is on enhancing data security, data management and storage, node recovery, and the energy efficiency of a WSN [9-14],[16-19].

2.1 Blockchain for Data Security and Reliability

WSNs are identified, authenticated and connected through management through cloud servers or a BS, where data processing and storage are typically performed. This model of interaction between devices has a number of significant drawbacks that adversely affect network security and data correctness: 1) Each node in the network can become a bottleneck or a point which may cause the entire network to fail. In particular, IoT devices are vulnerable to DDoS attacks, hacking, data theft, and remote management capture. Hackers can also hack the BS and it is illegal to use its data, and under threat may be all that is connected to it. For example, in "smart" water meters, collecting data and transmitting notification of leaks for the smartphone consumers while having access to data on water consumption, hackers can find out when the owners are not at home. 2) The centralized model is vulnerable to manipulation. When collecting real-time data, there is no guarantee that the information is used for its intended purpose. If local authorities or utility providers believe that they may incur high costs or be sued, they may themselves change the data and analytical information collected by wireless sensor nodes that have sensors for air pollution, water pollution, etc. Such sensors could prevent the well-known situation in the Russian Federation with landfills in the city of Volokolamsk, when the city authorities for several months assured local residents that the air is safe and the substances contained in it do not exceed the maximum permissible concentrations [6].

The security problem of the current WSN system has been analyzed by Feng et al. (2018), they proposed a blockchain-based collocation storage architecture for sensed data process platform. The proposed structure consists of a hierarchical Byzantine Fault Tolerant (BFT) which is a consensus protocol and asymmetric signature system in approved blockchain of WSN. The simulation and experiments showed that the proposed scheme and architecture achieves high output performance with high security. They verified that the proposed scheme allow blockchain to work as a service solution for distributed storage system of WSN [9].

A next generation industrial blockchain-based WSNs is proposed by Buldin et al. (2018). Such networks use the decentralized model of blockchain for data transmission and storage. The model is achieved on top of the routing protocol EDNCP [15] and tested in real time using Onion Omega2+ [31]. The experimental results show that proposed model can enhance the network security by the following [2]:

1) Protection from spoofing and injection of phantom devices using a unique digital signature for each received transaction.

2) Control the information distortion against hacking devices which can attack storing

transactions and previous information on nodes and modify the original code.

3) Encrypt traffic coding to guarantee data privacy. The data is protected and available only to the users participate in a particular transaction.

4) Protect data destroying through a decentralized data storage of data. The model authenticate users using decentralized public key infrastructure. In addition, if the network nodes entered data on the manufacturer of electronic devices, this model can provide proof of warranty.

The developed model provides control of data integrity and secured data transmission based on the blockchain concept and the use of smart contracts to ensure data stability. However, this model has a limitation of the incapability to update the software, since when a new block is added to the blockchain, the firmware hash is compared with its value in the previous blocks.

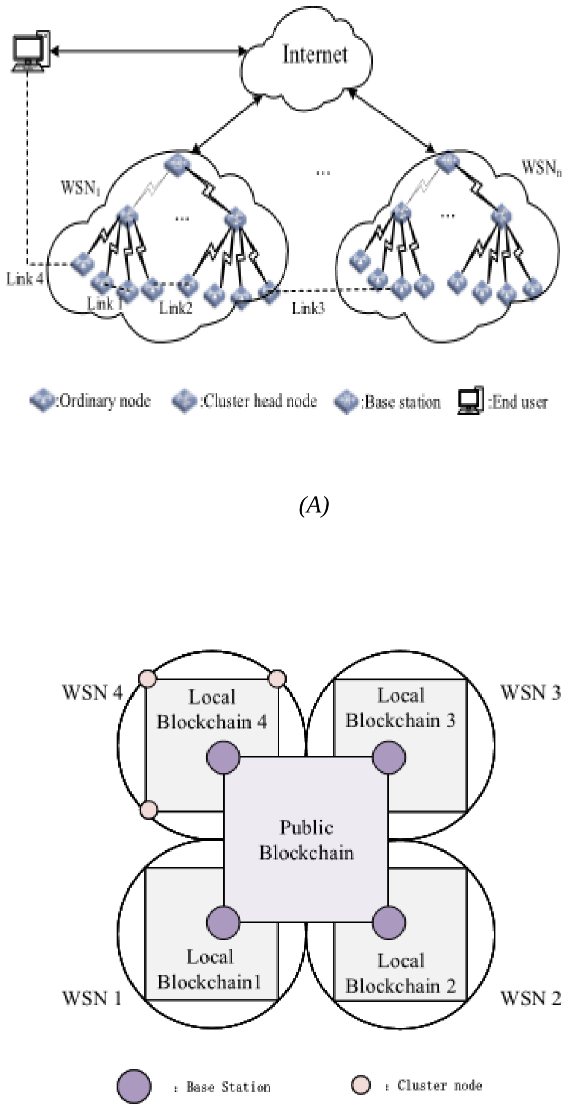
Youssef et al. (2019) proposed a system architecture designed for the dam site surveillance, consists of an unmanned aerial vehicle (UAV) cloud and a sensor cloud. The sensor cloud is responsible for sensing data and the UAV cloud gathers and delivers data to the dam monitoring center (DMC). The proposed system is based on the Blockchain technology which provides data storage, authentication, data integrity, traceability, and payment of the entities employed for the sensing and delivery tasks. To evaluate the proposed system, a simulation is conducted and the data delivery delay ratio is measured. The results show that the delay ratio decreases with the increase of the intergeneration time of alert, and the more the intergeneration time of alerts increases the less data are generated and the delivery delay decreases [13].

Moinet et al. (2017) showed that IoT monitoring can deliver valuable information for evaluating shellfish quality during cold storage. Nevertheless, this data storage relies on the centralized topology, which can be tampered [29].

Therefore, they proposed blockchain based multi-sensors (WSN) monitoring technique to collect and verify gathered information of quality parameters to improve trust and transparency in cold storage. The SVM algorithms and K-means were employed in quality evaluation applications for prediction and classification of the quality loss of frozen shellfish. The results show blockchain based WSN monitoring can ensure the data security and reliability while monitoring dynamic indicators continuously. The percentage of the training set and the test set is 88.89% and 87.17% respectively. The root mean square error (RMSE) are 0.1502 and 0.1793 by SVM model for training and test set respectively. The results of using both K-means and SVM model show higher accuracy than neural network model. The proposed system can help to decrease the risk of food losses and improve safety and quality management of frozen shellfish in cold storage [10].

Casado-Vara (2018) showed that WSN sensors may lose accuracy in their collected information. This causes a problem of low quality data and requires a high maintenance cost of WSN if inaccurate sensors are not known. The author proposed a stochastic model based on Blockchain for early prediction of the sensor accuracy degradation, by knowing its current status. The results expected that the prediction with a high degree of accuracy show sensors that will be inaccurate in the near future to perform required maintenance and conserve data quality [11].

Cui et al. (2020) proposed a blockchain based multi-WSN security system for IoT. The nodes of IoT are divided into cluster head nodes, ordinary nodes, and base stations based on their capability differences, to build a hierarchical network. A blockchain is built from different types of nodes to form a hybrid blockchain model, with local and public chain. In this hybrid model, mutual authentication of nodes is realized in different communication scenarios, the identity authentication of cluster head node is realized in public blockchain, while the identity authentication of ordinary nodes is achieved by local blockchain. The performance of the security system is evaluated and shows that the proposed scheme achieves better performance with comprehensive security. Figure 2 (A) shows the hierarchal model of multi-WSN, and Figure 2 (B) shows the hybrid model of blockchain [14].



(A)

(B)

Figure 2: (A) Hierarchal Model of Multi-WSN (B) Hybrid Blockchain model [14]

Kushch and Prieto-Castrillo (2019) proposed the concept of “Rolling Blockchain” which builds a WSN where its nodes are represented by Smart Cars. The researchers proposed the structure of the chain and the block formation. As well as creating a mathematical model to determine the required number of connections between nodes and the best number of nodes to achieve high network reliability. The results showed that with the increasing number of lost nodes and connection, the Blockchain can still be built and the network remains stable. However, some blocks can be lost depending on the intensity of the attack and the density of nodes. Network reliability relies mainly on the number of nodes each time. Therefore, researchers determine the minimum number of nodes should be in the blockchain to avoid any network disruption. The results show that it is possible to construct a "Rolling Blockchain" with mobile nodes if the beginning and the end of the route are known. However, the proposed approach needs more work in order to be implemented in real life, as handling the security issues and protection against hacking [16].

2.2 Blockchain for Data Management and Storage

Since the WSN is a data-centric network, the data storage is an essential issue, which needs to be managed. The users of a WSN concern about data, rather than the network or the sensor node itself. Although, WSNs support reliable and efficient data access and storage in the unreliable or heterogeneous environment, the energy and the storage space of each node are limited. Several studies have been conducted to answer the question of how to store data effectively in a limited storage space. The normal process of a WSN includes the cooperation of nodes in the network. Nevertheless, due to their limited resources some network nodes may take selfish behavior. If many network nodes choose selfish behavior and do not relay packets, the entire network will not work properly. Thus, inciting selfish nodes to cooperate to ensure the normal process of the network are part of the main researches in WSNs [17].

Ren et al. (2018) built the first incentive mechanisms of nodes for data storage in WSN based on the blockchain technology. In the proposed system, the stored data in each node is considered as a block in the blockchain. The digital money reward will be gained by the node who stored the data, and if the stored data increases the reward for the node implementation increases Moreover, it builds two blockchains. One for controlling the access of the data, and the other to store data for each node. In addition, they replace the proof of work (PoW) in main bitcoins, which performs the storage and mining of the new data block. Different from the PoW mechanism, it extremely cuts down the computing power. Also, to make use of the preserving hash functions, the new data is stored in the nearest node to the currently existing data, and only different sub-blocks are stored. As a result, the proposed system can highly save the storage space of nodes [17].

The problem of data management and storage in the heterogeneous distributed WSNs needs new solutions. Casado-Vara (2019) proposed a nonlinear cooperative control algorithm using blockchain and game theory. The author presented a new model for the automatic management and processing of heterogeneous distributed WSNs. The proposed algorithm is applied for enhancing the data quality of a temperature in indoor surfaces. The researcher applied an algorithm which guarantee the collected data reliability and robustness. The data is collected by the WSN and stored in a blockchain. Then, the game theory (GT) is applied to the data stored in a blockchain. The game is self-organized and distributed, therefore it can work on a WSN regardless of the architecture of the network, the number of sensors, or the type of sensors [12].

2.3 Blockchain for Node Recovery

The network nodes in a WSN have limited resources in terms of storage, energy and computational power. Node failure is expected due to environmental features, battery power draining, adversary attacks, etc. When node failure occurs, a strong mechanism is needed for recovery. Noshad et al. (2019) proposed a Blockchain-based Node Recovery (BNR) scheme for WSNs. In BNR scheme, failed nodes recovery is based on node degree. The procedure of the scheme includes detecting the failed nodes using the state of clusterheads (active or inactive). Then, the recovery technique is performed for the inactive nodes. The main objective of this stage is to restore the active states of the cluster nodes, by recovering the failed clusterheads. For this purpose, node recovery smart contract is written. The researchers perform a cost analysis for node recovery as well as a security analysis to ensure proposed scheme security. The simulation results presents the effectiveness of the proposed model [18].

Figure 3 shows the proposed BNR model, blockchain is implemented at clusterheads since it is a distributed peer-to peer technology. Each clusterhead is linked with other clusterheads via a peer-to-peer connection and also connect with the sink node. Each clusterhead keeps a neighbor list encloses the node state, ID, reputation and degree. If there is a change in the clusterhead state from working to non-working, i.e., state=0, other nodes receives an alert. The recovery process starts once a clusterhead failure is detected. Recovery is performed based on the reputation and the degree of cluster nodes. Node with the highest reputation and least degree is selected as the best candidate. Best candidate replaces the failed clusterhead. Figure 4 shows a flowchart of the node recovery process.

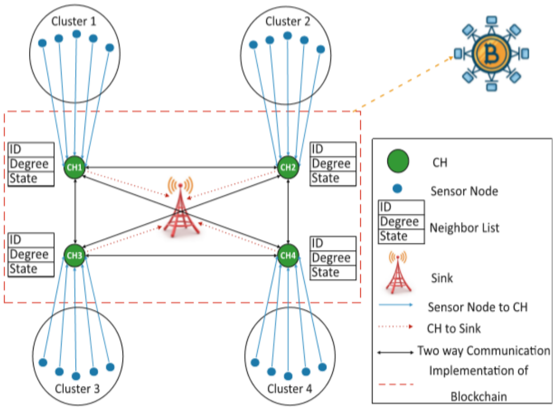


Figure 3: Proposed System for BNR [18]

2.4 Blockchain for Energy Efficiency

The interest in Smart Building research by the scientific community is because they consider it as a better replacement to the traditional building management system [23]. Moreover, laws are implemented by regulatory authorities to encourage the smart buildings adoption. Technology-driven building are begun to be assumed by Building contractors [19], as technology makes the buildings more energy efficient and rises the value of their properties [1]. The concept of smart building defines a set of technologies that are developed to enable various sensors, objects, and functions in a building to communicate with each other and be controlled, automated and managed remotely [20] .

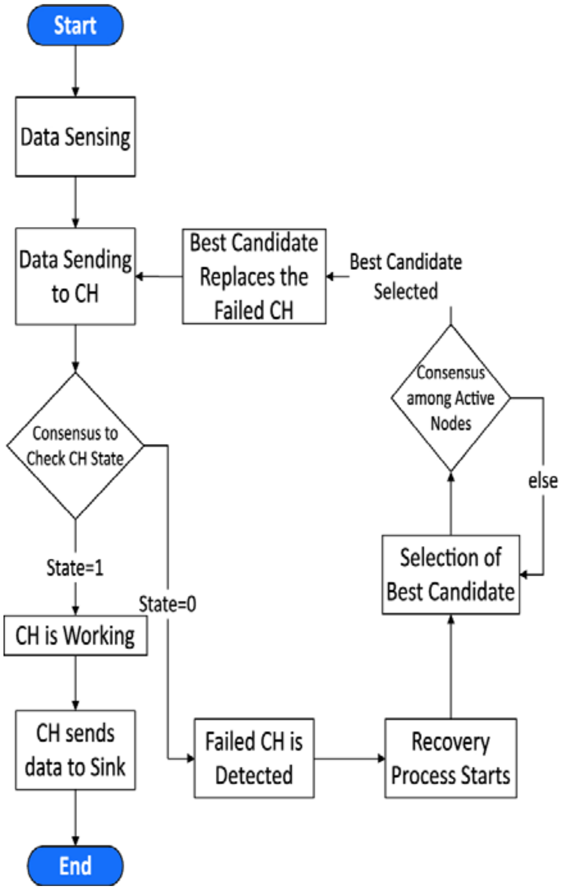


Figure 4: Node Recovery Process

These technologies connect different building subsystems like heating, air conditioning, ventilation, lightening, security and other systems in the house which are based on wireless sensor networks, and the main focus of this technology is to achieve energy efficiency [21]. Casado Vara (2019) shows in his research that it is probable to further improve the energy efficiency of a smart building and WSNs based on current control and monitoring systems using blockchain technology [12].

Islam (2018) proposed a Blockchain based protocol appropriate for WSNs to attain service immutability [25], availability, and network transparency [26], by using a cooperative multiple BS network to reduce the probability of network failure caused by any attack on the BS and reduce energy consumption since most of the energy lost in transmitting data to BS [27], [28]. Also, a new clustering algorithm is proposed, which aims to balance the energy consumption in the network through dividing the targeted area in a perceptive way.

To select the best clusterheads, a two-layered routinization procedure is proposed to guarantee minimum energy consumption from the network and minimize the blind spot problem which arises when the nodes start dying. The proposed protocol is evaluated by simulation in terms of communication, computational overhead and memory.

The results show that the adoption of Blockchain do not affect negatively the network lifetime or the network performance. The clustering algorithm proposed is evaluated in terms of energy consumption of clusters and nodes, number of alive nodes per round, , and dissemination of alive nodes in the network. A significant enhancement in energy consumption among clusters and a lessening of the blind spot problem is shown in the results [24].

The deployment of underwater wireless sensor networks (UWSNs) is so advantageous; nevertheless, some issues limit the performance of the network. For example, high end to end delay, maximum energy dissipation and less reliability. Controlling these issues is a challenging task for researchers. In UWSNs, the inevitability of battery consumption has a direct impact on the network performance [30]. Regularly, energy wastes due to the imbalanced network deployment and the creation of void holes.

Mateen et al. (2019) proposed a blockchain-based WSN and two routing protocols to evade the void hole and extra energy consumption problems and so the network lifetime will increase. To evaluate the proposed protocols, they are compared with the recent protocols. Simulation results show that the proposed systems has better results than their similar systems [22].

2.5 Discussion

Researchers have proposed employing blockchain technology in WSNs for different purposes; the majority of researchers focus on improving the data security and reliability in WSNs using blockchain technology. They exploit the decentralized model of blockchain for data transmission and storage, which is more secure and reliable structure than the centralized form of WSNs.

Many researchers use blockchain for managing and storing the data collected by sensors, since the energy and the storage space of each node are limited, they consider the stored data in each node as a block in the blockchain. Also, to improve the energy efficiency of a WSN, several researchers use blockchain. Researchers show that it is probable to improve the energy efficiency of a smart building and WSNs based on monitoring systems using blockchain technology.

Some researchers use blockchain technology for node recovery. Node failure in WSNs is expected due to environmental features, battery power draining, adversary attacks, etc. When node failure occurs, a strong mechanism is needed for recovery. Blockchain as a robust distributed peer-to peer technology can be effective in the recovering process. Table 1 summarizes the recent approaches of blockchain-based WSNs.

2.6 Conclusion

Because of its wide applications and the combination of multiple technologies of sensing, computing, and wireless communication. Wireless sensor network has become a very hot research topic in the field of communication, microelectronics, network, database, etc. They are part of the perspective directions of development of the Internet of Things. However, the limitations of the security, energy and storage capabilities of sensors affect the whole performance of the network. Blockchain as a robust distributed peer-to peer technology can be employed to enhance the WSNs' performance. This paper presents recent proposed blockchain-based WSNs approaches which aim to improve security, reliability, and lifetime of the network. The proposed approaches showed that they can achieve better performance when employing blockchain.

Nevertheless, these approaches need more work to be implemented in real world, as handling the security issues and protection against hacking.

REFERENCES:

[1] Abreu, D. P., Velasquez, K., Curado, M., and Monteiro, E. (2017). A resilient internet of things architecture for smart cities. Annals of Telecommunications, 72(1-2):19–30.

[2] Buldin, I. D., Gorodnichev, M. G., Makhrov, S. S., & Denisova, E. N. (2018, November). Next Generation Industrial Blockchain-Based Wireless Sensor Networks. In *2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)* (pp. 1-5). IEEE.

[3]Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

[4] Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., & Shen, J. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Generation Computer Systems*, *82*, 727-737.

[5] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for internet of things: a comprehensive survey. *Security and Communication Networks*, *2017*.

[6] 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.

[7] Biswas, S., Sharif, K., Li, F., Nour, B., & Wang, Y. (2018). A scalable blockchain framework for secure transactions in IoT. *IEEE Internet of Things Journal*, *6*(3), 4650-4659.

[8] Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, *15*(6), 3680-3689.

[9] 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.

[10] Moinet, A., Darties, B., & Baril, J. L. (2017). Blockchain based trust & authentication for decentralized sensor networks. *arXiv preprint arXiv:1706.01730*.

[11] 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.

[12] Casado Vara, R. C. (2019). Adaptive model for monitoring and control of dynamic IoT networks.

[13] 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.

[14] Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid BlockChain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), 241-251.

[15] Erokhin, S. D., & Makhrov, S. D. (2013, October). Neural Mechanisms in Wireless Sensor Networks. In *Proceedings of the 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 340-343).

[16] Kushch, S., & Prieto-Castrillo, F. (2019, April). Blockchain for dynamic nodes in a smart city. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 29-34). IEEE.

[17] 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.

[18] 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.

[19] 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.

[20] Afsar, M. (2015). Energy-Efficient Coalition Formation in Sensor Networks: a Game-Theoretic Approach.

[21] Agrawal, R., Gehrke, J., Gunopulos, D., and Raghavan, P. (1998). Automatic subspace clustering of high dimensional data for data mining applications, volume 27. ACM.

[22] Mateen, A., Javaid, N., & Iqbal, S. (2019). Towards energy efficient routing in blockchain based underwater WSNs via recovering the void holes (Doctoral dissertation, MS thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan).

[23] Rajesh, B., Kishore, P. V. P., Yadav, E. S., & Srinivasan, C. R. (2018). A study on onion omega 2 plus IOT device in weather application. *Journal of Advanced Research in Dynamical and Control Systems*, *10*(3 Special Issue), 196-200.

[24] Islam, N. (2018). Towards a Secure and Energy Efficient Wireless Sensor Network using Blockchain and a Novel Clustering Approach.

[25] Helland, P. (2015). Immutability changes everything. *Communications of the ACM*, *59*(1), 64-70.

[26] Pappas, C., Argyraki, K., Bechtold, S., & Perrig, A. (2015, November). Transparency instead of neutrality. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks (pp. 1-7).

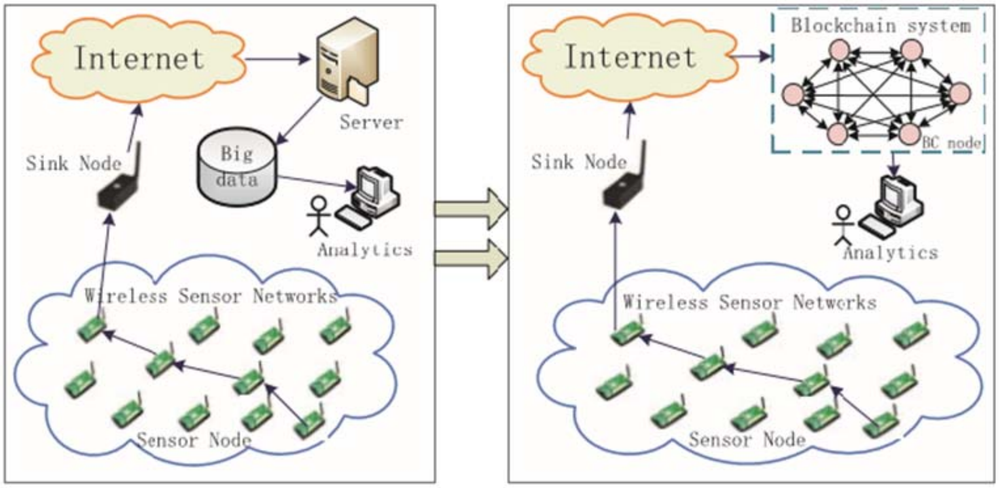
[27] Dandekar, D. R., & Deshmukh, P. R. (2013, February). Energy balancing multiple sink optimal deployment in multi-hop wireless sensor networks. In 2013 3rd IEEE International Advance Computing Conference (IACC) (pp. 408-412). IEEE.

[28] Jain, T. K., Saini, D. S., & Bhooshan, S. V. (2014, April). Increasing lifetime of a wireless sensor network using multiple sinks. In 2014 11th International Conference on Information Technology: New Generations (pp. 616-619). IEEE.

[29] Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, 102022.

[30] Pandey, D., & Kushwaha, V. (2020). An exploratory study of congestion control techniques in Wireless Sensor Networks. Computer Communications.

[31] Rajesh, M. (2018). A signature based information security system for vitality proficient information accumulation in wireless sensor systems. International Journal of Pure and Applied Mathematics, 118(9), 367-387.



(a) Traditional Process of WSN *(b) Blockchain-based WSN*

Figure 1: Comparison between traditional and blockchain-based WSN [9]

Table 1: Recent Blockchain–based WSNs Approaches

Author	Approach	Objectives
Moinet et al. (2017)	Proposed blockchain based multi-sensors monitoring technique to verify the quality of shellfish storage system.	Enhance data security and reliability of a WSN
Feng et al. (2018)	Proposed a blockchain-based collocation storage architecture for secured data process platform.	Achieved high security and high output performance for WSNs.
Buldin et al. (2018)	Proposed a next generation industrial blockchain-based WSNs.	Enhance data security and reliability of a WSN
Casado-Vara (2018)	Proposed a stochastic model based on blockchain for early prediction of the sensor accuracy degradation.	Enhance data security and reliability of a WSN
Ren et al. (2018)	Built the first incentive mechanisms of nodes for data storage in WSN based on the blockchain technology**.**	Enhance the Storage space of the nodes
Youssef et al. (2019)	Proposed a system architecture designed for the dam site surveillance based on Blockchain technology.	Enhance the data security and reliability of a WSN, by reducing the delay of delivery
Islam (2018)	Proposed a Blockchain based protocol appropriate, by using a cooperative multiple BS network.	Reduce the probability of network failure and reduce energy consumption
Mateen et al. (2019)	Proposed a blockchain-based underwater WSN and proposed two routing protocols.	To evade extra energy consumption problems, and increase network lifetime.
Casado-Vara (2019)	Proposed a nonlinear cooperative control algorithm using blockchain and game theory.	Achieve automatic management and processing of heterogeneous distributed WSNs.
Noshad et al. (2019)	Proposed a Blockchain-based Node Recovery (BNR) scheme for WSNs, based on node degree.	Recover the failed cluster heads.
Cui et al. (2020)	Proposed a blockchain based multi-WSN security system for IoT.	Enhance the data security and reliability of a WSN