sciendo

Journal of Smart Internet of Things (JSIoT)
VOL 2023, No.02 | 01-12 | 2023
DOI: 10.2478/jsiot-2023-0007

Article

Blockchain Based Wireless Sensor Networks for Detecting Nodes

Abothar Mohmood Alkhfaji [1]

[1] Department of Information Technology and Computer Engineering, University of Qom, Iran

*Corresponding author: Shakir Salman Ahmad (email: abotharalkhfaji@qom.edu.ir)

Received 12 October 2023; Accepted 30 October 2023; Issue Published 15 December 2023

Abstract: The versatility of Wireless Sensor Networks (WSNs) and other unique qualities inspired by real-time collaboration between the sensor nodes make them widely used for a range of applications in monitoring and surveillance. As solutions for malicious node identification involve a single, centralized decision-making process, security in WSNs is becoming more and more important. Errors are difficult to prevent with this paradigm, and repeatability and traceability are problems. Therefore, the detecting ability and integrity of the developed detection method cannot be guaranteed by malicious node identification technology in ordinary WSNs. This article provides insights into this innovative idea as well as a thorough investigation of the use of blockchain technology to WSNs (Blockchain-Based WSN), including a full analysis of a blockchain-based method for identifying rogue nodes. The Blockchain-Based WSN architecture, business-specific applications, and use are all included in this study. The Blockchain-Based WSN architecture model for tracking malicious nodes and the smart contract features of malicious node detection is both included in the explanation of harmful node identification based on Blockchain-Based WSN in this paper. The second part of this study investigates the use of blockchain technology to the management of WSN data, which necessitates online information aggregation and may also require auditing, event logging, and storage for information analysis and offline query processing. The traditional WSN data management approaches are discussed first in this study, followed by the blockchain-based WSN data management choices. The benefaction of blockchain to WSN security management is also included in this survey. Before discussing blockchain-based WSN security management solutions, such as those that provide access control, protect data integrity, ensure anonymity, and prolong the life of WSN nodes, it first looks at the security vulnerabilities of centralized WSN models.

Keywords: Blockchain, Wireless Sensor Network (WSN), Blockchain Based WSN, Security Management Solutions.

Copyright © 2023 Journal of Smart Internet of Things (JSIoT) published by Future Science for Digital Publishing and Sciendo . This is an open access article license CC BY (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

Wireless sensor networks (WSNs) are often made up of scattered small devices, also known as sensors. These sensors can be embedded and have a variety of different detecting capabilities. Due to their extensive coverage areas support, high fault tolerance, ease of use, rapid stabilization, huge precision monitoring, remote monitoring, fast stabilization, and self-organization, these networks are widely used in a variety of fields such as military, smart homes and industrial use cases [1].

However, sensor nodes are intrinsically constrained since they have a certain amount of energy, computing power, trans-mission range, and onboard memory. Additionally, because of these restrictions, sensor nodes are open to attack. Security threats to WSNs frequently come from both inside and outside the network, where legitimate network nodes can be taken advantage of and even made to behave maliciously. The timely identification, containment, and elimination of rogue nodes within networks is a crucial aspect of WSN security. The design and development trends of WSNs have been significantly impacted by the need to address security-related challenges, which has garnered considerable attention in the literature. Additionally, a number of methods for the identification of malicious blocks in wireless sensor blockchain networks have been already presented. For instance, Min and Ranxin [1] presented a method to stop selective forward assaults utilizing Malicious node Detection using a Triangle Module Fusion Operator (MDTMO). This widespread network assault causes nodes to deliberately reject some or all data packets, preventing the cluster head and base station from receiving total monitoring information. According to the information packets that are transmitted to a node, retrieved by the node, and forwarded by the same node, the MDTMO approach provides packet loss send- receive and receive-forward membership functions. Then, to find a possibly malicious device, it applies the triangle module fusion approach to the membership functions. The base station (BS) device receives notification of the possibly vulnerable node, determines its proper channel and buffer occupancy, then attempts to determine if the packet loss is caused by a clogged network. If the WSN quality is improved, data loss and congestion shouldn't occur. In that situation, the device is considered hostile since it is believed that the packet loss resulted is not from jamming but from a selective forward assault.

An approach that separates the discovered harmful nodes logically by an inter-node vote was put out by Kimura et al. [2] and involves the cooperation of honest nodes to identify malicious nodes. This strategy is particularly useful for WSNs installed in remote locations where physical tampering is more likely than remote infiltration. In these situations, attackers frequently try to physically introduce rogue sensor nodes into the network or steal encryption key information. Because there is no assurance that encryption information is always secure, a faulty node finding strategy that is independent of data encryption is important.

The weighted trust approach, a popular method for malicious node identification, was also investigated by Jaint et al. [3] in a WSN that included a BS, nodes sensing, cluster heads, and forward nodes. In the weighted trust technique, each and every sensor node is assigned a weight that is actively reviewed depending on the node behavior and corresponds to the level of trust related. The trust weight theoretically drops each time a node gives erroneous information, and once it drops below a certain point, the node is classified as malevolent. The sensor node's data were collected for the research and delivered to a cluster heads. All cluster heads then forwarded the data to a forward node, which then sent it to the BS. The authors took into account two scenarios: one in which there was just a single cluster head and no other cluster heads, and the other in which there were many cluster heads and no other cluster heads. In the latter case, they discovered that the weighted trust technique moved more quickly. Even if comparable harmful node detection techniques give a workable solution to the damaged node detection issue in Wireless Sensor Network, not one of them offer a means to preserve the implementation method of malicious node detection and fot future precise trackability provide storage of the original node data. A new method for identifying rogue devices in WSNs has been made possible by the development of smart

contracts and blockchain technology.

Additionally, Blockchain allows for faster peer-to-peer transmission through the use of a distributed digital ledger. The digital distributed ledger in this instance is tamper-proof, preventing interpretation errors or false authentications. Furthermore, blockchain enhances the confidentiality as well as integrity of WSN data, ultimately making it much more dependable. It also enables WSNs to perform transactions of informational data among the devices cooperatively. A smart contract may arrange all processed data and details into information blocks that can be regularly be monitored and confirmed, execute predetermined procedures when limit conditions or recognized unusual behavior are triggered. The data transfer is safer and more reliable thanks to the use of blockchain in WSN. Therefore, network harassment by hostile nodes in Blockchain-Based WSNs may be guaranteed to be traceable and transparent, in addition to being regulated. The main focus of this work is the accuracy of malicious node detection and data provenance, two benefits of BLOCKCHAIN-BASED WSNs. More details on distributed blockchain technology and smart modern contracts are provided in the WSN malicious node detection papers by Dhaliwal, Siddique, Sapra, Rashid and Sidhu [4]–[6].

WSNs lack of prerequisites for distributed blockchain applications use case and smart modern contracts and are inherently resource-constrained [7]. In order to do this, Pace and Ellul [8] described a reference of a architecture design and further execution of a split virtual machine for WSNs, in which the computation costly procedures for gaining access to the blockchain network systems are removed to unconstrained nodes. In order to address the resource limitations in Internet of Things (IoT) networks, Pan et al. [9] presented an edge-chain structure based on blockchain where resource-unrestricted edge servers supply resource-restricted devices. Each and every IoT device account and resource use are connected to the edge cloud resource pool, and smart modern contracts are used to priorities access resource based on the nodes' historical actions. These research directions imply that distributed blockchain is becoming more popular as a potential technical advantage for WSNs in the future.

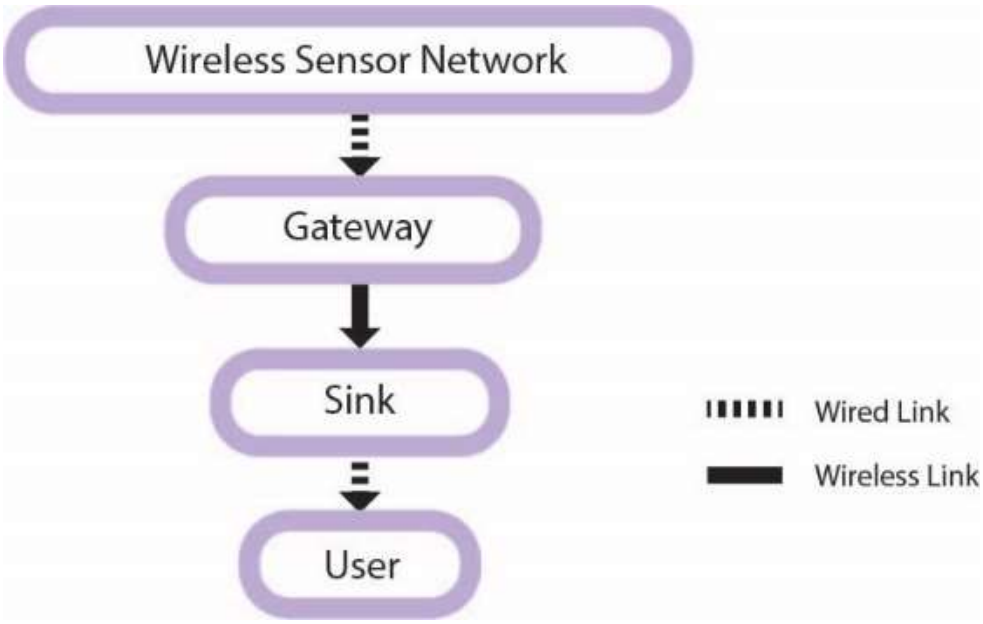


Figure 1: A Typical Wireless Sensor Network Block Diagram Representation.

2. BLOCKCHAIN TECHNIQUES AND WIRELESS SENSOR NETWORKS

This section covers a WSN overview, wireless sensor node classifications, WSN challenges, an overview of blockchain approaches, key features of the blockchain, and a blockchain security analysis.

2.1. WSN (Wireless Sensor Networks):

Current sensors are widely used in a variety of devices, including automobiles, cell phones, computers, electrical appliances, industries, machinery, wrist watches, and even the human body. As depicted in Fig. 1, the WSN architecture, WSNs are typically described as a network of connected blocks that collectively detect informational details and, in general, enable connections with distant computational devices, people, and immediate ecosystem [10].

In WSNs, every node has a sensor to detect physical phenomena like pressure, temperature, light, humidity, and so forth [11], analyse the data, and then forward it to a base or sink station for additional processing, collecting data and analysis. WSNs may have hundreds of small sensor nodes and may be diverse [12]. The processing, storage, and broadcasting capacities of a single node are often quite low [13]. These nodes are used in many commercial and military applications despite having a restricted feature set; their early development was supported by military applications for battlefield monitoring.

The United States Defence Advanced Research Projects Agency (DRPA) launched the Distributed Sensor Network (DSN) programme for the US military in the 1980s, which marked the beginning of research on wireless sensor networks [14]. Although it was thought that the distributed sensor network would have low-cost cooperating nodes and be capable of autonomous control, this was not the case. The application of the sensors proved insufficient for a number of prospective applications since they were rather large (i.e., larger than a shoebox) [15]. However, since then, there has been a dramatic change in WSN research, bringing it closer to its pioneering goal, thanks to the development and advancement in micro-electro-mechanical, processing and communication technologies.

In 1998, the WSN research trend improved and sparked the curiosity of experts from all over the world. At the beginning of this trend, WSN research concentrated on network related data processing and extracting information and network technologies appropriate to ad-hoc environment and mostly dynamic sensor nodes. Development of multiple civil applications such as environment monitoring, vehicle sensor networks and body sensors was facilitated by technological developments that also resulted in smaller and cheaper sensor nodes [16]. With about 24 million actuators and wireless sensors are installed worldwide, the use of WSNs in the industrial automation industry is currently prominently visible.

The nodes' position information is necessary for many applications. There is significant interest in techniques for determining the positions of specific nodes because this data is not always available. The precision and computational complexity of such "localization" methods continue to be significant issues. However, there are instances where the nodes are situated in a certain set of parameters. Calculating the nodes' relative locations to one another in certain circumstances could be sufficient to determine their actual placements. The energy efficient node stabilisation technique in optical WSN was proposed by [17]. Additionally, PSO-based node based on low energy optically located on the WSN was suggested.

The WSN is initially briefly addressed in the next part, then subsection 2.1.2 lists the difficulties with WSNs.

2.2. Challenges of WSN:

The following are briefly discussed difficulties with wireless sensor networks:

2.2.1. Energy:

Smart sensors need some type of power reserves to perform various tasks whenever necessary. A major problem in WSN is energy management [18]. The associated battery that powers nodes often have a finite capacity. Sensing, gathering, analysing, 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 registration of sink nodes or BSs inquiries, sensors must also be operational. Nodes accomplish nothing useful during this period while wasting the energy that has been used.

Hence, the energy that is available to us is used during transmission, idle operation and reception [19].

2.2.2. Routing and Communication:

Finding a transmission path from each and every sensor node to the BS is very difficult aspect of the architecture network. Keeping the nodes alive for a long time is often the goal. Since the nodes often only provide limited range for transmission, intermediary nodes for forwarding are used. The WSN's communication profile and general performance are directly impacted by the deployment method and routing protocols. Nodes in WSNs function wirelessly, which is distinct from typically used routing in different networks in several other ways. Due to the absence of a wired infrastructure and wireless media routing is typically much less dependable than media routing through wiring. When some types of local organization are used into and as cluster cells, WSN nodes normally transfers informational data hop-by-hop to sink, directly to the base station directly or through heads of cluster.

2.2.3. Security:

Another significant WSN concern is security. Data from WSNs are transmitted wirelessly across the air, and as these types of wireless signals are public, anybody may see and take part in this conversation even not having permission being invited [20]. Most WSN developed nodes work in the license-free Independent Side Band (ISB). Security is therefore essential in both military and commercial aspect of many applications to thwart hostile assaults such as DoS attacks and unauthorized gaining access Following are some categories for security demands for WSNs:

Information confidentiality: Information confidentiality is the promise of authorized access to information. Because the radio spectrum constitutes of a very open medium and is widely accessible to everyone, it poses a serious security risk to wirelessly run networks. To get around this, common techniques like signatures, message authentication codes, broadcasting authentication and secret keys can be used to keep data authenticity.

Information reliability Errors are a part of WSNs by virtue of the non-stability of wireless channels communication. Because of diffraction, reflection, signal fading, scattering, and different types of sound and noise, information moving via electromagnetic medium might alter, necessitating retransmissions. In the WSN, a large amount of re-communication be quite costly in terms of energy usage. Message integrity codes can be used to guarantee data integrity.

2.2.4. Availability:

Particularly in critical applications, a sensor node's continuous lifespan is vital. Early battery drain on a sensor node's power supply is caused by using energy for extraneous or unneeded communication and processing. Routing techniques that are energy efficient and necessary protocols are necessary to ensure the availability of nodes.

2.2.5. Operating System (OS):

The sensor node of the operating system will offer crucial management of resources and memory

since sensor node's storage is of finite amount, restricted processing power capability, and tiny size. Compared to standard OS, it ought to be simpler. For wireless sensor networks Nano-Q, Mantis OS, and Tiny OS have been optimized particularly to suit the developments according to the WSN design pattern, improvements are essential.

2.2.6. Hardware & software issue:

For WSNs, the speed and power of implementing program instructions and details are an issue since sensor devices are constrained in size and have confined memory space. The device typically includes a sensor, microprocessor, reserve for power and transmitter. The memory sensor collects information and sends to a microcontroller for proper processing. The software commands are carried out by microcontroller and uses the transceiver to transmit the gathered data and information to the sink device. The WSN communication and computation protocols are managed by the micro-controller. Flash memory is speedy and affordable, hence using flash memory devices is advised. The three operating modes of idle, active, and sleep must be used by sensor nodes in order to safeguard the microcontroller power.

2.2.7. The MAC Layer Problem:

Much of the energy loss in a wireless sensor network happens due to collision in the MAC layer, empty hearing packet overhead, and busy traffic. Free nodes need 50 to 100% of their total power to receive required packets when they are idle. To solve this problem, the Sensor-MAC of periodic hearing including rest protocol is suggested. 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 after a certain amount of time, nodes choose a schedule and send synchronization information to the BS. Dynamic sensor MAC, Timeout MAC, and Traffic-Adaptive MAC are three other MAC protocols. Each follows a separate protocol and has advantages and disadvantages of its own.

2.2.8. Time Synchronization:

Field of nodes including sensors are separately operated. The required information detected may be ambiguous or imprecise if their locally developed clocks are not in sync with any of the other nodes [21].

3. BLOCKCHAIN INTEGRATION WITH WIRELESS SENSOR NETWORK

This section covers the architecture of the blockchain with WSN integration (Blockchain-Based WSN) as well as the applications of Blockchain-Based WSN.

3.1 Blockchain-Based WSN Creation:

There are more and more WSN instances, which increases the likelihood that it will have more communicating nodes. Because there are more devices, there will be more communication among them, resulting in the formation of a wireless network. However, as the information obtained in WSNs is often housed on a central server, several issues would arise if this were to happen. Based on the centralized network topology, if a node wants to use data from another node, the required information that flows will go through to the central server. The expanding WSN is shown as a very large-scale system because of which the centralized server's strategy will always be impractical by the growing demands of WSN and applications. Blockchain technology offers a better response to the problems WSN is facing.

3.2 Blockchain-Based WSN Malicious Node Detection:

The Blockchain-Based WSN architecture for the detection of malicious nodes is presented in this section. Additionally, it describes malicious node detection using smart contracts. Table 1

contains the application and usage of blockchain based sensor network by industry.

TABLE 1. Applications and usage of blockchain-based sensor networks by industry

Application Area	Instances
Healthcare	archiving genomic data, digital reports from patients, electronic medical records, prescription data, etc.
Business	managing data on exports and imports, software development, digital records, etc.
Agriculture	Delivery of agricultural goods, management of soil information, implementation of records related to agriculture information
Economics	Money transfers, deposits, smart contracts, cryptocurrency, etc
Smart City	Information management for water and pollution, enabling transactions based on digital data, etc. .
Logistics and Transport	Tracing of vehicles, identifiers for logistical services, reporting on the transit of products, recording of toll information, etc.
Distribution Logistics	Storage and delivery of documents, sales data, virtual currency, used goods, etc.
Power	Information management for power generation, raw material information, and resource availability, etc.

A Wireless sensor networks with a blockchain foundation are designed to detect malicious nodes. Figure 2 illustrates the change from a conventional WSN to a Blockchain-Based WSN. The network controller, sensor nodes, and sink nodes are all components of the standard WSN, as shown in the first section of the figure. Real-time perception of the necessary indications by the sensors in their immediate surroundings produces meaningful monitoring data. Through the cellular network, sensors transmit the data to the related sink nodes. The required sink nodes compile data supplied with the help of sensor within its range of area, assess sensor's operational status in real time, and then transmit the results by the help of backhaul links of network to the network controller.

Distributed blockchain-Based WSN, that has four primary devices — CA, the contract supplying, standard devices and verification — adopts the WSN's basic structure as shown in the lower half of Fig. 2. The device that issues contracts is in charge of modern smart contracts in the network controller. The sink nodes simultaneously serve as a CA device and a verification device. The CA device may create or revoke a member's identity certificate and provides identify data based on blockchain issued digital certificates of community members.

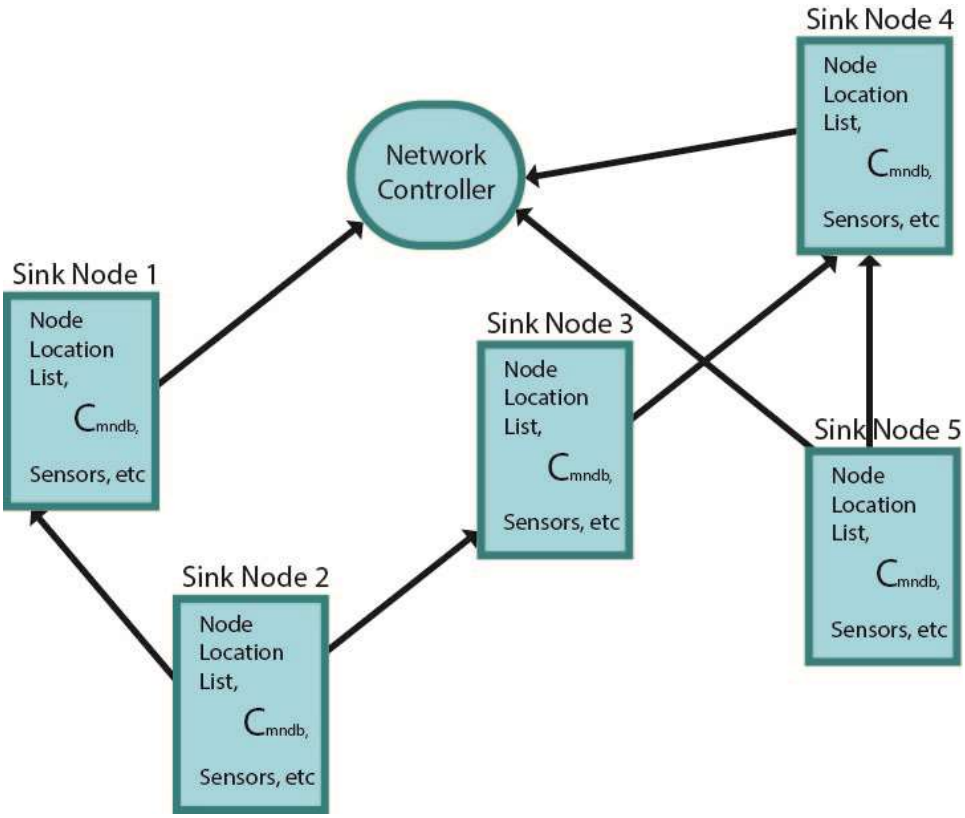


Figure 2: Wireless sensor network architecture based on blockchain for detecting malicious nodes.

3.3 Blockchain In WSN Data Management:

Data management in this WSN comprises storage for information analysis, auditing, offline query processing and event logs in addition to online information aggregation. For high-level WSN applications, information management systems must thus have these capabilities and be able to answer abstract multidimensional questions [22]. Data query is processed and carried out by a middleware layer between the network and application in many WSN topologies. Despite the restricted capabilities of WSN nodes, WSN management of information techniques will be very time conscious due to numerous time-critical WSN application domains.

3.4 Blockchain In WSN Security Management:

This current section looks at the various security problems associated with the centralized WSN structure and how can this research decentralize the WSN by utilizing the security benefits of a distributed blockchain based WSN.

3.4.1 Centralized WSN Models and Security Problems:

The WSN's constantly growing edge is what presents security issues. Devices near the edge of a WSN might potentially fail, making them vulnerable to assaults like Distributed Denial-of-Service (DDoS) [23]. As seen in the August 2016 botnet assault, compromised nodes might work together at the WSN edge to crash the WSN service provider. The Mirai botnet recently developed and increased the already most powerful assault against WSN security in the most recent attack by infiltrating the secure WSN nodes then generating malicious network traffic in the range of Tbsp. [24]. Following the open release of the Mirai botnet source code, a plethora of assaults were launched, with the most noteworthy one being in October 2016 and temporarily taking down many popular websites.

The centralised architecture of WSN poses another risk to the availability of its services [25]. Accessibility, authorisation, and confidentiality risks are a major point of failure [26]. A centralised WSN lacks built-in safeguards against provider misuse or tampering with users' WSN information. WSN privacy has to be guaranteed in a data-driven economy [27]. WSNs must defend themselves against identity spoofing, routing data analysis, traffic and reliability assurance attack like the Byzantine routing attack and modification assaults on data [28].

4. COMPARISONS WITH PREVIOUS PUBLISHED WORKS

This article provides an overview of blockchain technology and its integration with traditional wireless sensor networks (WSNs), sometimes known as blockchain-based WSNs (Blockchain-Based WSNs). A discussion of malicious node detection techniques, implementation of WSNs, and a demonstration of node data, including its verification and detection, are provided in this work. This study also outlines the Blockchain-Based WSNs' shortcomings and talks about specific applications, notably in access control.

The usage of blockchain in WSNs has been covered in a number of published studies. For example, Buldin et al. [29] provided research on the trends of blockchain-based WSNs for industrial applications, which enable the transmission and recording of information accessible with the blockchain model, guaranteeing immutability of the information, and using smart contracts.

A blockchain-based energy-efficient and secure data provenance method was presented by Zeng et al. [30] for data provenance. To make sure that data coming from a node hasn't been tampered with along the way, data provenance is necessary. However, traditional data provenance techniques include several encodings and occasionally compression, which can be taxing on a network that is already restricted. According to the packet route, source information is dispersed across devices in [31], and the evidence may be recalled by running a BS query. In close proximity to the Wireless Sensor Network, a superviso- ry network based on edge devices is set up, with high-performance devices keeping the provenance data of the WSN in a blockchain-based database. The provenances are then safeguarded for authenticity and security.

Blockchain-based information gathering and visualisation in WSNs were the main topics of Wang et al [32].'s study. Blockchain-based information gathering and visualisation in WSNs were the main topics of Wang et al [33].'s study. They used the blockchain method, which treats all mobile databases as blocks, in conjunction with WSN sensing in their study. Each block will first determine the maximum amount of sensor data it can store before combining it with data from other blocks and its own measurement information. Each block device in this system stores the sensor data for the whole WSN. The submitted data from these sensor devices is then displayed and examined.

For a real-time high data sensing situation, Marchang et al. [34] presented a routing protocol based on a private communication blockchain foundation. The Load Balancing Multi-Hop (LBMH) routing protocol, which is suggested, extends battery life by reducing the overhead associated with block updates. Blockchain in WSNs may, however, never become a reality due to the limited local storage and power of the sensor nodes, according to the authors. On the other hand, a routing protocol based on a blockchain framework and a traffic load balancing mechanism was proposed by Lazrag et al. [35] to decrease interference in WSNs and IoT. It is expected that the network nodes detect various events, producing enormous amounts of information that must naturally be stored over several packets. They demonstrated the viability of the plan by introducing a routing protocol that makes use of blockchain technology to offer a distributed memory across the network's nodes.

In terms of malicious node identification, Kumar and Paris [36] introduced a blockchain-based deter- ministic filtering technique that aims to screen out manufactured or fraudulent data supplied by an adversary at the intermediary nodes. The suggested technique reduces the storage and communication costs associated with security keys by eliminating the requirement for key exchange

across sensor devices, but because the nodes are not isolated, hostile assaults can be so powerful that they deplete the network's energy. Furthermore, the resilience of the intermediary forwarding nodes against attacks is a need for the scheme's success.

This study was encouraged by the lack of prior research on blockchain integration in WSNs. This article provides a comprehensive overview of the situation, including the opportunities and difficulties presented by blockchain technology for data management and security in WSNs, specifically for the identification of rogue node data. Overall, a thorough analysis of the existing works is provided along with a discussion of the many benefits and difficulties related to the use of blockchain in WSN.

5. CONCLUSION

This article explored current blockchain technology developments with a particular emphasis on the current research on distributed blockchain on based wireless sensor of networks (Blockchain-Based WSNs). A digital distributed ledger containing verified and unaltered payment details and data is one of the survey's important points about blockchain technology. Through the use of a distributed consensus method, it becomes immutable. Distributed blockchains will be used to store the outcomes of the consensus vote. However, several crucial protocols for malicious node identification in Blockchain-Based WSNs often use a once-only centralized routing process, rendering the original data irreversible, making it difficult to reproduce and verify the execution, and increasing the risk of difficulties. The article also goes over the advantages of various smart modern contracts for distributed blockchain enhancement and increased number in Blockchain-Based WSN nodes for malicious detection of nodes and localization. Report concludes with important takeaways on storage needs, data sharing, malicious node identification, and securing data for blockchain based applications in networks and IoTs. The Internet of Things, vehicle ad hoc networks, mobile ad hoc of networks and cloud computing and other well-known networks will be able to integrate with blockchain in the future.

References

[1] Min, L., & Ranxin, G. (2019, December). Malicious nodes detection algorithm based on triangle module fusion operator in wireless sensor networks. In *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (Vol. 1, pp. 118-121). IEEE.

[2] Kimura, Y., Nii, E., & Takizawa, Y. (2019, December). Cooperative detection for falsification and isolation of malicious nodes through inter-node vote for wireless sensor networks in open environments. In *2019 Global Information Infrastructure and Networking Symposium (GIIS)* (pp. 1-3). IEEE.

[3] Jaint, B., Singh, V., Tanwar, L. K., Indu, S., & Pandey, N. (2018, October). An efficient weighted trust method for malicious node detection in clustered wireless sensor networks. In *2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)* (pp. 1183-1187). IEEE.

[4] Abd El-Moghith, I. A., & Darwish, S. M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. *IEEE Access*, *9*, 103822-103834.

[5] Sivaganesan, D. D. (2021). A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks. *Journal of Trends in Computer Science and Smart Technology*, *3*(1), 59-69.

[6] Shah, K., & Jinwala, D. (2021). Privacy preserving secure expansive aggregation with malicious node identification in linear wireless sensor networks. *Frontiers of Computer Science*, *15*, 1-9.

[7] Manuel, A. J., Deverajan, G. G., Patan, R., & Gandomi, A. H. (2020). Optimization of routing-based clustering approaches in wireless sensor network: Review and open research issues. *Electronics*, *9*(10), 1630.

[8] Ellul, J., & Pace, G. J. (2018, February). Alkylvm: A virtual machine for smart contract blockchain connected internet of things. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-4). IEEE.

[9] Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., & Zhao, Y. (2018). EdgeChain: An edge-IoT

framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*, *6*(3), 4719-4732.

[10] Islam, M. N., & Kundu, S. (2018, April). Preserving IoT privacy in sharing economy via smart contract. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)* (pp. 296-297). IEEE.

[11] Kang, E. S., Pee, S. J., Song, J. G., & Jang, J. W. (2018, April). A blockchain-based energy trading platform for smart homes in a microgrid. In *2018 3rd international conference on computer and communication systems (ICCCS)* (pp. 472-476). IEEE.

[12] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, *6*(2), 1594-1605.

[13] del Rio, J., Toma, D. M., Martinez, E., O'Reilly, T. C., Delory, E., Pearlman, J. S., ... & Jirka, S. (2017). A sensor web architecture for integrating smart oceanographic sensors into the semantic sensor web. *IEEE Journal of Oceanic Engineering*, *43*(4), 830-842.

[14] Lu, W., Gong, Y., Liu, X., Wu, J., & Peng, H. (2017). Collaborative energy and information transfer in green wireless sensor networks for smart cities. *IEEE Transactions on Industrial Informatics*, *14*(4), 1585-1593.

[15] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, *4*(6), 1832-1843.

[16] El Khediri, S., Thaljaoui, A., Dallali, A., & KACHOURI, A. (2018, December). Clustering algorithm in wireless sensor networks based on shortest path. In *2018 30th International conference on microelectronics (ICM)* (pp. 335-338). IEEE.

[17] Dhote, K., & Asutkar, G. M. (2017, March). Optimization of routing techniques in wireless sensor network using queue management. In *2017 Devices for Integrated Circuit (DevIC)* (pp. 500-504). IEEE.

[18] Verma, P., Shaw, S., Mohanty, K., Richa, P., Sah, R., & Mukherjee, A. (2018, February). A survey on hierarchical based routing protocols for wireless sensor network. In *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)* (pp. 338-341). IEEE.

[19] Xu, C., Xiong, Z., Zhao, G., & Yu, S. (2019). An energy-efficient region source routing protocol for lifetime maximization in WSN. *IEEE Access*, *7*, 135277-135289.

[20] Ahmad, N., Hussain, A., Ullah, I., & Zaidi, B. H. (2019, March). IOT based wireless sensor network for precision agriculture. In *2019 7th International electrical engineering congress (Ieecon)* (pp. 1-4). IEEE.

[21] Wu, Y., Chen, J., Qian, L. P., Huang, J., & Shen, X. S. (2016). Energy-aware cooperative traffic offloading via device-to-device cooperations: An analytical approach. *IEEE Transactions on Mobile Computing*, *16*(1), 97-114.

[22] Wang, L., Hu, F., Ling, Z., & Wang, B. (2017). Wireless information and power transfer to maximize information throughput in WBAN. *IEEE Internet of things journal*, *4*(5), 1663-1670.

[23] Yetgin, H., Cheung, K. T. K., El-Hajjar, M., & Hanzo, L. H. (2017). A survey of network lifetime maximization techniques in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, *19*(2), 828-854.

[24] Qiu, T., Zheng, K., Han, M., Chen, C. P., & Xu, M. (2017). A data-emergency-aware scheduling scheme for Internet of Things in smart cities. *IEEE Transactions on Industrial Informatics*, *14*(5), 2042-2051.

[25] Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2019, November). Blockchain leveraged task migration in body area sensor networks. In *2019 25th Asia-Pacific Conference on Communications (APCC)* (pp. 177-184). IEEE.

[26] Imoize, A. L., Oyedare, T., Otuokere, M. E., & Shetty, S. (2018). Software intrusion detection evaluation system: a cost-based evaluation of intrusion detection capability. *Communications and Network*, *10*(4).

[27] Yan, Z., Mukherjee, A., Yang, L., Routray, S., & Palai, G. (2019). Energy-efficient node positioning in optical wireless sensor networks. *Optik*, *178*, 461-466.

[28] Yan, Z., Goswami, P., Mukherjee, A., Yang, L., Routray, S., & Palai, G. (2019). Low-energy PSO-based node positioning in optical wireless sensor networks. *Optik*, *181*, 378-382.

[29] Liu, T., Wang, X., & Zheng, L. (2017). A cooperative SWIPT scheme for wirelessly powered sensor networks. *IEEE Transactions on Communications*, *65*(6), 2740-2752.

[30] Gandino, F., Ferrero, R., & Rebaudengo, M. (2016). A key distribution scheme for mobile wireless sensor networks: $ q $-$ s $-composite. *IEEE Transactions on Information Forensics and Security*, *12*(1), 34-47.

[31] Imam, S. A., Singh, M. K., Sachan, V. K., Choudhary, A., & Zaidi, A. M. (2017, November). An energy-efficient data transmission scheme based on DSC-MIMO for wireless sensor network. In *2017 2nd IEEE International Conference on Integrated Circuits and Microsystems (ICICM)* (pp. 309-312). IEEE.

[32] Ogbebor, J. O., Imoize, A. L., & Atayero, A. A. A. (2020). Energy efficient design techniques in next-generation wireless communication networks: emerging trends and future directions. *Wireless communications and mobile computing*, *2020*, 1-19.

[33] Alamu, O., Gbenga-Ilori, A., Adelabu, M., Imoize, A., & Ladipo, O. (2020). Energy efficiency techniques in ultra-dense wireless heterogeneous networks: An overview and outlook. *Engineering Science and Technology, an International Journal*, *23*(6), 1308-1326.

[34] Choudhari, E., Bodhe, K. D., & Mundada, S. M. (2017, February). Secure data aggregation in WSN using iterative filtering algorithm. In *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 1-5). IEEE.

[35] Liu, X., Jia, M., Zhang, X., & Lu, W. (2018). A novel multichannel Internet of Things based on dynamic spectrum sharing in 5G communication. *IEEE Internet of Things Journal*, *6*(4), 5962-5970.

[36] Kwan, J. C., & Fapojuwo, A. O. (2017). Radio frequency energy harvesting and data rate optimization in wireless information and power transfer sensor networks. *IEEE Sensors Journal*, *17*(15), 4862-4874.