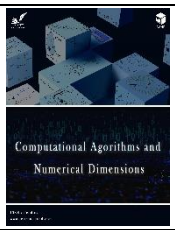
Computational Algorithms and Numerical Dimensions

www.journal-cand.com

Com. Alg. Num. Dim Vol. 2, No. 1 (2023) 7–11.



Paper Type: Original Article

Review of Blockchain Integrated WSN

Samira Torabi*

Griffith Centre for Coastal Management, Griffith University Gold Coast Campus, Queensland 4222, Australia; s_torabi@gmail.com.

Citation:

Torabi, S. (2023). Review of blockchain integrated WSN. *Computational algorithms and numerical dimensions, 2*(1), 7-11.

Received: 24/11/2022 Reviewed: 12/11/2022 Revised: 05/01/2023 Accept: 23/01/2023

Abstract

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

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

1 | Introduction

Remote sensor organizations are for the most part made out of scattered miniature gadgets (named sensors), which might be inserted and have basic or different detecting abilities. These organizations are generally utilized in different regions, for example, shrewd homes, military and modern applications because of their wide scope of inclusion regions support, gigantic accuracy observing, remote checking, quick adjustment, high adaptation to non-critical failure and usability and extraordinary qualities including self-association. Typically, sensor hubs are sent arbitrarily or as indicated by a determined model, they communicate intimately with the general climate. These sensor hubs work unattended or with no remote checking framework. That implies they are working in a climate that is powerless against programmers and has an extraordinary gamble of being messed with. Programmers can go after sensor networks utilizing actual techniques. What's more, exploiting a few slip-ups in the organization sending cycle and programmers can go after the organization. Blockchain is an innovation that permits the transmission of information safely founded on an incredibly mind-boggling encryption framework, like an organization's bookkeeping record, where information is firmly checked and record all exchanges on the distributed organization. Each square contains data about its creation time and is connected to the past square by hash code and exchange information.

Corresponding Author: s_torabi@gmail.com

https://doi.org/10.22105/cand.2023.163352

When the information is recorded by the organization, it is basically impossible to change it. Blockchain is intended to oppose extortion and adjustment of information.

Integrating blockchain technology into WSNs will bring a lot of benefits. A large number of connections between sensor devices will be handled thanks to the distributed nature of blockchain. This will significantly decrease the costs related with introducing and keeping up with enormous concentrated server farms. Simultaneously, figuring and stockpiling needs are disseminated to all gadgets in the organization. Also, when block chain innovation is coordinated into WSNs, it will dispose of the brought together engineering of WSNs. They viewed the weighted trust approach as more quick in the last situation. While comparative malignant hubs location approaches offer a functional goal to the noxious hub recognition issue in WSN, none gives an instrument to store the execution cycle of pernicious hubs discovery or to store the first hub information for exact discernibility later on. The rise of savvy contracts and block chain strategies gives a clever course for identifying malevolent gadgets in WSNs.

2 | Literature Review

2.1 | Wireless Sensor Networks

Cutting edge sensors are omnipresent; our regular routines are consumed with sensor-based applications in vehicles, PDAs, PCs, electrical contraptions, processing plants, machines, wristwatches, and, surprisingly, in the human body. WSNs are for the most part summed up as an organization of hubs that sense data together and, by and large, permit collaborations with remote figuring gadgets, people, and the close by climate. In WSNs, all hubs are furnished with sensors to detect actual peculiarities, like temperature, light, tension, dampness, etc to handle data and afterward send them to a sink or base station for seriously handling and investigations. WSNs can be heterogeneous and may have great many minuscule sensor hubs. A solitary hub generally contains incredibly low handling, stockpiling, and broadcasting ability.

2.2 | Maintaining the Integrity of the Specifications

Security Requirements. The up to this point recorded security prerequisites of WSN are information classification, information honesty, information newness, and information confirmation and accessibility. With the presentation of blockchain, confirmation and distinguishing proof of gadgets will be gotten over dispersed information base innovation. Each IoT hub can be enlisted and verified in the blockchain also, will have an exceptional ID and address. In this way, it will help in extraordinary distinguishing proof of the gadget. In conventional WSNs, information will be gotten to utilizing an incorporated organization by various gadgets through a focal server. The most common way of getting to this information is displayed in *Fig. 1*. Be that as it may, the quantity of gadgets taking part in the organization and the interest for enormous scope network applications are expanding. In this way, utilizing an incorporated server is presently not a successful methodology for enormous scope WSN frameworks. The WSNs framework requires the combination of the most trend setting innovations.

3 | Our Study

This part makes sense of outline of WSN, Classifications of Wireless Sensor Nodes, WSN Challenges, overview of block chain strategies, important block chain features, and block chain security examination. Before you start to organize your paper, first compose and save the substance as a different text document. Complete all happy and hierarchical altering prior to organizing. If it's not too much trouble, note areas A-D underneath for more data on editing, spelling and language structure.

An encryption and trust assessment model is proposed based on block chain in which the characters of the Aggregator Nodes (ANs) and Sensor Nodes (SNs) are put away. The validation of ANs and SNs is

Torabi| Com. Alg. Num. Dim. 2(1) (2023) 7-11

acted openly and private block chains, separately. Notwithstanding, inauthentic hubs use the organization's assets and perform vindictive exercises. Additionally, the SNs have restricted energy, transmission range and computational capacities, and are gone after by pernicious hubs. A while later, the noxious hubs send wrong data of the course and increment the quantity of retransmissions because of which SN's energy is quickly consumed. The life expectancy of the remote sensor network is diminished because of the quick energy scattering of the SNs. Moreover, the throughput increments and bundle misfortune increment with the presence of vindictive hubs in the organization. The trust upsides of SNs are figured to annihilate the malevolent hubs from the organization. Secure directing in the organization is performed considering lingering energy and trust upsides of the SNs. Also, the Rivest-Shamir-Adle (RSA) man, a cryptosystem that gives hilter kilter key, is utilized for getting information transmission. The reproduction results show the adequacy of the proposed model regarding high parcel conveyance proportion.

For various applications, the area information of the hubs should be known. Since this information isn't really realistic, there is incredible interest in strategies for surveying the areas of individual hubs. The exactness and computational intricacy of such "confinement" calculations is as yet a significant issue. Be that as it may, there are situations where the hubs are situated in one of a few pre-decided conditions. In those cases, ascertaining the overall places of the hubs comparative with one another might be sufficient to choose their actual positions.

4 | Blockchain-Based WSN Solutions for Data Management

In spite of the fact that adaptability and dormancy stay an immediate test for data capacity with blockchains, data the executives' structures for WSN utilizing blockchains enjoy the benefits of wide forced data believability and non- dependence on semantics to logging WSN data development activities. With conveyed capacity strategies, as Inter Planetary File Systems (IPFS), executed alongside blockchains, the WSN mass data can be saved off-chain while keeping permanent logs and connected to the data inside the blockchain. Blockchain-based arrangements are imagined to be essentially incompletely dispersed. The WSN data of the client is kept up with protected and private, selective of outsider impedance for administration arrangement. Katzis et al. [24] proposed a design for saving clinical records utilizing blockchain only for keeping reports and requests while utilizing accessible WSN data capacity strategies for facilitating WSN data. The author's proposed solution is built in two stages:

I. Off chain-based cloud information storage on Decentralized Hash Tables (DHT) blockchain-based method for the WSN information access control saved in the DHT, and the WSN edge devices.
II. Off-chain capacity with related arrangements has shown promising for an appropriated data the board technique in the WSN. For example, a cloud blockchain with a multitiered structure was proposed to store WSN data.

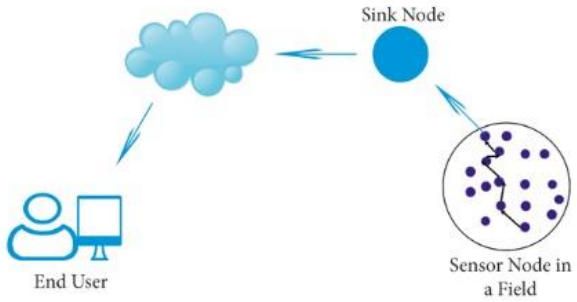


Fig. 1. Centralized, decentralized, and distributed WSN and WSN data flow and BWSN data flow.

Table 1. Comparision between types of WSNs.

WSNs with Blockchain	WSNs without Blockchain
Decentralized	Centralized
Distributed ledger	Client-server architecture
High power consumption	Low power consumption
High security	Low security
Requires a device with a large processing speed and storage capacity	WSN devices have limited processing speed and storage capacity
More difficult to implement and maintain	Simple to implement and maintain

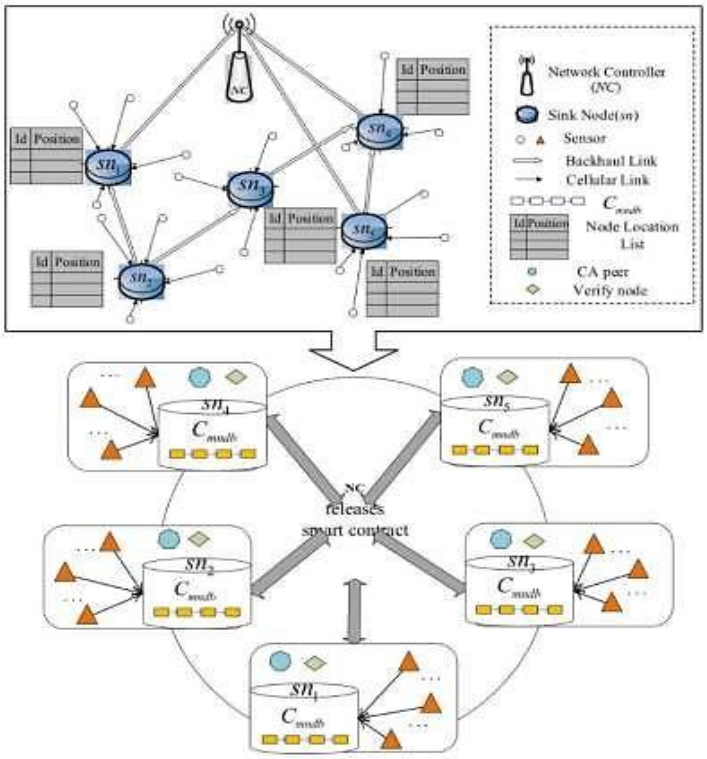


Fig. 2. Blockchain-Based wireless sensor network structure for malicious nodes detection.

4.1 | Conclusion

This paper examined late patterns in blockchain innovation, zeroing in on ongoing investigations on blockchain-based remote sensor organizations. Collecting information from the general climate becomes simpler on account of the solid advancement of sensor innovation. Subsequently, significantly working on individuals' lives because of the advantages that remote sensor networks bring. Be that as it may, the ongoing WSN engineering depends on the server/client model, so there are as yet numerous limits, particularly adaptability, security, and appropriated information capacity. With remarkable benefits in the development of Blockchain innovation, this is viewed as a compelling answer for beat the above constraints. In this article, we have given an outline of the advantages and difficulties of applying Blockchain innovation to WSN. At last, we can show, the interest of Blockchain innovation will settle the constraints of WSN.

References

[1] Mohapatra, H., & Rath, A. K. (2020). Fault-tolerant mechanism for wireless sensor network. *IET wireless sensor systems*, *10*(1), 23-30.

[2] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. *IET wireless sensor systems*, *9*(6), 358-365.

[3] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, *9*(6), 447-457.

[4] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *IET networks*, *9*(4), 145-155.

[5] Mohapatra, H., & Rath, A. K. (2021). Fault tolerance in WSN through uniform load distribution function. *International journal of sensors wireless communications and control*, *11*(4), 385-394.

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

[7] Mohapatra, H., & Rath, A. K. (2022). IoE based framework for smart agriculture. *Journal of ambient intelligence and humanized computing*, *13*(1), 407-424.

[8] Mohapatra, H., & Rath, A. K. (2021). A fault tolerant routing scheme for advanced metering infrastructure: an approach towards smart grid. *Cluster computing*, *24*(3), 2193-2211.

[9] Mohapatra, H., & Rath, A. K. (2021). An IoT based efficient multi-objective real-time smart parking system. *International journal of sensor networks*, *37*(4), 219-232.

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

[11] Panda, H., Mohapatra, H., & Rath, A. K. (2020). WSN-based water channelization: an approach of smart water. In *Smart cities—opportunities and challenges* (pp. 157-166). Springer, Singapore.

[12] Mohapatra, H., & Rath, A. K. (2020). IoT-based smart water. *IoT technologies in smart cities: from sensors to big data, security and trust*, 63-82.

[13] Mohapatra, H. (2021, September). Socio-technical challenges in the implementation of smart city. *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 57-62). IEEE.

[14] Mohapatra, H. (2020). Offline drone instrumentalized ambulance for emergency situations. *IAES international journal of robotics and automation*, *9*(4), 251-255.

[15] Mohapatra, H., & Rath, A. K. (2020). *Fundamentals of software engineering: designed to provide an insight into the software engineering concepts*. BPB Publications.

[16] Mohapatra, H. (2021). *Designing of fault tolerant models for wireless sensor network* (Doctoral Dissertation, Veer Surendra Sai University of Technology). Retrieved from http://hdl.handle.net/10603/333160

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

[18] Mohapatra. H. (2021). *Smart city with wireless sensor network*. KDP.

[19] Mohapatra, H. (2018). *C Programming: practice.cpp*. Independently Publisher.

[20] Mohapatra, H., & Rath, A. K. (2020). *Smart bike wheel lock for public parking*. Application Number.

[21] Mohapatra, H., & Rath, A. K. (2020). Advancing generation Z employability through new forms of learning: quality assurance and recognition of alternative credentials. DOI: 10.13140/RG.2.2.33463.06560

[22] Mohapatra, H. (2009). *HCR using neural network* (PhD Dessertion, Biju Patnaik University of Technology). Retrieved from https://www.academia.edu/29846341/HCR_English_using_Neural_Network

[23] Mohapatra, H. (2019). *Ground level survey on sambalpur in the perspective of smart water* (No. 1918). Retrieved from https://easychair.org/publications/preprint/CWpb

[24] Katzis, K., Berbakov, L., Gardašević, G., & Šveljo, O. (2022). Breaking barriers in emerging biomedical applications. *Entropy*, *24*(2), 226. https://doi.org/10.3390/e24020226