Blockchain Frontier Technology (B-Front)
Vol. 2 No. 2 January 2023

P-ISSN: 2808-0831
E-ISSN: 2808-0009

Ensuring Security Using Blockchain Technology

Padeli[1], Jawahir[2], Muhammad Sholahudin Aprizal[3], Muhamad Yaser Fadilla[4], Mochamad Rivaldi Apriana Adha[5]

Information Technology, University of Raharja, Indonesia[1,2,3]
Multimedia Audio Visual and Broadcasting, University of Raharja, Indonesia[4,5]
e-mail: padeli@raharja.info , jawahir@raharja.info , mohamad.sholahudin@raharja.info, muhamad.yaser@raharja.info, mochamad.rivaldi@raharja.info

Author Notification
01 January 2023
Final Revised
04 January 2023
Published
05 January 2023

Padeli, Jawahir, Sholahudin Aprizal, M., Yaser Fadilla, M., & Apriana Adha, . M. R. (2022). Ensuring Security Using Blockchain Technology. Blockchain Frontier Technology, 2(2), 54–57.
DOI: https://doi.org/10.34306/bfront.v2i2.201

Abstract

The world is heading toward an era of digitization and automation, especially in the development of Blockchain technology. Blockchain in the Internet of Things network is an innovative approach that can make communication between such network devices distributed, autonomous and secure. Blockchain, in this context, is a set of cryptographically linked blocks. Transactions in the network act as the primary carrier of information about the state of the nodes, as well as output information from the nodes themselves for autonomous network functions. A node is a "smart" device, sensor, or microcontroller that connects a group of sensors. Blockchain will be used to provide secure data transmission and device processing on the Internet of Things network. This study discusses the main challenges of applying technology in distributed networks.

Keywords: *Internet of Things, Blockchain, Peer-to-peer Networks, Authentication.*

1. Introduction

With the advancement of communication technology and the ubiquitous introduction of 5G networks, Internet of Things technology is developing exponentially [1]. Smart homes, smart cities, e-Health, the Internet of Things for industrial enterprises, distributed intelligence, and other systems are practical and community-friendly ways to improve many processes, for example, sensor-based crop irrigation and other processes that can become automated . Such a process approach reduces the influence of the human factor and contributes to an increase in the efficiency of the enterprise, for which there are all the prerequisites for the use of IoT technologies [2]. Despite all its effectiveness and prevalence, Internet of Things technology has many challenges and issues related to IoT devices' security and secure configuration. The existence of a large number of such devices is fraught with danger, as attackers can control them and manage DDoS attacks and other traffic manipulation using IoT devices to send these devices to the server [3]. One example of a unified attack on multiple IoT devices is a botnet. A botnet is a collection of compromised devices under the control of an attacker. Mirai is a worm and botnet formed by hacked (infiltrated) devices such as the Internet of Things (video players, intelligent webcams, etc.) [4]. This botnet hacks devices by guessing the password for port 23 (telnet) [5]. In a centralized IoT system, it is sometimes sufficient to hack the server or microcontroller responsible for communication between a large group of devices to control all the devices communicating via a centralized protocol with the compromised server [6].

P-ISSN: 2808-0831
E-ISSN: 2808-0009

2. Research Method

A decentralized approach to the internet of things [7]. Centralized IoT governance systems can be a vulnerability, as such an architecture significantly reduces the time it takes for all devices in such a network to be controlled by an attacker [8]. The solution is to use a decentralized approach method to set up such a network, where each device acts as an independent node [9]. In the case of such communications, the attacker would have to compromise every device, not just the central server. Using centralized communication protocols in a decentralized network is not sufficiently secure and effective [10]. Using Blockchain technology to regulate communication between devices in such a network is the most appropriate solution because the information will be transferred in the form of secure and signed transactions that must be recorded in a ledger distributed across each node [11].

This approach provides the following benefits and properties of device interaction in a distributed network :

a. Decentralization
b. Safety
c. Identification
d. Network Flexibility
e. Autonomy of The Network
f. Reliability of Information

Decentralization involves removing security concerns from a centralized approach to managing the Internet of Things, increasing the margin of error, and increasing the network's effectiveness and security [12]. Transactions between nodes are secure, signed with the secret key of the sending node, and verified by the receiving node, ensuring security and identification. At any time, any number of devices can be connected to the network, receiving a copy of the most recent distributed ledger – thus ensuring network flexibility [13]. The autonomy of work consists of the impossibility of suspending the operation of the entire network, and disabling one of its components, as can happen in a centralized network when a server breaks down [14]. The reliability of the information in the network lies in the fact that the distributed ledger blocks will only contain transactions verified by miners or vice versa, which will contain device output information. Decentralized and peer-to-peer network organization demonstrates a high level of security, reliability, network flexibility, and the possibility of autonomous operation of its parts [15].

3. Result and Discussion

Consider effective consensus and distributed ledger storage. With all this the following challenges remain relevant to the advantages of a decentralized network : how to keep a distributed ledger on a single node and which consensus algorithm to use for efficient network operation.

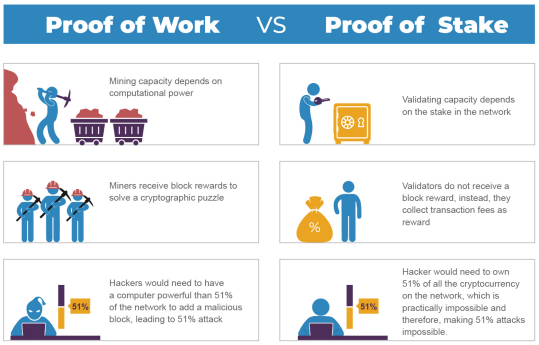

Figure 1. Proof of Work and Proof of Stake

Proof-of-work is a standard Bitcoin network algorithm that allows, based on proof of several complex calculations, to prove the work done to verify transactions and cryptographically close blocks. In large networks, this convention is very expensive in terms of the energy expended on the calculation of drawdowns and block closures. The Internet of Things network must provide communication and decision-making in real-time mode. This requirement makes proof of work ineffective for solving the problem. Because in a closed Internet of Things network, the proof of work device itself must be used - the operation of such a network can interfere with the device when calculating proof of work. A miner is considered a member of the network who is interested in maintaining performance. Such a network for some gifts. It is possible to set up a distributed network on a proof-of-work basis simply by making the Internet of Things open to external miners. In such a case, you should ensure that the miner engagement is high enough so that there is no delay in the creation of new blocks and no additional burden on the nodes in the network.

Another solution might be to opt for a lighter weight consensus algorithm. For example, Proof-of-Stake or section proof. This consensus algorithm is less resource demanding than proof of work (see Figure 1). The preferred and lightweight consensus algorithm for the distributed internet is Proof-of-Authentication. To implement this algorithm, it is necessary to store in the general communication table the matches of the device's public key and MAC address.

Proof of authentication can be implemented as follows :

a. The trusted node is selected.
b. Untrusted nodes aggregate transactions into blocks.
c. Untrusted nodes sign the block and send it to all trusted nodes.
d. The trusted node matches the node's public key and MAC address.
e. If all trusted nodes have successfully authenticated the node that sent the block, then this block is sent to all network nodes.
f. When receiving a block, the other nodes find the hash of the header and open a new block with this hash value in the "Previous hash" field.

If the trusted node cannot authenticate the block and the node that sent the block, the trust rating drops. With a low trust rating, reassignment occurs to trusted hosts on the network. This algorithm allows you to significantly reduce the burden on the device and verify the authenticity of information sent using the EDS mechanism. Using the above algorithm, in addition to the strong consensus algorithm, also helps to increase the security of the stored data. Distributed ledger storage can be implemented in the cloud so that each node can access its part of the cloud. Thus, data will not occupy space on the device itself. It is also possible to store not all of them but only the blocks most relevant to the data on the device. This method will allow you to refuse to interact with the cloud and save the node's memory.

4. Conclusion

The application of Blockchain technology in the organization of a secure distributed network, the Internet of Things, is an up-and-coming and innovative technology. This approach in the organization's distributed network makes it possible to ensure node autonomy, a high level of security of infrastructure and elements of the Internet of Things, as well as identification using EDS. However, the application of this technology has some limitations: standard consensus algorithms are unsuitable due to their attachment to external miners or high power consumption. However, the proof of authentication algorithms is reliable as a consensus algorithm for networks where the network nodes act as miners. This algorithm can provide the required device and communication speed in real-time. Data storage can be implemented with the two proposed in this study by

providing node access to the part of the cloud where a copy of the registry will be stored and storing only the most relevant blocks in the memory of the node itself, thereby providing convenience for the registry.

References

[1] M. Pilkington, "Blockchain technology: principles and applications," in *Research handbook on digital transformations*, Edward Elgar Publishing, 2016.
[2] G. Albeanu, "Blockchain technology and education," in *The 12th International Conference on Virtual Learning ICVL*, 2017, pp. 271–275.
[3] S. Santoso, E. P. Harahap, A. Khoirunisa, and K. Zelina, "A Systematic Review Through Intellectual Based Blockchain-Intermediary," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–7.
[4] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in *2018 International Conference on Information Networking (ICOIN)*, 2018, pp. 473–475.
[5] D. Dujak and D. Sajter, "Blockchain applications in supply chain," in *SMART supply network*, Springer, 2019, pp. 21–46.
[6] F. Allon, "Money after Blockchain: gold, decentralised politics and the new libertarianism," *Aust Fem Stud*, vol. 33, no. 96, pp. 223–243, 2018.
[7] Ž. Turk and R. Klinc, "Potentials of blockchain technology for construction management," *Procedia Eng*, vol. 196, pp. 638–645, 2017.
[8] M. H. Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchain technology," *Managerial Finance*, 2019.
[9] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, 2018, pp. 1–6.
[10] W. Nowiński and M. Kozma, "How can blockchain technology disrupt the existing business models?," *Entrepreneurial Business and Economics Review*, vol. 5, no. 3, pp. 173–188, 2017.
[11] R. Cole, M. Stevenson, and J. Aitken, "Blockchain technology: implications for operations and supply chain management," *Supply Chain Management: An International Journal*, 2019.
[12] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Mathematical foundations of computing*, vol. 1, no. 2, p. 121, 2018.
[13] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," *Trends Food Sci Technol*, vol. 91, pp. 640–652, 2019.
[14] H. Hou, "The application of blockchain technology in E-government in China," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 2017, pp. 1–4.
[15] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl Energy*, vol. 195, pp. 234–246, 2017.