AN OVERVIEW OF SECURED COMMUNICATION THROUGH IOT NETWORK USING BLOCKCHAIN

Mona Gupta*, Dr. Ashwani Sethi**

*Research Scholar, **Professor
Guru Kashi University (Punjab) – INDIA

Abstract

Internet of Things (IoT) research and industrial growth is accelerating, yet it still has privacy and security issues. Due to the decentralised architecture and resource constraints of the majority of IoT components, conventional security and privacy solutions are typically inapplicable to IoT. Each block in a blockchain is connected to the one that came before it. Every block contains the cryptographic hash code, the hash of the previous block, and the block's data. BC transactions are the primary data transfer units used between IoT nodes. IoT nodes are intelligent physical objects having embedded sensors, actuators, and programming that can communicate with other IoT nodes. The function of BC in the IoT is to provide a method for processing encrypted data records via IoT nodes. BC is a technique that can be utilised publicly and safely. This type of technology is required by IoT in order to ensure secure communication between IoT nodes in a complex environment. In this article, communication via Blockchain technology adoption in an IoT network is regarded as safe and secure.

Keywords: Blockchain, IOT network, Security, Vulnerabilities, Privacy.

DOI Number: 10.14704/nq.2022.20.9.NQ44367 **Neuro Quantology 2022; 20(9):3194-3201**

1. INTRODUCTION

The proliferation of IoT devices is on the rise, with the number of linked devices surpassing 7 billion in 2017, with predictions of 20-50 billion connections by 2020. Blockchain, being a distributed ledger technology, promotes itself as a viable solution to this problem. This is mostly due to blockchain's usage of cryptographic IDs, immutability of records, and provenance. These capabilities, when combined, provide a foundation for implementing IoT device identity management functions that may assure a worldwide and unique identity for the devices, as well as a means to maintain it over the device life cycle [1]. When it comes to the Internet of Things (IoT), Blockchain (BC) is a game-changing technology that utilises a decentralised, distributed, public, and real-time ledger to record transactions that take place between IoT nodes. A blockchain is a distributed ledger that is made up of a series of blocks, each of which is connected to the blocks that came before it [2]. The Internet of Things (IoT) is expanding at an exponential rate, with the goal of 5G technologies such as Smart Homes and Cities, e-Health, distributed intelligence, and so on; however, it has issues in terms of both security and privacy. The gadgets that make up the Internet of Things are connected in a manner that is decentralised [3]. The BC is a method that ensures the safety of financial transactions via Internet of Things devices. It offers a shared ledger that is decentralised, distributed, and open to the public for the purpose of keeping data from blocks that have been processed and confirmed in an IoT network [4].

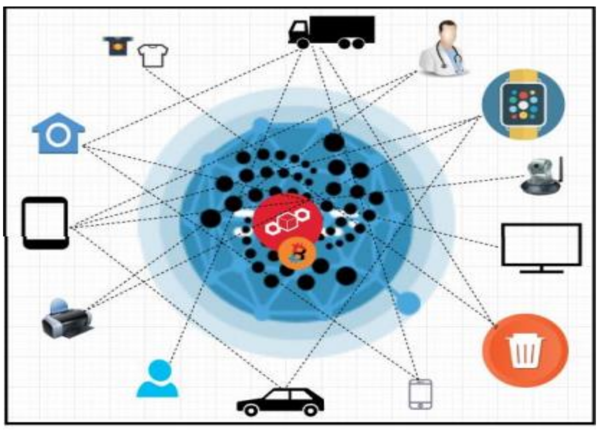

Figure 1: Blockchain and IOT

The data that is kept in the public ledger is automatically handled by the Peer-to-Peer architecture that is being utilised. Transactions that take place between IoT nodes are recorded in the form of a block in the blockchain through a method known as the BC. The blocks are connected, and each device knows the address of the prior device it was connected to. Within the context of Internet of Things and cloud integration, Blockchain and IoT work together. In the future, the BC would completely revolutionise the networking of the IoT [5]. As a result, the implementation of Blockchain technology in Internet of Things applications has seen a significant rise in the past few months. One of the most intriguing applications of blockchain is in the banking industry, where security and privacy are major concerns. With so many possible uses in so many fields, this new technology has the potential to make a big difference in the Internet of Things (IoT) vision in a number of ways, such as by increasing decentralization, making communication and transactional models more efficient, and letting devices work together on their own [6].

2. SECURITIES, VULNERABILITIES AND PRIVACY RISKS

The Internet of Things (IoT) is a paradigm-shifting technology that has surfaced as a consequence of progress made in the areas of sensor technology, embedded system technology, and communication. The wireless sensor network gave rise to this global network [7], which spans the entire planet. The Internet of Things is a completely decentralised and diverse system, which has resulted in significant increases in both privacy and security concerns. The network layer is in charge of establishing a connection between the perception layer and the Internet as a whole. In the case of fog computing or edge computing, this layer can also perform data analysis and storage before sending it to a cloud server for processing. The application layer is the third tier, and it is responsible for performing tasks such as data analysis, data storage, and data interpretation [8].

IoT security has been identified by a number of industry professionals as a primary concern for the successful widespread adoption of the technology [9], which has resulted in the Defense Advanced Research Projects Agency placing a significant emphasis on the development of IoT security shields (DARPA). In addition, [10] outlined ten different research topics related to the internet of things. These ideas have been sorted into the following three categories: cognitive Internet of Things security, adaptive and context-aware security, and end-node security [11]. As a consequence of this, a number of recent publications [12] investigated the use of machine learning (ML), artificial intelligence (AI), and blockchain technology as potential solutions to the problem of IoT security.

The most significant attacks on Internet of Things systems [13], including assaults on end devices, communication channels, network protocols, sensory data, denial of service attacks, and software attacks. It should come as no surprise that attacks on the Internet of Things might have significant ramifications; for instance, hackers in a single nation could get unauthorised access to traffic light controllers and manage the flow of traffic to their advantage [14]. A ransomware attack on the colonial pipeline system in the United States in 2017 resulted in a significant economic loss and created a disruption in the supply of fuel [15]. Because victims are required to pay a ransom in exchange for the release of kidnapped information technology resources or personal data, ransomware is an extremely profitable form of hack [16]. The use of ransomware, a new sort of assault that targets wearable technology, is one form of ransomware.

Security challenges

In today's cybersecurity scene, there is a severe lack of qualified personnel. This difficulty is exacerbated in the blockchain security area due to the fact that even fewer cybersecurity professionals possess blockchain expertise or comprehend the new security threats of the growing Web3 decentralised economy. Nonfungible coins, record-breaking investment, and market capitalization have given the blockchain sector a fresh lease of life in 2021. Aside from headlines and enthusiastic supporters, though, market excitement and activity draw greater attention. Existing cybersecurity concerns are becoming increasingly complex, and decentralised organisations introduce new threats. Rather than focusing on the technology, recent attacks against blockchain have focused on human weaknesses. Bitfinex's $73 million hack in 2016 was likely caused by the theft of secret digital signatures known as cryptographic keys [17].

Endpoint vulnerabilities, such as those at the device, app, wallet, or third-party vendor level, are additional entry points for malicious actors. Vendors and their employees, too, are at risk. In 2017, for example, an employee's PC was used to attack the Bithumb crypto exchange. Other things to watch out for are wrong data input and incompetent developers, even if they don't mean any harm.

TCP/IP and the Internet of Things network stack are quite similar. The protocol stack of the TCP/IP protocol is vulnerable. The need to protect IoT devices from cyber threats is urgent since they vary from sensors to industrial automation. Port scanning, spoofing, and sniffing/eavesdropping are examples of network flow attacks that are described by detailing IoT attacks and their methods. The RINA architecture is used to protect Internet of Things devices from the aforementioned network attacks. It focuses on safeguarding communication in a closed environment with RINA [18].

Every node has to do a block check, which adds a significant amount of time to the latency. You may make the selfish miner's assault worse if you have control of some nodes. When an attacker mines a block, the slave nodes can be set to retransmit it as fast as possible. Due to their decreased latency, attacks might be a benefit for attackers. By disclosing his blocks whenever he acquires a new block, the attacker can coerce the honest nodes to work for him. A portion of trustworthy nodes that have received an attack block will work on it so as to offer an attacker a power boost. In addition, the total number of blocks added to the chain is equal to the sum of the blocks that were added by persons who were either honest or dishonest. On the other side, forks cause the blocks to be thrown away, which then causes them to get stale. This difference in the number of blocks included is critical to ensure that the new difficulty, which nodes will recalculate based on fewer blocks than the prior difficulty, is lower than the total number of blocks created [5].

3. SECURITY IN INTERNET OF THINGS

When it comes to information systems, security and privacy are two key concepts to follow. Availability, integrity, and confidentiality are the three components of safety that we use. The technical security threats are, for the most part, comparable to those that are posed by desktop computers, smartphones, and conventional servers. It is imperative that weak authentication, failure to change default credentials, the exchange of unencrypted messages between devices, SQL injections, and bad security upgrades be addressed as soon as possible. But many Internet of Things devices are severely restricted in their ability to operate due to significant operational limits in terms of processing capacity. Some claim that government regulation is required in order to safeguard IoT devices and the larger internet, arguing that market incentives to secure IoT devices are inadequate [19]. Man-in-the-middle attacks on IoT development boards are easy to use due to predictable and weak keys. Numerous researchers have suggested fortifying SSH's implementation and weak keys.

The huge volume of data collected by sensors is a problem for developers of Internet of Things apps, who must clean, analyse, and interpret the data. Wireless Sensor Networks (WSNs) are a solution that has been presented for the analysis of information. These networks send sensor data to a distributed system for analysis. Large data storage is another issue. Depending on the application, data collection may require a lot of storage. The Internet uses 5% of all energy, and it's "daunting" to power IoT devices that capture and store data.

Blockchain Enhances Security and Privacy in the Internet of Things

The devices that make up the Internet of Things gather, create, and analyse data, and then transmit that information over the Internet, resulting in a massive amount of data that can be used by a variety of applications. Despite the advantages, there may be serious privacy concerns that must be addressed. When it comes to the creation of decentralised apps that will be used by billions of devices, the blockchain has the potential to be critical. It is difficult to comprehend how and when this technology may be utilised to guarantee security and privacy, and various writers have pointed out the difficulties in this regard.

A blockchain was originally a set of linked blocks deployed on untrusted peer nodes. Each block is responsible for protecting transaction data, the hash of the block that came before it, as well as its own hash. The many components of blockchain systems are broken down in the research and presented in Figure 2, as can be observed. The distributed ledger is the underlying database that blockchain technology uses (bampers). Without the need for a central authority, the blockchain protocol is managed by a peer network, which also makes it possible for transactions to take place. User identities are checked and managed by membership services. Smart contracts are software in blockchain technology that may perform certain tasks. Data integrity is ensured by the use of cryptography. Events are notifications of network changes, such as new transactions, new blocks, and new peers. System management develops, monitors, and modifies system parts. The third component is system integration, which connects the blockchain to other systems.

Blockchain provides privacy and access control for the IoT. Privacy in the Internet of Things is a challenge because "things" disclose owners' behaviour and preferences. One concept is to construct Internet of Things apps that employ a solid blockchain, where the Proof of Work algorithm and many honest miners would ensure integrity and anonymity. These challenges necessitate more prudence, which means IoT devices must utilise a unique address for each update, generate a new address for each receiving resource, and not rely on third-party services to receive changes. They won't guarantee perfect anonymity, but will protect identities [20].

Data storage and access control are two further applications for the Blockchain. Take, for example, a presence sensor that intends to record daily data on a blockchain. It will construct a transaction that includes the data that has to be maintained and sign it, which will make it possible for anyone to recognise the sensor. The data-reading public keys will be included in the transaction output that is produced by the sensor. The miners are notified of this transaction so that they can validate it and add it to the distributed ledger (blockchain). Additionally, due to the fact that the blockchain is accessible to the general public, everybody is aware of all the transactions that have taken place and is aware of the fact that a certain user has been given permission to examine the history that has been generated by the presence sensor. Whoever has possession of the private keys, on the other hand, will be able to access the daily history that the sensor has released.

Consensus algorithms ensure the blockchain's integrity and security. It's a way for block-chain network nodes to agree on the ledger's entries and transactions. When it comes to reaching agreement, different block-chain platforms employ a variety of algorithms, and, of course, each platform operates and executes in a unique way [21]. The Internet of Things (IoT) research field has become a lot busier because there are so many new items in communication and networking technologies.

The ability to exchange data, simplify access, and perform remote monitoring are just some of the benefits that may be gained from connecting many smart devices over the internet. One of the most significant challenges that the Internet of Things will need to surmount is getting past the centralised structure of its client-server architecture. Because a lack of trust between participating devices has the ability to bring down the entire network, a credible solution is necessary to prevent this from occurring. Following a number of different techniques developed over the past several years, the blockchain has gained appeal because of its characteristics such as decentralised structure, security, and immutability [22]. These issues call for a greater degree of caution, which means that Internet of Things devices need to make use of a unique address for each update, generate a new address for each resource that they receive, and not rely on third-party services to receive changes. They will not enable complete anonymity, but will provide a certain level of protection to allow identities to be preserved.

Network Attacks

An attack on a network is an intrusion into a network in order to gather information and exploit the target via open ports or IP addresses that are available. Although port scanning assaults are the first stage in a cyber-attack, they remain a significant concern. It is common practice for attackers to do a port scan on a target machine. The attacker may easily access the target system by using this port number to locate the services operating on the system [23].

Spoofing is an attack that uses fabricated information to get access to someone or something. IP address spoofing, ARP spoofing, DNS spoofing, and email spoofing are all examples of spoofing. This is a common assault in today's world. Eavesdropping is a form of a Man-in-the-Middle attack in which the attacker intercepts the private data, alters it, and presents it to the victim hosts as if it was the original data. It's a problem that's been around forever. In order to acquire access to network characteristics, an attacker listens in on the conversation between the victim hosts. Then, a virus or some other kind of bad software can be put into the system [24].

4. BLOCKCHAIN IN INTERNET OF THINGS FOR SECURITY ENHANCEMENT IN COMMUNICATION

IoT security and privacy are essential success elements in attaining the technology's lofty goals of transforming many aspects of our society and economy. The suggested blockchain-based IoT architecture addresses the majority of communication security and privacy risks while taking into account the resource restrictions of numerous IoT devices. After conducting a qualitative analysis of the architecture's overhead, we discovered that, at the very best, it maintains a constant performance in terms of its communication overhead, and at the very worst, the majority of its transactions scale with the number of clusters in the network rather than with the number of nodes. Our solution has been demonstrated in the context of a smart house; nevertheless, it is applicable in a more general sense to the majority of multi-tiered Internet of Things network topologies [25]. BlockChain (BC), the technology that forms the basis of the cryptocurrency Bitcoin, has recently been put to use in peer-to-peer networks with topologies that are analogous to those of the Internet of Things (IoT) in order to guarantee security and anonymity for users. [26] It is not necessary for the cryptocurrency blockchain technology to be accessible in the public domain for the purpose of communication. There is the potential for there to be private blockchains; nodes are the points on a private network, and a blockchain operates in the same manner as a distributed ledger. A large number of financial institutions are already using blockchain technology to certify compliance with regulatory requirements... Securing technologies, such as Blockchain, can be an important aspect of reducing the costs associated with compliance [27]. BCs, on the other hand, have high processing costs and result in significant bandwidth overhead and delays, which renders them unsuitable for use in IoT devices. This article presents a new architecture for the Internet of Things (IoT) that is safe, private, and lightweight. It is built on blockchain technology and eliminates the overhead of blockchain while preserving the bulk of the benefits it gives in terms of security and privacy. The presented method is investigated on an application known as a smart home application [28], which serves as an example case study for broader Internet of Things applications. The proposed architecture is hierarchical and consists of smart dwellings, an overlay network, and cloud storages that coordinate data flows with BC in order to provide privacy and security. Our strategy makes use of a number of different kinds of BCs determined by the level in the network hierarchy at which a transaction takes place, in addition to distributed trust mechanisms, in order to guarantee a decentralised topology. A qualitative review that made use of conventional threat models [29] highlights how helpful the architecture is in delivering security and privacy for applications related to the internet of things (IoT).

The application of block-chain technology is not limited to financial transactions only. A multi-step transaction in which traceability and visibility are required can be implemented using this methodology. In the supply chain, Blockchain may be used to monitor and sign contracts as well as verify product provenance, which is a prominent application of the technology. Voting systems, title management, and deed administration are just a few of the applications that may be made possible by this technology. It is expected that the number of practical uses of blockchain will increase as the digital and physical worlds become more closely integrated. The merging of public and private blockchains will result in an ecosystem in which businesses, customers, and suppliers may work in a safe, auditable, and virtual environment, resulting in exponential and disruptive development for blockchain [27].

With blockchain, fraud and hacking are expected to be extremely difficult. To better understand how blockchain technology can protect against fraud and other undesirable activities, this research looks at the weaknesses of the system. This study's suggestions for good defensive measures encourage more research into how to stop criminal behaviour related to blockchain [30].

5. CONCLUSION

This research looks on a ground-breaking method for ensuring the safety of communication known as BC and IoT. Because it can replace the current internet system with a new one in which every smart device links to other devices in real-time via a peer-to-peer network, which is more secure, this technique has the potential to be the future of the internet. It is able to cut down on the time and money already spent while simultaneously delivering precise information to the appropriate device in real time. The application of blockchain technology to the Internet of Things has the potential to enhance users' safety and privacy while also serving a useful purpose. Both the Internet of Things (IoT) and blockchain, which can be described as a distributed ledger system, are relatively recent conceptual developments. It is possible to develop software applications with the same fundamental capabilities as the Internet of Things and the Blockchain. Consider how the decentralised nature of the Blockchain could be of value to the Internet of Things while also redefining paradigms and bringing up new opportunities. This is one way. The blockchain technology, which is already widely used in cryptocurrencies like bitcoin and ethereum, may be able to improve the safety of devices that are part of the internet of things. The Blockchain contains built-in security safeguards that prevent data from being altered, such as limiting access to Internet of Things devices and turning off networks that have been compromised by hackers. First of its kind, Hyundai has made an investment in an Internet of Things (IoT) security start-up that is based on blockchain technology.

REFERENCES

1. Omar, A. S., & Basir, O. (2018). Identity management in IoT networks using blockchain and smart contracts. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*.
2. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/ijwgs.2018.095647
3. Alam, T., & Benaida, M. (2018). The role of cloud-MANET framework in the internet of Things (IoT). *International Journal of Online and Biomedical Engineering (IJOE)*, *14*(12), 97. https://doi.org/10.3991/ijoe.v14i12.8338
4. Alam, T., & Sharma, B. K. (2010). A new optimistic mobility model for mobile ad hoc networks. *International Journal of Computer Applications*, *8*(3), 1–4. https://doi.org/10.5120/1196-1687
5. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generations Computer Systems: FGCS*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046
6. K. Ashton (2009). That ‘internet of things’ thing. RFID Journal.
7. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/comst.2015.2444095
8. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*, 1–25. https://doi.org/10.1155/2017/9324035
9. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied*

Sciences (Basel, Switzerland), *10*(12), 4102. https://doi.org/10.3390/app10124102

10. Sfar, R., Natalizio, A., Challal, E., & Chtourou, Y. (2018). A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw*, *4*, 118–137.
11. Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*(100227), 100227. https://doi.org/10.1016/j.iot.2020.100227
12. Sinha, P., Rai, A. K., & Bhushan, B. (2019). Proceedings of the Information Security threats and attacks with conceivable counteraction. In *Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 1208–1213).
13. Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, *181*(103050), 103050. https://doi.org/10.1016/j.jnca.2021.103050
14. Ben Dhaou, I. (2021). A secure IoT-enabled sensor node for traffic light management and level of service computation. *2021 18th International Multi-Conference on Systems, Signals & Devices (SSD)*.
15. Tsvetanov, T., & Slaria, S. (2021). The effect of the Colonial Pipeline shutdown on gasoline prices. *Economics Letters*, *209*(110122), 110122. https://doi.org/10.1016/j.econlet.2021.110122
16. Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*. https://doi.org/10.1145/3514229
17. Cui, X. (2016). The internet of things. In *Ethical Ripples of Creativity and Innovation* (pp. 61–68). Palgrave Macmillan UK.
18. Atzori, L., Lera, A., & Morabito, G. (2018). The Internet of Things: A survey. *Tạp Chí Nghiên Cứu Dân Tộc*, *24*. https://doi.org/10.25073/0866-773x/64
19. Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, *32*, 17–31. https://doi.org/10.1016/j.adhoc.2015.01.006
20. Matsuo, S. (2017). How formal analysis and verification add security to blockchain-based systems. *2017 Formal Methods in Computer Aided Design (FMCAD)*.
21. Kim, Y.-J., Thottan, M., Kolesnikov, V., & Lee, W. (2010). A secure decentralized data-centric information infrastructure for smart grid. *IEEE Communications Magazine*, *48*(11), 58–65. https://doi.org/10.1109/mcom.2010.5621968
22. Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2019). Blockchain technology implementation in logistics. *Sustainability*, *11*(4), 1185. https://doi.org/10.3390/su11041185
23. Liu, M., Yu, F. R., Teng, Y., Leung, V. C. M., & Song, M. (2019). Performance optimization for blockchain-enabled industrial internet of things (IIoT) systems: A deep reinforcement learning approach. *IEEE Transactions on Industrial Informatics*, *15*(6), 3559–3570. https://doi.org/10.1109/tii.2019.2897805
24. Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*.
25. Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: Challenges and Solutions. In *arXiv [cs.CR]*. http://arxiv.org/abs/1608.05187
26. Amoozadeh, M., Raghuramu, A., Chuah, C.-N., Ghosal, D., Zhang, H. M., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, *53*(6), 126–132. https://doi.org/10.1109/mcom.2015.7120028
27. Ko, T., Lee, J., & Ryu, D. (2018). Blockchain technology and manufacturing industry: Real-time transparency and cost savings. *Sustainability*, *10*(11), 4274. https://doi.org/10.3390/su10114274

28. Gross, H., Hölbl, M., Slamanig, D., & Spreitzer, R. (2015). Privacy-aware authentication in the internet of things. In *Cryptology and Network Security* (pp. 32–39). Springer International Publishing.
29. Skarmeta, A. F., Hernandez-Ramos, J. L., & Moreno, M. V. (2014). A decentralized approach for security and privacy challenges in the Internet of Things. *2014 IEEE World Forum on Internet of Things (WF-IoT)*.
30. Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., & Zhang, Y. (2019). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal*, *6*(3), 4660–4670. https://doi.org/10.1109/jiot.2018.2875542