EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Blockchain Technology: A Panacea for IoT Security Challenge

Nehemiah Adebayo[1,*], Amos O.Bajeh[1], Micheal Arowolo[1], Erondu Udochuckwu[1], Kayode Jesujana[2], Ajayi Mary[3], Abdulrasaq Surajudeen[3], and John Onyemenam[4]

[1]Department of Computer Science, College of Pure and Applied Sciences, Landmark University, Nigeria
[2]Department of Computer Engineering, Faculty of Engineering, Ekiti State University, Nigeria
[3]Department of Computer Science, College of Pure and Applied Sciences, Landmark University, Nigeria
[4]Department of Electrical and Information Engineering, College of Engineering, Landmark University, Nigeria

Abstract

The Internet of Things (IoT) platforms, despite the wide range of application is not without loop holes of which cyberattackers can take advantage. In order to improve the platform's security while also increasing other features, it has been proposed that blockchain technology be implemented in any IoT system. However, while blockchain technology has many advantages, it is important to consider other options because they all have their own drawbacks that may not be ideal for every use case situation. IoT network devices have limited computer power, storage space, and bandwidth. As a result, these systems are easily prone to assault than other network connected devices, such PCs, cell phones and tablets. With focus on IoT security challenges and the countermeasures offered by the blockchain technology, consensus algorithm, data encryption and smart contracts were discovered to be the common and effective algorithm employed by the blockchain technology in securing Iot systems over time.

Keywords: : IoT, Blockchain technology, Consensus algorithm, Connected devices, Smart contracts.

Received on 08 June 2022, accepted on 26 September 2022, published on 04 October 2022

I]_
doi: 10.4108/eetiot.v8i3.1402

*Corresponding author. Email: adebayo.nehemiah@lmu.edu.ng

1. Introduction

IoT technology has grown exponentially in recent years, and the usage of connected devices and their applications has risen significantly in industrial and personal environments. [1], [2]. The number of connected devices is expected to reach 29 billion by the year 2022, with around 18 billion being connected to the Internet of Things [3], [4]. The Internet of Things (IoT) represents a major leap in information technology [2]. The Internet of Things has a wide variety of applications across various industries, including consumer electronics, the military, and industrial manufacturing. Health monitoring, remote monitoring, surveillance systems, smart buildings, and smart cities are examples of these applications. [5].

As the number of IoT devices grows at such a fast pace, data protection has become a serious challenge. Data collection and processing are critical to IoT applications, but privacy issues emerge throughout this process [6]. In smart city apps, for example, a user's location and travel information might be stolen or captured by an attacker, raising privacy problems. IoT privacy issues will be addressed by developing new techniques for preventing eavesdroppers from accessing personal information. [7]–[9].

Block chain technology is one method of enhancing Internet of Things (IoT) security. In the IoT, researchers have carried out a number of studies on blockchain technology and its use. Using the Joint Cloud platform, Xie

et al. undertake blockchain research on the Internet of Things using blockchain to manage to manage distributed control and access [10]. Using blockchain to safeguard IoT data has been studied by [11]. According to the study, security is one of the most difficult aspects of the IoT to deploy, but blockchain technology can be used to enhance the security of the Internet of Things. According to the study's findings, four different approaches may be taken to strengthen the security of the Internet of Things. These include utilizing blockchain technology for strong encryption, user authentication, recognizing genuine IoT, and IoT configuration. [11].

Using blockchain technology concepts, this article provides an outline of the current IoT security concerns and how these challenges might be addressed. Additionally, this presentation will address the limitations of blockchain technology in the IoT.

2. Internet of Things

The Internet of Things (IoT) is a network of connected objects that uses embedded systems, sensors, software, and artificial intelligence to collect data from the internet and use it in various intelligent applications [12]–[15]. Every linked gadget will have a distinct identification.

The primary goal of the Internet of Things is to enhance the quality of human existence by linking devices and people in order to make data collection simpler through the internet. The Internet of Things (IoT) in this situation enables new types of communication between gadgets and people, as well as between devices themselves [16]. Because of its extensive variety of applications [17], Iot is commonly referred to as the Internet of Everything [18]. These applications are sometimes classified as consumer, commercial, industrial, and infrastructural [18], [19].

Many IoT solutions aimed at the general public, such as connected cars, smart homes, smart clothing, smart health, and other devices that can be monitored remotely, are becoming increasingly popular. IoT gadgets are also part of home automation, a broader umbrella term encompassing anything from home lighting to climate control to media and security. Long-term benefits could include saving energy by having lights and other electronic equipment turn off automatically and letting people know how much energy is being used.[15], [18].

Despite the fact that IoT brings several advantages to people, there are some concerns about the risks connected with the expansion of IoT technology and services, notably in the areas of privacy and security [20]. Hackers are targeting IoT devices in order to steal sensitive information. This security risk reveals itself in all three IoT levels, namely the application, network, and perception layers. The emergence of this security risk is attributed, in part, to security rules that are violated in order to build affordable, simple, and small IoT devices [21].

2.1. Architecture of IoT

Since IoT technology can be used for so many different things, it's only going to get more popular. The Internet of Things works in a variety of ways depending on the specific use cases for which it was intended or created[2], [5]. It does not, however, have a universally adhered-to standard defined architecture of operation. The architecture of IoT is influenced by how it is used in different industries. Still, there is a fundamental process flow that underpins Internet of Things[22].

It is generally agreed that a three-layer high-level design is optimal as shown in figure 1. Perception, network, and application layers make up this architecture's three tiers [23], [24].

The perception layer

This layer contains sensors, actuators, and other devices. This sensing layer contains physical and environmental sensors, actuators, and gadgets. Input data (such as physical or environmental factors) is received, processing is carried out, and then outgoing data is sent over the network.

Network layer

In this tier, you will find the Data Acquisition System (DAS) and Internet/Network gateways. Data gathering and conversion are two of DAS's primary responsibilities (receiving and aggregating data, and translating analog data from sensors into digital information). In addition to linking sensor networks to the Internet, sophisticated gateways provide a wide range of vital gateway tasks. These functions include virus protection and monitoring, decision-making centered on input data, and other services.. Software applications, sometimes called "business apps," have access to the data stored in this pre-processed location and can monitor and manage it as well as plan out next steps once it has been sent to the central data center. At this point "Edge IT" or "Edge analytics" will come into.

Application layer

The third layer of the Iot architecture is the stage of data management where data is managed and utilized by applications such as agriculture, medical services, aviation, agriculture, military, and so on [23].

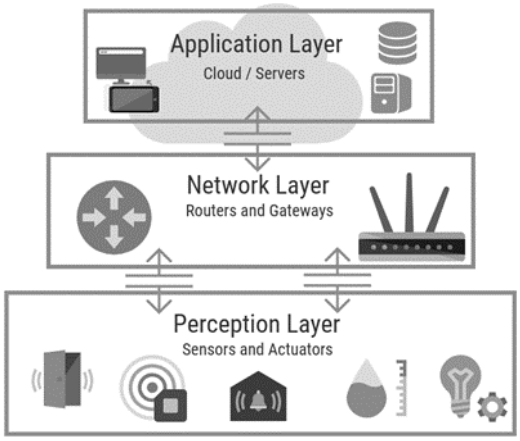

Figure 1. Iot 3 layer architecture

3. Security Challenges of Iot

Over 23 billion devices are presently connected to the Internet of Things. This number will rise to 60 billion by the end of 2025 and there is a price to pay for this avalanche of new gadgets. Device security is a major issue for tech companies manufacturing these devices, and this is one of their biggest failings.

In many circumstances, these gadgets and IoT devices do not get the essential updates, and in other cases, none at all. Despite its consumers' original perception that it was secure, a previously protected piece of equipment can become accessible to hackers and other security concerns. In the early days of computers, automated updates helped to address this problem. There is a hurry to develop and market IoT devices as soon as possible, with little consideration for security. Most manufacturers only provide firmware upgrades for a certain amount of time before moving on to the next product that will attract everyone's attention. However, the reasons for this practice are not always clear. The company's loyal clients are exposed to hackers due to these outdated gear and software.

Users must be protected from such attacks. Each device must be properly tested before it is distributed to the public, and companies must regularly upgrade their gadgets to keep them safe at all times. Failure to do so is a terrible idea for both businesses and their consumers, since a single large-scale leak of consumer data may completely devastate a company.

IoT-enabled equipment benefit various industries, including health care, retail, manufacturing, and life sciences. It identifies several problems in a broad variety of networked devices [25]. The main offenders for the absence of security in internet of medical things(IOMT) devices are computed tomography (CT) equipment and magnetic resonance imaging (MRI). Inadequately secured devices, such as ventilators, lighting, and infusion pumps, are subject to hacking efforts, which may result in: interruption of operations; exposed customer data and safety; financial losses; and damaged reputations [8], [9], [25].

The above-mentioned IoT security threats can be significantly mitigated by deploying IoT security solutions. The end-to-end solution requirements of customers are met, as are the fundamental device security challenges addressed by device management. These platforms may aid in the improvement of how IoT assets are configured, software is updated, security problems are recognized, alarms are delivered, and they are reported.

Khan and Salah divided IoT security concerns into three categories: low-level, intermediate-level, and high-level IoT security.

Jamming, spoofing, sleep deprivation attacks, and an unsafe physical interface are examples of low-level security flaws. These occur at the communication's physical and data connection levels, as well as at the hardware level.

At the intermediate level of security, communication, routing, and session management are the main issues. Fragmentation and buffer reservation attacks, which cause denial-of-service when successive fragment packets are refused due to space filled by unfinished packets sent by the attacker, are common security weaknesses at this layer. Compromised nodes already in the network can launch several attacks on the Routing Protocol for Low-Power and Lossy Networks (RPL) at this layer. Resources might be depleted, and confidential information could be intercepted as the attack proceeds. Eavesdropping, violations of users' privacy, and denials of service are only some of the primary issues that might arise from sinkhole and wormhole assaults on the transport layers.

Most of the high-security concerns revolve around applications running on IoT. Insecure firmware, software, and interfaces in the cloud, on the web, and on mobile devices are the most common sources of security problems in this environment [26].

4. Blockchain Technology

The distributed ledger technology (DLT) that blockchain is an implementation of is designed to foster an environment of trust and confidence. A distributed ledger system is what blockchain is based on, and it is copied and spread over a network of computers. It allows all defined nodes or members to access encrypted transactional data on the blockchain. [27].

To get access to the encrypted data contained in blocks, the originating entity may utilize verification, validation, and consensus. The blockchain network is intended to provide data integrity and provenance, to be tamperproof and auditable, pseudonymized, resistant to Distributed Denial of Service attacks, and to be safe, private, and secret. These characteristics make the blockchain network a one-of-a-kind, transparent, and secure method of managing online transactions [28].

A comprehensive risk assessment is performed to ensure the security of a blockchain system or network. Cybersecurity frameworks, security testing processes, and safe coding standards are used to protect a blockchain system against online fraud, breaches, and other attacks. Blockchain security is a vital technology that should be employed to secure the dependability and quality of IoT technology [28].

5. IOT and Blockchain Technology

Blockchain and the Internet of Things (IoT) are both mature and expanding at the same time. As a result of their interdependence, being together allows for the greatest potential for growth. Supply chain management may benefit greatly from IOT's security, immutability, and smart contracts, while the blockchain relies on IOT's ability to transform the data input into a big-time opportunity [29]

As a new platform for the Internet of Things, blockchain technology has recently been developed to offer a secure mesh network and dependable connections, eliminating the dangers that come with traditional central server architectures. The blockchain already powers many IoT systems needing remote sensors and automation for many companies, including banks, industrial enterprises, and agricultural businesses. An eco-friendly Internet of Things (IoT) relies on a decentralized, low-power blockchain network that eliminates the need for centralized cloud servers [22].

Authentication and integrity can be ensured by the use of a unique public key and a globally unique identifier (GUID) for each IoT device linked to the blockchain network. In addition, each transaction involving an Internet of Things device is added to the distributed global ledger maintained by blockchain technology and may be linked to the original device at any point in time. [26]. In addition, Khan and Salah claim that the decentralized authentication rules and logic made possible by blockchain smart contracts may be utilized to give single and multiparty authentication to an Internet of Things device. Unlike OpenID, OAuth 2.0, and LWM2M, smart contracts can provide far more effective access rules to linked IoT devices than the traditional authorization protocols. It is normal practice to utilize these protocols for IoT devices to authenticate and operate. Protect the privacy of stored or transmitted data, "smart contracts" can establish the criteria and timeframes under which a particular individual, set of users, or machines own, manage, use, or access the data. [26].

5.1. Previous Works

Mohanta et al., 2021 implemented a typical IoT blockchain system using smart contracts and a consensus algorithm. As indicated in Figure 2, a set of smart contracts is distributed in the network, where they will run independently. The Ethereum platform executes a smart contract automatically after it has been verified and validated by a network node. Digital signatures and encryption are used to broadcast the smart contract's conclusion across the network.

An ethereum platform-based blockchain-based authentication mechanism for IoT devices was established outside of the IoT network in order to increase trust in the IoT application. The scaling of the IoT network was rigorously regulated using blockchain permission.[30]

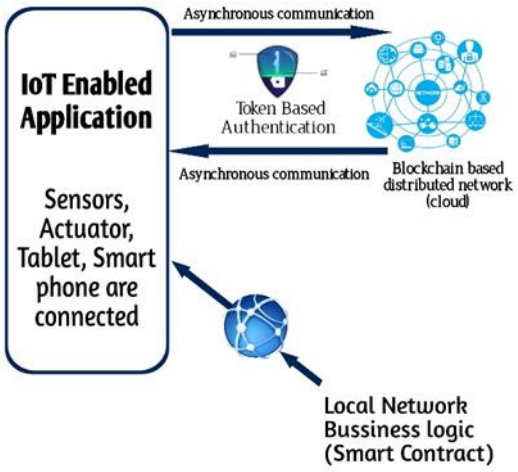

Figure 2. Iot blockchain network using smart contract

On the subject of IoT permission delegation and access control, a study by Ali et al. (2019) has been published. There is a restricted set of permissions that an IoT device or user can have at first. Additional permissions are granted through permission delegation. Using BC, Mohanta et al technique of permission delegation is replicated. Smart contracts on BC are created by IoT device owners to protect their resources. To access a

resource, an IoT device or user submits a request via the BC's resource smart contract.

BC verifies the trustworthiness and delegation rules of the delegatee platform prior to permission activation. Their approach combines event-based and query-based permission delegating capabilities. The Confidentiality, Integrity, and Availability model is used to assess the security of our architecture. [31]

Gattolin et al. (2018) suggested a blockchain-based method to key management transparency utilising a three-layer architecture known as block chain-assisted key transparency for device authentication (BlAsT), which enables the establishment of an infallible and publicly certifiable linear history. Blockchain technologies such as Bitcoin and Ethereum are supported by the framework. For better management transparency, it has incorporated BC. The identity provider links the user ID to the public key upon registration. The Signed Tree Root (STR) is then entered by the identity provider in BC. ECDSA signatures, current and prior epochs, and current and previous Merkle Roots are all part of the STR. With BlAsT, users may retrieve STR from the BC and use it to verify the accuracy of their personal information held with the identity provider. According to the findings, BlAsT is a cost-effective method that enables end users to monitor and recognise bogus keys connected with their identities. [32]

Tapas et al. (2018) presented a decentralized design for resource access authorization and delegation duties as a boost to an IoT-Cloud solution. The proposal includes blockchain as a technological foundation for this scheme, as well as smart contracts as the primary engine for trustless decentralization and independent auditing of operations. [33]

It was proposed by Ding et al. 2019 that the Internet of Things may benefit from an attribute-based access control system based on blockchain technology to better manage device access management. The lack of confidence in the system was addressed by implementing a decentralised and scalable access control mechanism. The IoT devices are designed to be independent of the blockchain network's consensus process, which reduces overall processing and communication cost dramatically. The modular architecture of consensus algorithms like the AKA protocol enhances the system's flexibility and simplifies future maintenance and modifications. The work's security analysis showed that the method is secure in practice, and simulated trials showed that enforcing rigorous and fine-grained access control in IoT is effective and efficient. [34]

Previous research clearly demonstrates that the smart contract and consensus algorithm are the most commonly employed blockchain technologies to safeguard IoT systems.

5.2. Discussion

Decentralization and autonomy are inherent qualities of the blockchain, which makes it a perfect component for IoT systems. IoT can benefit from it, especially in terms of comprehending decentralized and private-by-design IoT. This study discusses a number of prominent properties of the blockchain that make it a promising technology for tackling the aforementioned privacy and security concerns of the Internet of Things. Some of the frequently used algorithm of blockchain in Iot sytems are further discussed below.

(i). Consensus Algorithm

When it comes to distributed blockchains, consensus addresses the issue of how they can be consistent. It is a key part of how the blockchain system works. The consensus mechanism makes sure that every node in a P2P network is fair. It is an integral component of the entire system and a set of guidelines that every node must adhere to. By finding and combining trustworthy nodes, the system is able to create a permanent record that cannot be altered. In the blockchain system, each node is responsible for maintaining a common ledger database with the same information, this makes it hard to change. As part of keeping the blockchain operational, every node in the system competes with the others to be the first to receive incoming transaction records. As part of this process, each node also checks the integrity of the data stored in the blockchain system. Proof of work (PoW), proof of share (PoS), delegated proof of sake (DPoS), and practical Byzantine fault tolerance (PBFT) are some of the consensus techniques on the blockchain[26].

Users' identities are distributed over the blockchain network using the asymmetric encryption public key. Therefore, a typical PKI-based certification authority is unnecessary and thus eliminates the problem of certificate authorities as we know them. Instead, the blockchain relies on a consensus process to keep the network safe and secure. This approach does not require you to reveal your identity; all you have to do is modify the address. Using the consensus technique, IoT data transmission may be made more secure while also protecting the privacy of specific devices or individuals [15].

(ii). Data Encryption

In order to send data securely across the blockchain system, an asymmetric encryption method is needed. In the asymmetric encryption technique, the transmitting and receiving nodes must produce a set of public and private keys ahead of time to secure their communications. Before exchanging information with the nodes receiving it, they will first exchange a public key. The information will then be encrypted by the sender using the receiver's public key, and the sender's private key will be the only thing that can decrypt the information. The only node that is aware of the private key is the one that gets the information. This ensures that the information sent is trustworthy and secure [20].

Encryption on a blockchain uses a method of encryption known as asymmetric encryption, which entails both the encryption of data and the use of digital signatures. With the encryption of data on a blockchain, you can be certain that your data is safe from unauthorized access and manipulation. To keep track of each transaction, the blockchain uses a timestamping mechanism. The ID enables the user to obtain specific transaction details. Each block's uniqueness can be demonstrated using a hash of the algorithm. More than half of the nodes must agree if data is to be changed. Because of the way the blockchain works and is constructed, this is a very remote possibility. Digital signatures are used to establish ownership of and approval for transaction data before it is delivered across the network. ECDSA, which stands for elliptic-curve digital signature algorithm, is one of the most common digital signature algorithms. [28].

(iii). Smart Contract

The IoT responds and performs the actions required to meet the rules and conditions that have been established, and the procedure should be carried out in the prescribed order. To decide whether or not to go forward, several procedures make use of the status parameter. This makes the operation complex and time-consuming. As a result, many processes cannot be conducted automatically and repeatedly in a satisfactory manner. Code-based agreements are known as smart contracts. Smart contracts are programs that automatically makes a guarantee. The smart contract automatically releases and transfers data when specific criteria are satisfied. A smart contract resembles a web server from a technological perspective. This server is not linked to the Internet. Instead, it performs blockchain-based contract programs. Smart contracts are agreements that can be programmed. They do this by converting user transactions into a code that is then recorded in a blockchain and given its own unique address. Because of the blockchain technology, smart contracts can look for after themselves and even have legal force. Smart contracts make it easier for Internet users to trust one another and build trust [17].

The logic of businesses, as well as their legal rights and duties, may be automated using smart contracts. In addition to this, they serve as the basis for the protection of users' security and privacy, and improving the general performance of the IoT. Smart contracts can automatically use different security measures based on what the user needs and how much private data they have. [10].

6. Conclusion

According to past studies [7], [15], [20], IoT security issues can be solved using blockchain technology. When it comes to the notion of defenses-in-depth, blockchain methods must be used in conjunction with other security measures such as firewalling, encrypted operating systems that can be trusted, and software updates that can be updated only by trustworthy sources. In the IoT ecosystem and on other platforms with privacy and security issues, blockchains offer the advantage of working at both the lower and higher tiers of the communications models, allowing for the mechanism to be used effectively across layers and domains. The blockchain technology algorithm currently provides the most dependable and secure structure for the development of IoT systems. Future research should concentrate on enhancing blockchain's capacity, security, and scalability in order to successfully aid in the synchronization of IoT with blockchain technology.

References

[1] Dachyar, M., Zagloel, T. Y. M., & Saragih, L. R. (2019). Knowledge growth and development: internet of things (IoT) research, 2006–2018. Heliyon, 5(8), e02264. https://doi.org/10.1016/J.HELIYON.2019.E02264.

[2] Perwej, Y., Ahmed, M., Kerim, B., & Ali, H. (2019). An Extended Review on Internet of Things (IoT) and its Promising Applications. Communications on Applied Electronics, 7(26), 8–22. https://doi.org/10.5120/CAE2019652812

[3] Collela, P. (2022). Ushering In A Better Connected Future - Ericsson. Ushering In A Better Connected Future. https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/ushering-in-a-better-connected-future

[4] Shurman, M., Obeidat, A. A.-R., & Al-Shurman, S. A.-D. (2020). Blockchain and smart contract for IoT. Ieeexplore.Ieee.Org. https://ieeexplore.ieee.org/abstract/document/9078958/

[5] Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F., & Kanhere, S. S. (2020). Blockchain Technologies for IoT. 55–89. https://doi.org/10.1007/978-981-13-8775-3_3

[6] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences 2020, Vol. 10, Page 4102, 10(12), 4102. https://doi.org/10.3390/APP10124102

[7] Liang, W., & Ji, N. (2021). Privacy challenges of IoT-based blockchain: a systematic review. Cluster Computing, 0. https://doi.org/10.1007/s10586-021-03260-0

[8] Patel, C., & Doshi, N. (2019). Security Challenges in IoT Cyber World. 171–191. https://doi.org/10.1007/978-3-030-01560-2_8

[9] Patel, C. (2021). IoT privacy preservation using blockchain. Https://Doi.Org/10.1080/19393555.2021.1919795. https://doi.org/10.1080/19393555.2021.1919795

[10] Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H. N., & Imran, M. (2020). Blockchain for cloud exchange: A survey. Computers & Electrical Engineering, 81, 106526. https://doi.org/10.1016/J.COMPELECENG.2019.106526

[11] Singh, M., Singh, A., & Kim, S. (2018). Blockchain: A game changer for securing IoT data. IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings, 2018-January, 51–55. https://doi.org/10.1109/WF-IOT.2018.8355182

[12] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International

Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

[13] Alam, N., Vats, P., & Kashyap, N. (2018). Internet of Things: A literature review. 2017 Recent Developments in Control, Automation and Power Engineering, RDCAPE 2017, 192–197. https://doi.org/10.1109/RDCAPE.2017.8358265

[14] 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 (Netherlands), 11, 100227. https://doi.org/10.1016/j.iot.2020.100227

[15] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Addressing Security and Privacy Issues of IoT Using Blockchain Technology. IEEE Internet of Things Journal, 8(2), 881–888. https://doi.org/10.1109/JIOT.2020.3008906

[16] Kamble, A., & Bhutad, S. (2018). Survey on Internet of Things (IoT) security issues & solutions. Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018, 307–312. https://doi.org/10.1109/ICISC.2018.8399084

[17] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things (Netherlands), 1–2, 1–13. https://doi.org/10.1016/j.iot.2018.05.002

[18] Peng, S. (2021). Applications of Blockchain Technology. In Blockchain for Big Data. https://doi.org/10.1201/9781003201670-5

[19] Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. Computer Communications, 136(August 2018), 10–29. https://doi.org/10.1016/j.comcom.2019.01.006

[20] Fakhri, D., & Mutijarsa, K. (2019). Secure IoT Communication using Blockchain Technology. ISESD 2018 - International Symposium on Electronics and Smart Devices: Smart Devices for Big Data Analytic and Machine Learning. https://doi.org/10.1109/ISESD.2018.8605485

[21] Mouha, N. (2022). The design space of lightweight cryptography. Eprint.Iacr.Org. https://eprint.iacr.org/2015/303

[22] Mezquita, Y., Casado, R., Gonzalez-Briones, A., Prieto, J., & Corchado, J. M. (2019). Blockchain technology in IoT systems: Review of the challenges. Annals of Emerging Technologies in Computing, 3(5 Special Issue), 17–24. https://doi.org/10.33166/AETiC.2019.05.003

[23] Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017. https://doi.org/10.1155/2017/9324035

[24] Aziz Rao, T. (2018). Security Challenges Facing IoT Layers and its Protective Measures. Article in International Journal of Computer Applications, 179(27), 975–8887. https://doi.org/10.5120/ijca2018916607

[25] Albesher, A., & Albesher, A. A. (2019). IoT in Health-care: Recent Advances in the Development of Smart Cyber-Physical Ubiquitous Environments. IJCSNS International Journal of Computer Science and Network Security, 19(2). https://www.researchgate.net/publication/331642487

[26] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

[27] Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain Technologies: foreseeable impact on industry and society. Computer, 50, 18–28.

[28] Idrees, S. M., Nowostawski, M., Jameel, R., & Mourya, A. K. (2021). Security aspects of blockchain technology intended for industrial applications. Electronics (Switzerland), 10(8). https://doi.org/10.3390/ELECTRONICS10080951

[29] Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149–160. https://doi.org/10.1016/j.dcan.2017.10.006

[30] Ali, G., Ahmad, N., Cao, Y., Asif, M., Cruickshank, H., & Ali, Q. E. (2019). Blockchain based permission delegation and access control in Internet of Things (BACI). Computers and Security, 86, 318–334. https://doi.org/10.1016/j.cose.2019.06.010

[31] Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access, 7, 38431–38441. https://doi.org/10.1109/ACCESS.2019.2905846

[32] Gattolin, A., Rottondi, C., & Verticale, G. (2018). BlAsT: Blockchain-Assisted Key Transparency for Device Authentication. IEEE 4th International Forum on Research and Technologies for Society and Industry, RTSI 2018 - Proceedings. https://doi.org/10.1109/RTSI.2018.8548405

[33] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Addressing Security and Privacy Issues of IoT Using Blockchain Technology. IEEE Internet of Things Journal, 8(2), 881–888. https://doi.org/10.1109/JIOT.2020.3008906

[34] Tapas, N., Merlino, G., & Longo, F. (2018). Blockchain-Based IoT-cloud authorization and delegation. Proceedings - 2018 IEEE International Conference on Smart Computing, SMARTCOMP 2018, 411–416. https://doi.org/10.1109/SMARTCOMP.2018.00038