



Review Article

A STUDY OF BLOCKCHAIN IN IOT ARCHITECTURE

Authors: Mehmet Ali Şimşek 

*Corresponding Author: masimsek@nku.edu.tr


To cite to this article: Şimşek, M.A., (2021). A Study of Blockchain In IOT Architecture, International Journal of Engineering and Innovative Research, 3(2), p 163-174.

DOI: 10.47933/ijeir.851109

To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



A STUDY OF BLOCKCHAIN IN IOT ARCHITECTURE

Mehmet Ali ŞİMŞEK^{1*} 

¹Tekirdağ Namik Kemal University TBMYO, Department of Computer Technologies, Tekirdağ, TURKEY.

*Corresponding Author: masimsek@nku.edu.tr
(Received: 31.12.2020; Accepted: 15.02.2021)

<https://doi.org/10.47933/ijeir.851109>

ABSTRACT: Industry 4.0 includes that components such as artificial intelligence, big data, autonomous systems, human-robot interaction, and the internet of things. Because of these components; some benefits are aimed, such as minimizing human impact, reducing costs, and increasing business volume. It is seen that the most fundamental problem of Internet of Things (IoT) technology, which is one of the basic concepts of Industry 4.0, is security. In recent years, blockchain architectures have been trying to find a solution to this problem. This study focuses on blockchain architectures used in the IoT ecosystem.

Keywords: IOT, Blockchain, Industry 4.0, IoT.

1. INTRODUCTION

IoT, which is one of the basic concepts of Industry 4.0, facilitates communication between different types of devices due to the development of the internet and hardware in recent years. These developments, where billions of devices access the Internet, have enabled the development of the Internet of Things concept. The goal of IoT is to develop a smarter environment and a simplified lifestyle by saving time, energy, and money [1-2].

IoT is the network of all kinds of things embedded with sensors, electronics, software, etc. connected to the internet according to the Global Standards Initiative of the International Telecommunication Union. Gartner predicted that by the end of 2015, 4.9 billion linked objects will be used, reaching 25 billion by 2020 [3]. In recent years, it has been observed that the devices connected to the internet have increased exponentially all over the world. These devices are expected to grow at a higher rate in the future. It is estimated that IoT will be able to connect 500 billion devices by 2030 [4]. It is seen that IoT is used in different areas as a result of the increasing use and importance.

IoT devices and applications appear in many areas such as smart cities and smart grids, education, finance, banking, communication, control, health, and defense. Such a trend, it is also called Internet of Things (IoT), Internet of Medical Things (IOMT), Internet of Battlefield Things (IOBT), Blockchain-Based Internet of Vehicles (IOV). In short, it also calls the internet the Internet of everything that includes the internet [5]. IoT technology is getting bigger and more complex. It is seen as an innovation that we can communicate with and manage with every object in our life.

It seems that the IoT ecosystem is growing steadily. Accordingly, the increase in the volume of data it carries causes security weakness. This raises the public and industry stakeholders to worry about being exposed to security breaches.

As IoT devices proliferate, these devices often lack the necessary authentication standards to keep user data safe. Hackers' wide variety of attacks enters the device is damaged critical infrastructure is to know. It needs to be widely adopted to ensure trust, authentication, and standardization among all elements of IoT [6]. It is important not to experience both financial and data loss in such attacks. Although there are some technologies to ensure security in data communication between IoT objects, the most prominent is the blockchain.

Blockchain provides a decentralized data storage service with a break-proof ledger made up of blocks serially chained in distributed networks. It can record and secure transactions or transaction events using encryption. The first blockchain was proposed by Satoshi Nakamoto in 2008. Cryptocurrency in 2009 - Bitcoin apply for the activation technique is MIS [7-8].

Although blockchain was originally designed for cryptocurrencies, thanks to its effective success, it is used in many areas today. Interestingly, blockchain is implemented in many industries beyond cryptocurrencies because of its unique and attractive features such as transactional privacy, security, data immutability, auditability, integrity, authorization, system transparency, and fault tolerance. This a la those some identity management, intelligent transportation, supply chain management, mobile crowdsensing, agriculture, industry 4.0, energy internet (IOA), and security in mission-critical systems emerge as [9].

Security of IoT devices; It can be divided into 3 main sections as authentication, connection, and operation. Efforts to prevent problems in identity verification, data communication, and processing have recently gained importance. Recently, blockchain applications have been used to ensure the physical and hardware security of IoT. With blockchain, it provides the reduction of danger, the creation of data privacy, and protection from third parties in data transfer. Thus, it also makes the end-to-end (P2P) communication safe. For all these reasons, it is said to play an important role in IoT security.

Although blockchain architecture was first used in cryptocurrencies in 2008, it was introduced in 1991. The first use of blockchain architecture with IoT was in 2015. When the relevant literature is scanned with the keywords "Blockchain", "IoT", "Internet of Things", it is seen that thousands of publications are made. It is seen that the usability of the existing two technologies together increases as time passes. Within the scope of this research study, researches, original articles, and conference papers that have been published in good journals and have a high number of citations will be scanned.

In the studies examined so far, it is seen that the data set cannot be kept on IoT devices due to security problems, but this can now be made possible with the help of blockchain technology. Different IoT architectures are also proposed where the data can be stored distributed without being collected in a center.

Authentication in IoT devices and sending information to other devices in the ecosystem are seen as another problem in terms of security. It is seen that the blockchain architecture can be used for end-to-end messaging transactions and for data security.

The structure of blockchain, its areas of use, why blockchain is important for IoT, the future of blockchain in IoT technologies, difficulties in its use, and the difficulties of using blockchain in today's IoT technologies constitute the scope of this study. In addition, examples of blockchain architectures used in IoT technologies are given in Section 3.2.

2. Blockchain and Uses

Although blockchain architecture was first introduced in cryptocurrencies in 2008, it was introduced in 1991. The first use of Blockchain architecture in conjunction with IoT was in 2015.

Blockchain can be thought of as blocks chained together. Since the advent of a new type of cryptocurrency (such as Bitcoin), they are also publicly referred to as digital notebooks. Blockchain is a comprehensively distributed architecture that emphasizes features such as data consistency, transparency, user privacy, resistance to backward changes, and so on. Unlike other centralized systems, blockchain-based systems often use a peer-to-peer (P2P) network to deploy data processing tasks to different nodes. Using a mechanism called compromise, information stored on each node and the data generated can be synchronized [10].

Generally, a blockchain is a distributed ledger with timestamps built on a P2P network using a consensus mechanism between nodes. Blockchain has neutralization, anonymity, traceability, transparency, and tamper-proof features. The blockchain is built on the P2P network and is located on every node in the P2P network. The P2P network implemented on the blockchain is a peer-to-peer, decentralized, and distributed network of computers. In a P2P network, the state and functions of all nodes are equal. Shared resources set up by nodes such as compute resources, storage resources, and network resources can be shared by other nodes. The more nodes added to this network, the more resources are shared, and the better the service quality of the whole system. The decentralized nature of the P2P network brings scalability and robustness to it, which is the basis for the success of the blockchain. The P2P network structure is shown in Figure 1 [11].

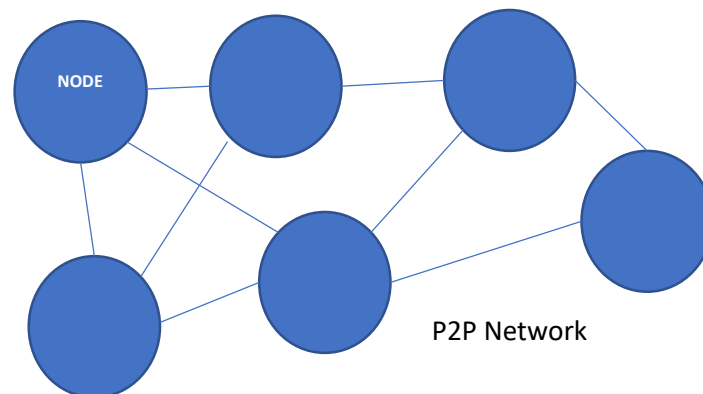


Figure 1. Blockchain P2P network structure.

A block in Blockchain architecture is a collective dataset that can be defined using a cipher function of each block. The created block contains a summary of the previous block. In this way, all data can be linked through a connected chain structure. Each block points to the immediately preceding block via a reference, which is the hash value of the previous block called the top block. Figure 2 shows a blockchain architecture. Each block; consists of two

parts, the head, and the body. Title part; the block version contains structures such as the password of the ancestor block, the time stated the current password format. The first block of a blockchain is called the genesis block, which has no main block [9, 12]. Figure 3 shows the general structure of a block.

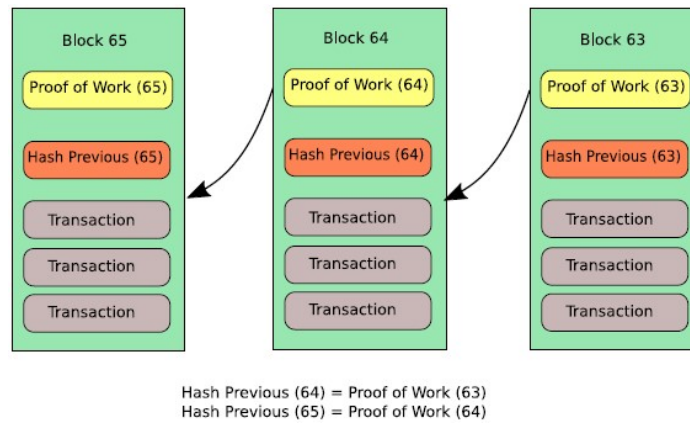


Figure 2. Architecture of Blockchain [9].

Block version	02000000
Parent Block Hash	b5ff0b1b1680a2862a30ca44d346d9e8 910d334beb48ca0c000000000000000
Merkle Tree Root	9d10aa52ee949386ca9385695f04ede2 70dda20810decd12bc9b048aaab31471
Timestamp	24d95a54
nBits	30e31b18
Nonce	fe9f0864

Transaction Counter

TX 1 TX 2 ... TX n

Figure 3. A block structure for blockchain [12].

Blockchain networks generally; the public blockchain is divided into three different categories: the private blockchain federal / consortium (Federated or Consortium) blockchain. The public blockchain provides access to everyone, nobody has access restrictions. Anyone can read and write data on this network. Private blockchain is based on permission. Nobody can access it unless the blockchain administrator has been given permission. Consortium or federated blockchain networks show similarities in permissions to private blockchain networks. Consortium blockchain is a specific blockchain that has authorized nodes to protect distributed data [13, 14].

Blockchain applications; many IoT applications now appear to be using blockchain for various purposes. Generally, it is seen that it is mostly used in digital payment, smart contract service, digital signature and data storage areas [10].

Digital payment: it is the first and most used area for blockchain. While initially operating on a distributed network supported by high-performance machines, now proprietary optimization supported by large blockchains such as Bitcoin and Ethereum is used for devices with insignificant computing power such as smartphones and pocket computers. Rather than being assigned large computational jobs, low-end devices often operate as lightweight nodes that do not keep the entire chain in their local repositories or participate in the most power-hungry

processes such as mining. These features have made mobile payment with the technical blockchain much more accessible than before [10].

Smart contract: a part of "crypto economically secure code execution" running on the basis of blockchain. Without any assistance from third parties, the smart contract automatically executes the relevant contract term after the defined condition is triggered. In addition, it provides real-time auditing as all actions are recorded and verified as transactions in a decentralized blockchain ledger. These operations are traceable and undeniable, thus increasing machine execution security. It converts various assets such as smart contracts, IoT devices, and digital assets into virtual identities on the blockchain and enables them to interact with other assets. The smart contract is attractive as an efficient and secure method to replace normal contracts. With the smart contract, the Blockchain is used to replace the Intelligent Transport Structure (ITS) and perform reliable software updates of IoT devices [7].

Digital signature: Each user has a pair of private keys and public keys. The private key is used to sign transactions. Digitally signed transactions are spread over the entire network and can then be accessed by public keys that are visible to everyone on the network [12].

Data Storage: It has shown that it can be used as a database for distributed and secure storage of data sets in blockchain data storage applications. The given chain can be used for data privacy. It can be used to group data such as health, financial and education.

3. BLOCKCHAIN FOR IOT

IoT and blockchain are customized and optimized blockchain systems to enable IoT applications. IoT applications have been developed and applied in many areas. However, most of these apps are prone to issues like data loss and systematic malfunction. To mitigate these problematic effects, blockchain has been used to provide higher security and stability for traditional IoT applications [10].

Blockchain was originally used to record financial transactions where transactions are encoded and held by all participants (Bitcoins and other cryptocurrencies etc.). Thus, all transactions have become transparent and any changes can be easily tracked and detected [5]. Blockchain offers actionable reality to increase IoT security. In this section, views on the importance of using blockchain for IoT security, architectural examples, usage challenges and future are given.

3.1 Importance of Blockchain Technology for IoT

Blockchain technology has been envisioned by the industry and the redial community as a stunning technology that is ready to play an important role in managing, controlling, and most importantly, securing IoT devices [15]. It is powerful enough to be a technology that provides an important opportunity to provide viable security solutions to blockchain's tough IoT security problems today.

Blockchain for IoT devices is what devices have done in the past; It allows it to be kept under a registry without being changed. These devices provide verification without being connected to third party devices. In addition, it provides the opportunity to securely provide device-to-device (P2P) messaging and data transmission. Blockchain brings new approaches to Internet of Things technology in privacy and security issues.

Figure 4 shows a typical blockchain transaction. When a transaction is made, a block is created. The block is broadcast to all nodes in the network. One of the nodes verifies the block (called mining in bitcoin) and streams it back to the network. If the block is validated and the block references the previous block correctly, the nodes add the block to their blockchain [5].

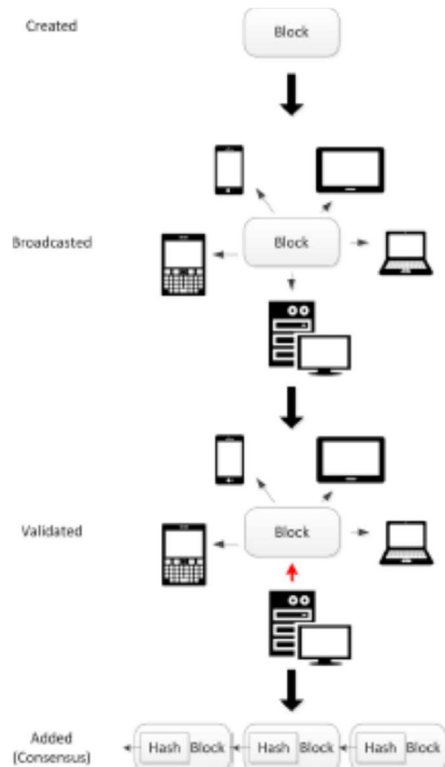


Figure 4. A typical blockchain workflow [5].

3.2. Samples of Blockchain Architectures Used in IoT Technologies

Blockchain technology is seen as one of the solution suggestions for the IoT ecosystem due to the increasing importance of concepts such as security, privacy, and confidentiality. Based on this approach, some architectures that include IoT and blockchain technology have been developed. OSCAR, ACE, BPIIoT architectures are one of them. Under this section, the architectures that have offered solutions from 2018 to the present are examined.

3.2.1. IoTChain

IoTChain, a program that combines the OSCAR and ACE authorization framework to provide an E2E solution for secure authorized access to IoT resources, Alphand (2018) et al [16]. Suggested by. Under the ACE framework, clients must create an encrypted and authenticated channel with a secure authorization server that requires the use of certificates or unlimited secret sharing. In addition, rogue authorization servers can freely issue access tokens for each protected resource. It replaces the only trusted authorization server in the ACE framework with a trusted authorization blockchain. The authorization block chain enhances the ACE authorization model by keeping resource access control robust, flexible and possibly confidential. The blockchain consensus protocol requires an attacker to control at least 51% of the blockchain before obtaining illegitimate tokens. In IoTChain, the resource owner discloses access rights in a smart contract, which automatically generates access tokens for the customer when certain conditions are met. Unlike ACE, the access token is not transmitted to the client, but the smart contract is stored securely in internal storage. The smart contract can then be

interrogated by other organizations to check the validity of the token [16]. In this architecture, the IoT device is responsible for data generation. The data owner is responsible for uploading the data to the blockchain. The OSCAR architecture and ACE authorization framework are responsible for ensuring the security of user data [10].

Figure 5 shows the main elements of the architecture and shows the sequence of operations leading to authorized access to IoT resources. The terminology specified by the IETF has been followed to avoid confusion regarding nomenclature and the roles of different organizations.

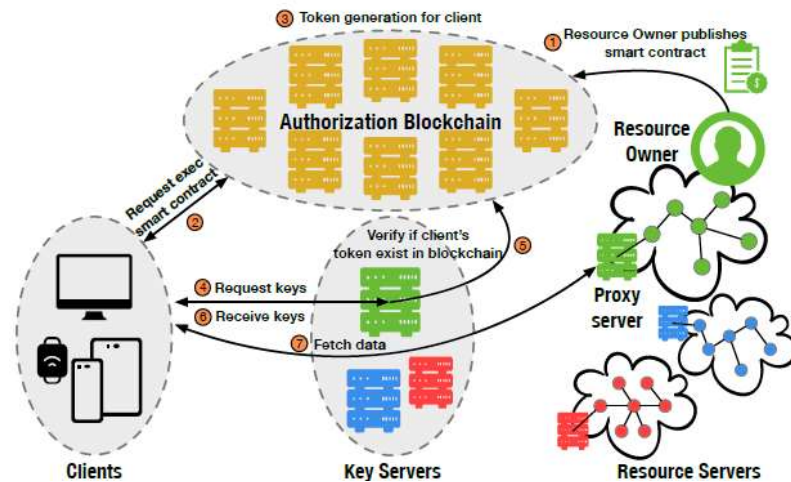


Figure 5. IoTChain architecture [16].

Source Servers (Resource Servers) creates and stores protected resources.

Resource owners (Resource Owners) are the legal owners of the resources that the source server and create them.

Clients are third parties seeking access to protected resources.

Proxy Servers (Proxy Servers) source server resources in a manner substantially restricted when stores encrypted.

Key Servers (Key Servers) to encrypt resources and create the necessary keys to decrypt.

Access tokens, (Access tokens) describes a particular client and the access rights of a particular resource.

Authorization Servers (Authorization Servers) creates access tokens.

3.2.2. Distributed access control system in IOT

Distributed access control system in IoT is proposed by Novo (2018) [17]. It is a new decentralized access management system in which access control information is stored and distributed using blockchain technology. All assets will be part of blockchain technology except IoT devices and headquarters nodes. Nodes in a blockchain network must contain a copy of the blockchain. The size of the blockchain can be quite large and will continue to increase over time. Most IoT devices will not be able to store blockchain information due to their constraints. As a result, the proposed architecture does not include IoT devices in the blockchain and

alternatively defines a new node called the management center that requests access control information from the blockchain on behalf of IoT devices.

In addition, the solution includes a single smart contract that defines all allowed operations in the access control system. This contract is unique and cannot be deleted from the system. Entities called administrators can interact with the smart contract to define the access control policy of the system [17]. Distributed access control system architecture in IOT is given in Figure 6. The architecture consists of 6 different structures: wireless sensor networks, administrators, agent node, smart contract, blockchain network, and management centers.

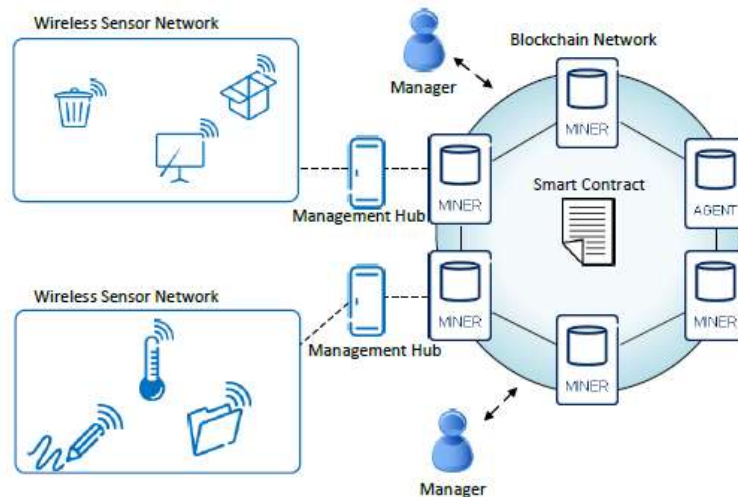


Figure 6. Distributed access control system architecture in IoT [17].

3.2.3. IIOT recommended for mild hybrid based blockchain's architecture

The lightweight hybrid-based blockchain architecture proposed for IIoT was proposed by Seok and Park (2019) [16]. Industry IoT (IIoT) includes many heterogeneous devices with limited resources . If we apply existing blockchain technology, it could affect the availability of the network. In order to increase the efficiency of IIoT, computational resources should be calculated and scalable, removing lag times.

Recommended block chain net "cell node" and "storage node" from the formed and the area between the layer and the control layer operates. Purdue model was used to design the proposed architecture. The architect area layer corresponds to level 0 and level 1 in the Purdue model. The proposed architectural control layer corresponds to level 2 in the Purdue model. To cover many heterogeneous devices in a large area, its area is divided into a small area called "Cell" and almost all IIoT devices connected to the located cell node. The cell node creates a block from data collected by connected devices and broadcasts to other nodes in the blockchain for block validation after block mining. After the block validation process, all the node participating in the block validation sends the return message to the storage node for the result validation notification, and then the block update is processed. Storage nodes, block and update records book ni is responsible for managing. In the block update process, the storage node adds the approved block. All of the processed transactions can be checked from the distributed ledger on the storage node [18]. Figure 7 shows our proposed architecture.

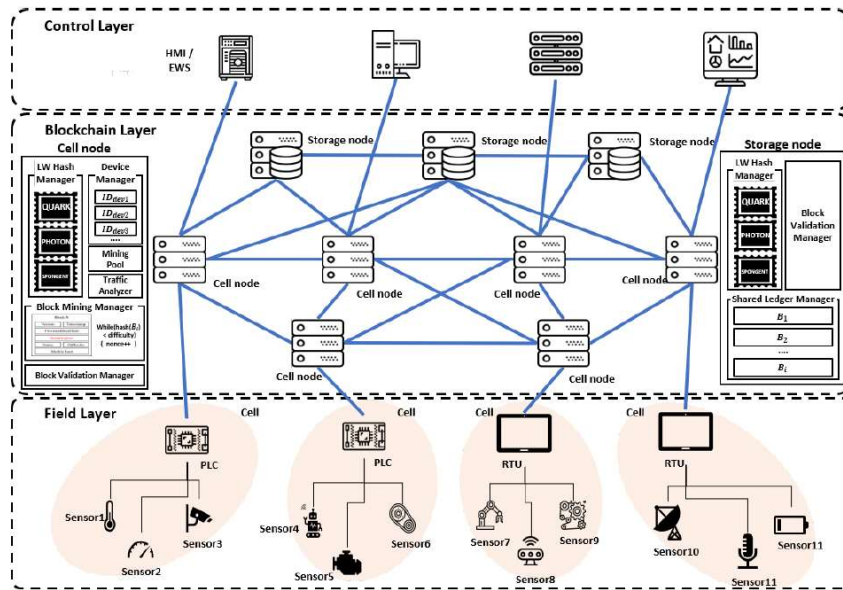


Figure 7. IIOT proposed for a lightweight composite based blockchain the architecture [18].

3.2.4. Health care monitoring architecture

The model proposed by Attia (2019) et al [19] focuses on a remote healthcare monitoring scenario of out-of-hospital patients. For this purpose, information on the health status (blood pressure and oxygen saturation, heart rate, body temperature, etc.) of each patient and a person is obtained. Other sensors can be installed in the patient's home to monitor the patient's immediate environment and allow detection of a person's activity and events such as falls. Data broadcast by these wearables and other sensors in the home are permanently uploaded to a remote database system. At this stage, a live monitoring system steps in to analyze this data to detect abnormalities and alerts clinicians who can take some action remotely if necessary. These data are also stored to keep track of all occurring events and can serve physicians following the evolution of patients' health status. All transactions between different parts of our scenario are carried out on very sensitive personal data. It is clear that these medical reports must be confidential and have limited access in a global system that ensures they are not objectionable. To meet all these requirements, an architecture based on blockchain technology has been proposed to remotely monitor patient status [19]. The architecture shown in Figure 8 basically consists of two blockchains, a monitoring system and medical devices.

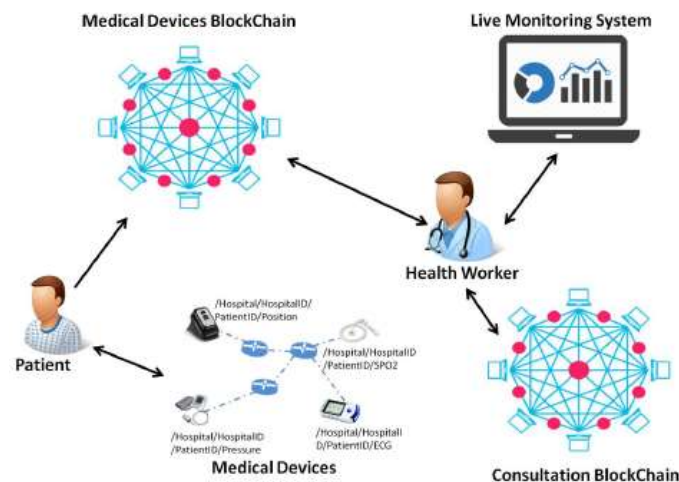


Figure 8. Healthcare monitoring architecture [19].

3.3. Challenges in Using Blockchain in IoT Technologies

Despite the benefit that blockchain brings to traditional IoT applications, there are still many hurdles in its implementation. The biggest problems arise from the limitations of IoT devices. Issues such as task distribution, power consumption, and computing capability need to be considered for blockchain to be effectively implemented in most IoT applications. To overcome these problems, there have been many attempts to adopt blockchain in IoT applications in recent years [10]. It is hoped that in the future, IoT devices will be able to work fully integrated with blockchain and gain more capabilities in the field of application.

A recent study found that the processing power and associated energy costs required for public blockchain networks are challenging for enterprise scenarios. In other words, the Bitcoin network consumes enough energy to power over 1.3 million US households [4]. Considering that many devices will join the IoT world day by day, energy consumption is seen as a huge problem. It emerges that studies on power consumption should be carried out among future studies.

Blockchain technology can be applied effectively in almost all areas of IoT. Considering the number of nodes and block size involved in the encryption process for such systems, it appears to affect power usage, network propagation, and network congestion [9]. In some cases, it may not be necessary to use a blockchain. It can be determined whether the system created will use blockchain or not and a choice can be made accordingly.

When too many verification requests are made, the prolongation of the time required for the processing of transactions is another problem. Stronger hardware structures are required in order to perform these processes in a shorter time.

It is known that data sets obtained from IoT devices are collected in a central device. Thanks to Blockchain technology, these data; In other words, membership information is recorded and shared by all members, including the center. In other words, membership information is recorded and shared by all members, including the center. But the lifetime of these data subjects is another problem that needs attention. Owners of datasets may not want to share them permanently. However, once any transaction is recorded by the blockchain, it cannot be changed or deleted. While this is a strong security property, if any record needs to be removed it may not be suitable for sharing. As a solution to this situation, the blockchain structure named Reference Integrity Metrics (RIM) has been proposed by Banerjee (2018) et al [5].

The industrial IoT ecosystem consists of many heterogeneous devices with constrained resources (Sensors, Actuators and Programmable Logic Controllers (PLC) etc.) and network availability should preferably be considered. Therefore, there are difficulties in implementing existing blockchain technology [18].

3.4. Blockchain Future in the IoT Ecosystem

IoT technology will play an increasingly important role in our society or in the foreseeable future in both civilian and military (hostile) contexts, including the internet of drones, the internet of battlefields, and the internet of military things [5]. Therefore, it is obvious that the security of all IoT devices used, especially in the defense industry, will be the most important issue. It is most desirable to protect data security and privacy in end-to-end communication of devices, whether in individual use or in industrial use, and that data is not

passed on to third parties. When all these situations are considered together, it is seen that the biggest issue in IoT devices is security.

Blockchain appears to be the most optimal solution to security for IoT devices. It is seen that blockchain-based solutions are recommended and used for the IoT ecosystem, increasingly since 2015. Although it is accepted that there are some problems experienced with the use of blockchain in the IoT ecosystem, it should not be ignored that the problems in the past have been solved. It is known that new studies are carried out to overcome the problems of the IoT ecosystem with the blockchain, which further increases the security by offering a distributed security system. Each step taken to solve the difficulties mentioned in Section 3.3 will serve to create a more optimal IoT ecosystem.

4. CONCLUSION

This study looks at the use of blockchain technology in the IoT ecosystem. In accordance with this purpose; It has been sought to answer the suggestions such as why blockchain is important for IoT, what is the future of blockchain in IoT technologies, what are the difficulties in its use and the difficulties of using blockchain in today's IoT technologies. In the literature studies, the use of IoT-blockchain, which has been increasing since 2015, is seen. Examples of architectures encountered in the literature are also included.

In every aspect of modern life, the existence of IoT devices and the existence of security problems of these devices are now seen. Although IoT-blockchain technologies appear to be used, IoT-blockchain applications are still in their infancy. However, the integration of IoT and blockchain is evolving and growing rapidly.

It is thought that the difficulties in using blockchain in IoT technologies specified in Section 3.3 will be solved and developed one by one in the near future. It is obvious that IoT-blockchain applications will develop rapidly in these days when it is important to ensure the security of communication, information and data.

Considering that the number of IoT-blockchain applications is increasing every year, it is believed that new consensus mechanisms to improve the performance of IoT devices in blockchain networking will be well in the coming years. Also, solutions to solve the problem of scalability, processing power or storage of the IoT device in the blockchain network are interesting issues.

REFERENCES

- [1].Mahdavinejad, M. S., Rezvan, M., Barekataan, M., Adibi, P., Barnaghi, P., & Sheth, A. P. (2018, August 1). Machine learning for internet of things data analysis: a survey. *Digital Communications and Networks*, Vol. 4, pp. 161–175. <https://doi.org/10.1016/j.dcan.2017.10.002>.
- [2].Ahmet Ali Sützen, "A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem", *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.12, No.1, pp.1-12, 2020. DOI: 10.5815/ijenis.2020.01.01
- [3].Charmonman, S., Mongkhonvanit, P., Ngoc Dieu, V., & van der Linden, N. (n.d.). Applications of Internet of Things in E-Learning. In *International Journal of the Computer, the Internet and Management* (Vol. 23). Retrieved from www.charm.SiamTechU.net.
- [4].Mouri, N. J. (2019). Nusrath Jahan Mouri IOT Protocols and Security Faculty of Computing and Electrical Engineering. (July).
- [5].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>.

- [6]. Shaik, K. (2018). Why blockchain and IoT are best friends - Blockchain Pulse: IBM Blockchain Blog. Retrieved April 25, 2020, from IBM website: <https://www.ibm.com/blogs/blockchain/2018/01/why-blockchain-and-iot-are-best-friends/>.
- [7]. 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>.
- [8]. Gürfidan, R., Akçay, Z. (2020). Blok Zincir Temelli Güvenli Elektronik Oylama Modeli. *International Journal of Engineering and Innovative Research*, 2 (3), 148-155. DOI: 10.47933/ijeir.746235
- [9]. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, 6(2), 2188–2204. <https://doi.org/10.1109/JIOT.2018.2882794>.
- [10]. Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Computing Surveys*, 53(1). <https://doi.org/10.1145/3372136>.
- [11]. Ren, Y., Zhu, F., Sharma, P. K., Wang, T., Wang, J., Alfarraj, O., & Tolba, A. (2020). Data query mechanism based on hash computing power of blockchain in internet of things. *Sensors (Switzerland)*, 20(1). <https://doi.org/10.3390/s20010207>.
- [12]. Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), 352. <https://doi.org/10.1504/ijwgs.2018.10016848>.
- [13]. Khan, A. G., Zahid, A. H., Hussain, M., Farooq, M., Riaz, U., & Alam, T. M. (2019). A journey of WEB and Blockchain towards the Industry 4.0: An Overview. 2019 International Conference on Innovative Computing (ICIC). Retrieved from <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8966700>.
- [14]. Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8), 3690–3700. <https://doi.org/10.1109/TII.2017.2786307>.
- [15]. 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>.
- [16]. Alphand, O., Amoretti, M., Claeys, T., Dall’Asta, S., Duda, A., Ferrari, G., ... Zanichelli, F. (2018). IoTChain: A blockchain security architecture for the Internet of Things. *IEEE Wireless Communications and Networking Conference, WCNC, 2018-April*, 1–6. <https://doi.org/10.1109/WCNC.2018.8377385>.
- [17]. Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184–1195. <https://doi.org/10.1109/JIOT.2018.2812239>.
- [18]. Seok, B., Park, J., & Park, J. H. (2019). A lightweight hash-based blockchain architecture for industrial IoT. *Applied Sciences (Switzerland)*, 9(18). <https://doi.org/10.3390/app9183740>.
- [19]. Attia, O., Khoufi, I., Laouiti, A., & Adjih, C. (2019). An IoT-Blockchain architecture based on hyperledger framework for healthcare monitoring application. 2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2019 - Proceedings and Workshop, 1–5. <https://doi.org/10.1109/NTMS.2019.8763849>.