IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

A PROXY REENCRYPTION METHOD FOR SECURING DATA SHARING USING BLOCKCHAIN

[1] JAYA J. KURIL, [2] PROF. H. R. VYAWAHARE

[1] P.G Student, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India,
[2] Assistant Professor, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India.

Abstract: IoT is a technology that enables us to connect and communicate in physical and digital environments. This enables us to obtain new digital services, which in turn improves our lives. Despite the numerous advantages of IoT systems, existing intermediate structures have numerous single point of failure issues such as data integrity and security. These barriers impede the future growth of IoT applications. Addressing these challenges will address the challenges of integrating IoT with broader ledger technologies. Blockchain is one of the most popular distributed ledger technologies. Combining IoT and blockchain technology has several potential benefits. As a result, this article describes the integration of IoT systems with blockchain technology. Following an overview of IoT systems and blockchain technology, a comprehensive review of the integration of blockchain and IoT systems is provided, highlighting the benefits of integration and how blockchain can help resolve IoT systems' complexities. Blockchain is defined as an IoT service, an example of how various components of blockchain technology can be used as services for different IoT applications.

***Index Terms* - Blockchain Technology, Cloud Computing Technology, Internet of Things, Information Technology, Proxy Server, Data Sharing, Security.**

I. INTRODUCTION

IoT devices are often used to solve common problems and to improve our lives by finding and collecting a variety of data about the environment and using it to create new digital resources. The Internet of Things has been a worldwide success, with billions of devices sold and used in various consumer markets[1]. People use IoT systems in a variety of industries, but centralised IoT buildings, where all IoT objects are connected, monitored, and managed on the same server, have a number of issues. These challenges hinder the development of future IoT applications. One point of failure affects the quality and availability of services provided by IoT. When the server falls, all related applications and IoT services are reduced. [2] .Network means communication or connection between one or more other peers using the connected i.e method. Wireless or wireless objects refers to wireless information to ensure safe data transmission. A brief overview of network properties, parameters, and features is provided. The network is generally regarded as a medium software platform for the purpose of calculating in the late 1970s, and Arpnet's invention has led to the modern Internet. It was one of the most influential consequences of the 20th century, which had the demands required to exchange data on the Internet, while the demands were growing in the early 20th century. Today, all the research and disciplinary centers are directly related to the infrastructure of communication directly or indirectly. In the form of a variety of new technologies, the local storage network, computer intelligence, processing backend, and data efficiency, including intelligent and display, including intelligent and display, including intelligent and display, demand for the world network (WWW) Review. Standard network model. The age of communication promotes long communication and reliability of communication through communication channels. Typically, communication modules are developing technologies and research on networks, which connect the modern infrastructure and connect a remote connection under a channel line that leads to a wireless connection system. The infrastructure adjusts a built-in communication system protocols such as TCP and Datagram User Protocol (UDP) [4, 5].

The research work provided in this paper navigates to the file sharing network over the network in multiple infrastructure areas of the P2P connection model [6]. Main understanding of the file testing of the network infrastructure is typically connected to a fixed attribute field, such as the type of file type, size, and type of format. These properties are defective properties because they can be changed through data channels and communication links. Important deviations in technology development are considered to be lacking intelligence that understand the local data address of the most frequently asked files or requested files. Therefore, this research question is explored and explored in this article. The main goal of this project overview is to design and develop an intelligent and secure file sharing infrastructure using blockchain-based peer-to-peer. The network has grown rapidly since the early 2000s and today covers almost everything in telecommunication and telecommunications [7].

II. OVERVIEW OF INTERNET OF THE THINGS

The IoT is a term that refers to the number of Internet-connected devices that include built-in computers. Many different types of things are referred to as "smart" technology.The use of information technology increased as computers became more common in modern technology (IoT). This new technology has been rapidly evolving, and it has made its appearance in the modern world. IoT devices have contributed to making our daily life easier. [one]. The term "Internet of Things" has no direct meaning because it is so broad and widely used. The Internet of Things has been described by several organizations and scientists.

In 2008, the number of IoT devices on the world surpassed the number of people. Because of the numerous advantages of Internet of Things systems, people are constantly developing new applications and services. According to Statista [9], there will be 31 billion Internet of Things (IoT) devices in use around the world by the end of 2020. This figure should be on more than 62 billion devices by the end of 2024, as shown in the figure. First and foremost, the IoT industry is rapidly expanding. According to information sources, IoT is expected to generate $743 billion in revenue in 2015. By the end of 2019, this figure is expected to more than quadruple to $1.71 trillion. [9].

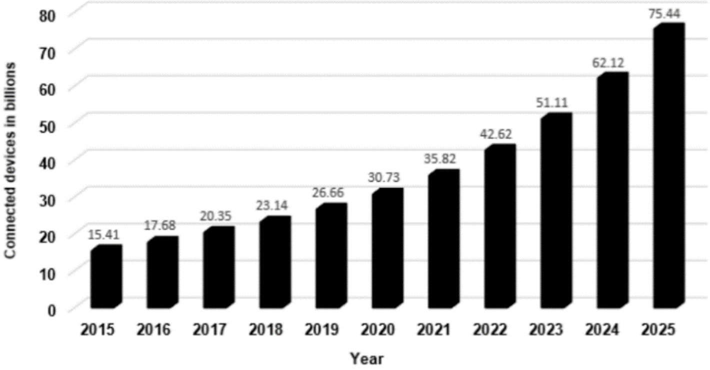

Fig. 1. Internet of Things growth from 2015 to 2025

“The architecture of the IoT reflects a contemplative design that can completely change us, our business, and our economy. The Internet of Things creates numerous digital controls and applications with little advantage over traditional systems. These applications and management share several common features, including” [1, 10]

[a]. Sensory capabilities: A new target driving development in various IoT environments is remote sensing (WSN) organizations. A WSN is a sensor organization that typically receives data about environmental factors and transmits this data via contact mode for control. Sensors are the square of the IoT architecture, giving the master the ability to collect all continuous and logical data on environmental factors to enable timely, accurate and accurate decisions to be made.

[b]. Accessibility: One of the key features of the IoT platform is the ability to remotely unlock billions of gadgets and things. It also integrates what's different from your current situation and allows you to communicate with each other online, allowing for new applications and management.

[c]. Largest Organization: The IoT framework contains billions of gadgets, and by the end of 2025, the framework is expected to contain 75 billion gadgets. This massive number of gadgets and things forms a massive network that cannot be controlled using traditional or traditional methods.

[d]. Robust Architecture: The IoT is inherently strong architecture. It can link different topics in different places. Additionally, sensors that collect a variety of continuous and logical data about environmental factors can radically modify IoT devices to change context and circumstances.

[d]. Scope of knowledge: Advanced technologies, capabilities that enable a collective of scheduling and related information enable IoT devices to make intelligent decisions in multiple situations and to intelligently participate in a variety of interactions.

[f]. Additional information: There are plenty of IoT devices generating enormous amount of information that traditional information validation methods cannot verify. This stands for the term "great knowledge". The Internet of Things is one of the most complex sources of information generating vast amounts of information that require innovative testing methods to make the most of our knowledge of the Internet of Things.

[g]. Notable features: IoT infrastructure enables various things to collaborate online. It is possible to ensure that the Internet will function if each gadget has a individual symbol or identifier, such as an IP. When a device joins the Internet of Things, the product assigns each device a unique identifier that can be used to track down other devices in the same category. If one of those devices has a problem, the other devices in that category can be kept up to date. There are also billions of IoT devices, but each one has a new set of characteristics.

[h]. Independent choice: IoT environments have many sensors, so you can gather reliable, up-to-date information about normal weather. These unique capabilities allow IoT devices to build on a balanced, stand-alone solution configuration.

III. LITERATURE REVIEW

CHI, J., Li, Y et al (2020) This article describes secure, efficient data exchange methods based on blocking technology and public arguments, and considers the importance of data and sharing. In this program, the data ring frame based on hyperel organizations load a large amount of sensory data and prepare a joint use of network blocks. A large number of customers are divided into interactions and similarities, and similar data, and are divided into several societies based on similar data, and they only transfer data to the distribution of useful information and the distribution of useful information and a significantly increased priced price. Data [16].

AGYEKUM ET Al (2021) because the device of the Internet device has a limited resource; Peripherals act as a hosting server that complete complex calculations. You can also use the information network to successfully communicate the data archived with the profile, so you can use information capabilities to improve service quality and take advantage of the perfect advantage of network bandwidth. In addition, our system is based on Blockchain technology, GAMECHANGING technology that allows expanded data exchange [17].

Fan, Q., Chen, J et al (2021) This study combines Blockchain technology to provide station bias authentication and IoT data exchange. They ensure that the validation of information and confidentiality is trusted and essential. Compares to other four similar solutions IoT, comparing the safety characteristics and measurement performance to provide an honest compromise between safety and performance [18].

Yu, Y. et al (2018) The Internet of Things brings great convenience to people's daily life by sharing data and making full judgment. However, this creates security and privacy concerns. Blockchain technology can solve these privacy issues in the IoT technologies. [19].

Xuan, S. et al. (2019) As the Internet of Things industry grows; Data is becoming an important asset of our culture and economy. Smart transportation, smart healthcare and smart homes are just some of the aspects of the Internet of Things that are generating and sharing large amounts of data. As a result, the data exchange market is gaining momentum. Data owners can use data exchange marketplaces for auctioning data to data consumers [20].

Banerjee, M., et al (2018) Internet Off Own (IoT) is increasingly distributed in social and military contexts, including smart cities, intelligent grids, internet of medical things, and Internet Battlefields. From January 2016, discuss the IOT security solutions to navigate to English published in English. They are the levels of the sensitive database of other related organizations as well as the level of public IoT databases for exchanging sensitive data data with the lack of public IoT databases for research, as well as the level of public IoT databases for exchanging sensitive data data with other related organizations as well as other related organizations [21].

ViriyAsitavat, W et al (2019), and profit creation of global scale global scale, provide limitations to solve safety requirements for permanent number of objects. It is a serious problem to measure the application when securing security. Blockchain technology (BCT) is a promising solution for securing and protecting large-scale personal security. In particular, smart contracts provide an opportunity to increase the reliability of IoT applications. Smart contracts establish what data is trusted and what the data does. Several tutorials and stop articles on BCT and IoT integration have been published recently [22].

H.N. et al. (2019) The purpose of this paper is to consider the integration of blockchain and IoT. This combination of blockchain and IoT is called BCoT. They did extensive research on BCoT. We start with a brief overview of online content and blockchain technology. Then we discuss the possibilities of BCoT and explain the structure of BCoT. Afterwards, they will discuss the challenges of researching next-generation blockchain networks. They discussed the discussion of potential applications of BCoT and proposed an open method for the study of BCoT [23].

Honar Pajooh, H et al (2021) pointed out various mistakes in centralized IoT deployment, and transitioning IoT to a decentralized LED system may be the wisest move. One of the most widely used ledger technologies is blockchain. We focus on isolation processes to maximize efficiency and avoid single errors. In addition, the safety and integrity of the data is improved due to evidence of Blockchain technology and continuous function. Blockchain and IoT technology integration can help reduce medical restrictions when opening paths for future development. As a result, the purpose of the study was to submit a comprehensive idea on the integration of IoT systems and block chain technologies. [24].

Zhang, Q ET AL (2021) created a universal data system that uses group signatures to use group signatures to control Wel lanalyzed access and data integrity by other groups. It also provides a Blockchain mechanism to provide the public audit of distributed data so that it does not require trusted third party audits in a traditional data audit system. Also using group signatures, our system provides anonymity and tracking for traitors. Analysis of security and performance tests showed that our system is suitable for large-scale online applications [25].

A. Shamir's article, he introduced a new cryptography that allows everyone to secure and verify everyone's signatures without having to store sensitive references or use resources and without exchanging private or public keys. third person. The program assumes that you have a trusted key generator, and its purpose is to provide each user with a smart card the first time they connect to the network. The information contained in this card allows you to log in when you encrypt a message that you send. The same card helps man to remove encryption and confirm the message that is completely independent, but it will help you identify the identity of the other side. When a card is issued, a new user must not be updated when joining an existing network. Various agencies should not control or connect or connectivity, or not support a list of users. The agency can be closed after completing the process of issuing the map, and the network can continue to operate on a special network for a weapon period.

D.Boneh,presented open key systems to find out the issues that retrieve encrypted data. Think about Bob users who send an Alice Open key encrypted an Alice user to an encrypted email. Email Gateway E-mail Keyword Make sure that there is an emergency that emergency situations can be placed correctly. Alice does not want to give all messages opportunities to open. The author explains and builds a method that can provide a gate key that can provide a gate key that can provide a gate key that can make sure that the Gateway is not read from emails and can make sure that the emergency words can be verified. It defines the concept of public key encryption via keyword lookup and provides several properties

IV. IOT WITH BLOCKCHAIN BASED DATA SHARING

Technology Blockchain sends a data node and data stream of a single computer science center to another computer science center based on a bit coin, leading to a selected public and security network to determine and improve the results of a series of information responses . In general, clogging is formed using a template associated with information to facilitate security transactions. As a result, this technology was concentrated and recognized in early 2015, and the box was impressed by the world of computer science and financial transactions. Full information on the Blockchain network is fully protected to all colleagues participating in marketing (Figure 2) on this network. Regularly, this information is stored in an access log that contains "books", manual, manually information about the system, the value of the node, and the configuration data set. Occasionally, the registry is asked to store all network information according to price terms. That is, the given value of each node is the total output factor for processing the node in the network.

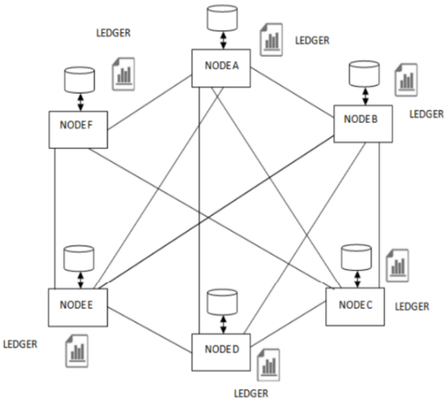

Figure 2: Distributed Ledgers

Also, a distributed ledger is one of the key features of any IoT device, has its own copy and is updated with changes in the IoT network in minutes if not seconds. The Register can be used to make copies with or without the permission of the owner. The type of ladder is critical for determining the location of the IoT and the number of network nodes. It will act as a central server system for that creates trust between network nodes connected to each other. Patented control is used to monitor and control various areas of IoT networks. The API interface provides access to block chain services for IoT applications. The top layer is a hierarchy of an application that helps integrate a variety of IoT applications and perform data view functions that lead to the production of various digital services, and to create appropriate and appropriate solutions based on data obtained from IoT portable devices.

The Internet on the Internet has been changed to Gamechanging technology connecting online types and virtual objects online. This leads to rich power in each of the various fields. The unexpected things have obtained a unique opportunity in many areas. However, IoT deals with various problems that are used as barriers for extensive accommodation of IoT resources. Trust and trust of trust are one of the problems. Currently, the parallel IoT paradigm depends on a third-party body that fully controls the data collection and processing of a variety of IoT objects without explicit constraints on how data obtained is used. As a result, the central power acts as a barrier for IoT users to attract most IoT devices owners. [10].Because blockchain technology creates a decentralized and isolated environment for people. Unlike Inpoint, a centralized model that has multiple disadvantages such as single point of failure, security, trust etc., blockchain uses a partitioning method to increase the processing power of all participating users, increasing efficiency and eliminating single points. failure. Blockchain technology also improves the security and integrity of data due to its intangible and consistent properties [11]. There are several similarities and differences between the Internet of Things and blockchain. Table 1 lists the most understandable elements that IoT can provide through blockchain.

TABLE I
THINGS THAT CAN BE PROVIDED IOT WITH BLOCKCHAIN

Items	IoT	Blockchain
Privacy	Lack of privacy	Ensures the privacy of the participating nodes
Bandwidth	IoT devices have limited bandwidth and resources	High bandwidth consumption
System Structure	Centralized	Decentralized
Scalability	IoT considered to contain a large number of devices	Scales poorly with a large network
Resources	Resource restricted	Resource consuming
Latency	Demands low latency	Block mining is time-consuming
Security	Security is an issue	Has better security

V. PROPOSED WORK:

Proxy re-encryption was first proposed by Blaze et al. [2], which allows the proxy to convert files created with the owner's public key into encryption for the data recipient. Let's say the data owner is the sender and the data user is the messenger. This program allows the messenger to send a temporarily encrypted message to the messenger without revealing the secret key. The sender himself or a trusted third party generates the key, or reset key. The proxy uses the key to reset the encryption text before you use the encryption algorithm to send a new remote encryption to the user. The traditional function of the proxy recovery system is that the agent is fully trusted. In other words, he means that she does not mean the main owner of the data owner. This is considered the main user of trusted encrypted data access, which is an integral part of the data exchange system. Using a proxy encryption system, you can share encrypted data between certified users and maintain confidentiality to illegal users. Data disclosure can be reduced using encryption because the data owner can access the exported data that only the authorized user.

This article uses this scenario to propose to combine proxy encryption with proprietary encryption, information network, and Blockchain technology to improve IoT data sharing. Shamir [3] First, the sender used the e-mail identifier to introduce the concept of identification encryption that the sender encrypted the message to the recipient. This was a very powerful tool used to battle multiple key deployment tasks, and many confidentiality contracts have been able to make many confidentiality agreements such as key encryption to disclose [4], [5], Secret Hand Shake [6]. The selected scenario password. Encryption method for public key protection [7]. Because heavy encryption, encryption, encryption, and key controls are included, encryption for encrypting properties is desirable and this method is not suitable for IoT devices that are detained by the application. Data owner has introduced data owner network exchange ideas that can distribute and provide a unique name of data that can be replicated from Network Storage [12], [13]. This ensures that network data critical to the IoT Ecosystem can be delivered and used efficiently, regardless of how much data is present on a large network. When trust issues arise, Nakamot devised a nationwide distributed distributed system that can accelerate safe and reliable data sharing. [14]. This is a BLOCKCHAIN technology and has a lot of interest due to the ability to support data confidentiality. The development problem occurs, but when you save the mass data size, the system's emerging system application uses the box to control access to database management. The confidentiality of data and user feedback is available using boxes.

In addition to proxy encryption, the proprietary encryption and information networks and blocking functions improve security and confidentiality in the data exchange system. Proxy encryption and proprietary encryption provide the Wellanalyzed Control control access to the data, but because the network archive provides the best data distribution, the data transfer data transmission concept promises appropriate service quality. This box is designed to prevent data from collecting and sharing and preventing security systems between the network organizations. In our article, the data owner deploys the access control device stored in the block. Only authorized users can access your data

VI. CONCLUSION:

Given the various flaws in the central IoT architecture, converting an IoT to distributed ledger technology may be the wisest course of action. One of the most widely distributed ledger technologies is blockchain. It uses the segregation of people to eliminate a one point of failure and increase efficiency. Furthermore, because blockchain technology is based on facts and is consistent, it improves data security and integrity. The use of blockchain and IoT technologies in tandem can help to solve problems with centralised systems and pave the way for future development. The goal of this research was to look at how the Internet of Things and blockchain technology worked together with a simple security model. After introducing each of the goals, the paper demonstrated how to connect the IoT with the blockchain, emphasizing how a proxy blockchain rerouter overcomes IoT challenges. In addition, the latest research on the integration of IoT and blockchain was introduced. Then, we show how various features of blockchain can be used as a comprehensive list of IoT applications in the proposed project, blockchain as an Internet of Things service is being studied.

REFRENCES:

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.

[2] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127–144.

A. Shamir, “Identity-based cryptosystems and signature schemes,” inProc.Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984,pp. 47–53.

[3] Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. Int. J. Intell. Syst. Appl. 2018, 10, 40–48.

[4] Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. IEEE Access 2018, 6, 32979–33001.

[5] Atlam, H.F.; Wills, G.B. Intersections between IoT and distributed ledger. In Advances in Organometallic Chemistry Volume 60; Elsevier BV: Amsterdam, The Netherlands, 2019; pp. 73–113.

[6] Karafiloski, E.; Mishev, A. Blockchain solutions for big data challenges: A literature review. In Proceedings of the IEEE EUROCON 2017—17th International Conference on Smart Technologies, Ohrid, Macedonia, 6–8 July 2017; pp. 763–768.

[7] Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173–190.

[8] Yin, S.; Lu, Y.; Li, Y. Design and implementation of IoT centralized management model with linkage policy. In Proceedings of the Third International Conference on Cyberspace Technology (CCT 2015), Beijing, China, 17–18 October 2015; pp. 5–9.

[9] Atlam, H.F.; Wills, G.B. IoT Security, Privacy, Safety and Ethics. In Intelligent Sensing, Instrumentation and Measurements; Springer Science and Business Media LLC: Berlin, Germany, 2019; pp. 123–149. 14. Atlam, H.F.; Walters, R.J.; Wills, G.B. Internet of Nano Things. In Proceedings of the 2nd International Conference on Cloud and Big Data Computing (ICCBDC 2018), Barcelona, Spain, 3–5 August 2018; pp. 71–77.

[10] Atlam, H.F.; Walters, R.J.; Wills, G.B. Intelligence of Things: Opportunities & Challenges. In Proceedings of the 2018 3rd Cloudification of the Internet of Things (CIoT), Paris, France, 2–4 July 2018; pp. 1–6.

[11] Conoscenti, M.; Vetro, A.; De Martin, J.C. Peer to Peer for Privacy and Decentralization in the Internet of Things. In Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina, 20–28 May 2017; pp. 288–290.

[12] Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog Computing and the Internet of Things: A Review. Big Data Cogn. Comput. 2018, 2, 10.

[13] Atlam, H.F.; Wills, G.B. An efficient security risk estimation technique for Risk-based access control model for IoT. Internet Things 2019, 6, 1–20.

[14] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: https://git.dhimmel. com/bitcoin-whitepaper/ (accessed on 13 October 2020).

[15] Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. 2014. Available online: http://kevinriggen.com/ files/sidechains.pdf (accessed on 13 October 2020).

[16] Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C., & Qiu, T. (2020). A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. Journal of Network and Computer Applications, 167, 102710.

[17] Agyekum, K. O. B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., & Gao, J. (2021). A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. IEEE Systems Journal.

[18] Fan, Q., Chen, J., Deborah, L. J., & Luo, M. (2021). A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. Journal of Systems Architecture, 117, 102112.

[19] Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications, 25(6), 12-18.

[20] Xuan, S., Zhang, Y., Tang, H., Chung, I., Wang, W., & Yang, W. (2019). Hierarchically authorized transactions for massive internet-of-things data sharing based on multilayer blockchain. Applied Sciences, 9(23), 5159.

[21] 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.

[22] Viriyasitavat, W., Da Xu, L., Bi, Z., & Hoonsopon, D. (2019). Blockchain technology for applications in internet of things—mapping from system design perspective. IEEE Internet of Things Journal, 6(5), 8155-8168.