Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Analysis of Information Handling and Security with Block Chain-Based Big Data Management

Megha Jagga[1], Omkar Pandharkame[2], Sarita Agrawal[3], Sidhant Das[4], Mr. Rishi Shikka[5], Dr. Vedantam Seetha Ram[6]

[1]Centre of Research Impact and Outcome, Chitkara University, Rajpura- 140417, Punjab, India megha.jagga.orp@chitkara.edu.in, Orcid Id- https://orcid.org/0009-0003-4292-7576
[2]Director, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashta, India, Email Id- omkar.pandharkame@atlasuniversity.edu.in, Orcid Id- 0009-0002-2050-0304
[3]Associate Professor, Department of Management Studies, Vivekananda Global University, Jaipur, India, Email Id- sarita.agrawal@vgu.ac.in, Orcid Id- 0009-0001-7206-9387
[4]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh-174103, India, Email Id- sidhant.das.orp@chitkara.edu.in, orcid Id- https://orcid.org/0009-0003-3540-5817
[5]Assistant Professor, Department of Electronics, Sanskriti University, Mathura, Uttar Pradesh, India, Email Id- rishisikka.ec@sanskriti.edu.in, Orcid Id- 0000-0002-6954-1951
[6]Associate Professor, Department of Finance, JAIN (Deemed-to-be Univesity), Bangalore, Karnataka, India, Email Id- vedantam_seetharam@cms.ac.in, Orcid Id-0000-0002-6375-1501

Introduction: In the ever-changing world of information technology, businesses need to manage their data effectively. Big data offers benefits as well as challenges, necessitating that businesses and government agencies handle enormous volumes of information with skill. Data manipulation and unauthorized access are two major security problems nowadays.
Objective: To address block-chain's limitations and leveraging on its capabilities, the study takes a comprehensive approach for analyzing information handling and security in the context of block-chain-based big data management.
Method: The paper offers a thorough examination of block-chain's weaknesses and proposes an innovative solution to these issues. The suggested strategy involves creating an innovative paradigm for data storage that makes use of both off-chain and within a chain technology. This concept attempts to effectively address data redundancy and lack storage capacity challenges.
Result: In the paper, the development of a prototype system is described. The features of this system include tracking, modifying, adding and querying employee data. This prototype's implementation validates the viability of using block-chain technology for large data management and information handling analysis. The findings reveal that the proposed method can effectively address the drawbacks of conventional file management and provide a strong way to improve data security and

integrity.
Conclusion: The study emphasizes the way block chain technology has the ability to completely transform information management. The paper presents an enhanced data storage model that offers an acceptable solution. The developed prototype demonstrates the way block chain technology could be used in practice to efficiently manage employee data.

Keywords: Information Handling, Block-chain, Big Data, Data Management,Elliptic Curve cryptography (ECC).

1. Introduction

The paradigm for information management and security that blockchain technology has brought is revolutionary, changing the ways in which data is validated, exchanged and stored. [(1)] Blockchain technology is decentralized, there is no longer need for federal level them, so reducing the likelihood of an individual point of malfunction and strengthening the system is less vulnerable to hostile assaults.[(2)] Beyond its fundamental tenets of immutability and decentralization, blockchain technology uses sophisticated cryptographic methods to safeguard the data contained in its blocks.[(3-4)] The effects of blockchain technology on information handling and security go beyond conventional data storage.[(5)] The goal of the present investigation analysis of information handling and security in the context of block-chain-based big data management is to overcome the limits of block-chain and capitalize on its strengths.

The study [(6)] proposed the scalability and data accessibility of the field of health care and to safely transmit patient data. Reliable data management was offered by proposed BSDMF between clouds servers along with personal computers and between embedded surgical instruments coupled with personal servers. The study [(7)] shown how to employ digital currencies for data validation, keeping records, security of information and data transport along with Internet of Things devices for data collection. The article [(8)] investigated the possible effect of integrating BIM and blockchain in a smart city setting on increasing the sustainability of buildings in the CIM/smart city concept. The paper [(9)] examined a number of blockchain-related research projects using a methodical literature review.

The paper [(10)] used network analysis and bibliometrics to perform a systematic review. They identified the important papers, important authors and collaborative patterns that the earlier publications on that aspect of supply chain management had overlooked. The study [(11)] proposed the rising market perceptions' future objective for integrating block chain technology into business; the study evaluated the application of distributed ledger in the marketing domain and aimed to identify significant elements, streams and problems. The paper [(12)] explained the integration of the block chain mechanism with the conventional pharmaceutical supply chain system. They presented a block-chain-based scheme.

The study [(13)] determined the crucial responsibilities of block-chain-based technologies played in resolving among the most urgent and difficult problems challenges encountering medical professionals, that article undertook a review of the literature. The study [(14)] explained the possible uses for the technology of block-chain in the building sector. The

study [15] suggested that solving those issues with block-chain technology. A plan for integrating block-chain technology into an intelligent logistics system was put out, complete with an authentication method based on consensus, data storage and access mechanism, as well as an operating principle.

2. Methodology

Blockchain-Based Information Handling Architecture

Blockchain-based personnel information management offers a ground-breaking method for improving data security, efficiency and transparency. There are three classifications in blockchain based on their admittance mechanism, Consortium, Private and Public block-chains. The oldest and most popular blockchain is known as the Blockchain Public. The Public Blockchain is decentralized and unregulated by any institution, anybody can participate in it, the Consortium the digital ledger, which is positioned between the Public as well as Private Block-chains, is mainly utilized in sectors of the economy where different user roles coexist, as in banks, governments and businesses.

Architecture of the System Configuration

Virtual ledgers are distributed databases that document each online transaction; the amount of data on it will increase. In addition, each blockchain node synchronizes the entire network data to prevent data manipulation, which results in an increasing quantity of data for an individual node and growing wait times for transaction confirmation, which causes the blockchain network as a whole to become bloated. Since nodes can join the public blockchain at will, Public blockchain development is not possible for it.

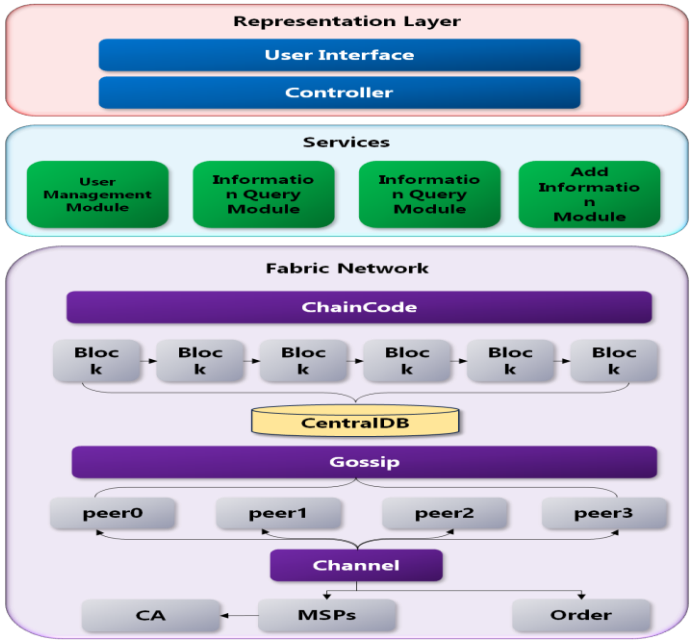

Figure 1. Architecture of the system configuration Data cleaning (Source: Author)

We expand upon and enhance this concept, putting forth an exclusive off-chain and on-chain information structure suitable for the Consortium Block-chain. A significant portion of the relevant data is kept outside of the block-chain in a central database, while the remainder, as much as possible, is saved in the block-chain itself. By tracking and validating the data with preserving the hash produced through the out-of-chain data in the block, this technique can minimize the distributed ledger network's data volume while maintaining the ability to avoid tampering with the out-of-chain data.

In the sector, increasing the block chain's capacity is a major issue. The following concepts are fundamental to the solution. Maintain the current ceiling while obtaining a way around the constraints. Expand directly to a predetermined maximum. Figure 1 displays the architecture of the system. The hyper ledger fabric network, service layer and user view layer are arranged top to bottom. Chain code is utilized to implement these modules. The User Administration Module, Details modules for adding information, changing details and modifying queries are the four functional modules that make up the service layer. Sophisticated contract activities of data kept on the blockchain are implemented using chain code. Transactions execution outcomes are stored in a CouchDB state database.

Handle data that is both off-chain and on-chain

The majority of the data can be separated among two groups, "core" and "non-core." For instance, the primary fields in the data structure of the mechanism for managing personnel information are "name," "identity number," "the editor of the information" and so forth. These data points will be assembled into a block and kept on the network's ledger. The other non-core fields that are left unchecked carry out the Secure Hash Algorithm 256-Bit (SHA256) operation. The block contains the hash value for the non-core information. When the data is removed from the central database, it undergoes SHA256 processing. In the event that the result matches the hash result that was recorded in the chain of blocks, it indicates that there have been no changes to the data. Figure 2 illustrates the data searching method. The distributed ledger network's nodes and the central repository are first searched using the keyword index. To get authentication result B, the data that was obtained from the central repository is hashed. The block chain network's block containing the earlier recorded hash value A is retrieved and contrasted with B. It is evidence that the data has not been altered if they are equal. The steps involved in using the SHA256 algorithm are explained below,

(1) Initialization settings

To obtain 8 prime numbers can be used to generate 8 parameters (2, 3, 5, 7, 11, 13, 17 and 19) in the natural number

$$I_0 = 0x6a09e667; I_1 = 0xbb67ae85;$$

$$I_2 = 0x3c6ef372; I_3 = 0xa54ff53a;$$

$$I_4 = 0x510e527f; I_5 = 0x9b05688c;$$

$$I_6 = 0x1f83d9ab; I_7 = 0x5be0cd19;$$

(2)Get the message list ready X_s

$$Y_u = O_u^{(l)}(0 \le u \le 15)$$

$$Y_u = \sigma_1^{(256)}(Z_{t-2}) + W_{t-7} + \sigma_0^{(256)}(Z_{u-15}) + Z_{u-16}(16 \le u \le 63)$$

(3) Set eight factors to start alongside the intermediary every hash's value algorithm round.

(4) For $0 \le s \le 63$, Execute the compression function

$$U_1 = i + \sum_{1}^{256}(h) + ch(h,g,j) + M_u^{256} + Z_u$$

$$U_2 = i + \sum_{0}^{256}(e) + O_{dk}(t,x,z)$$

$$j = i; i = h; h = x + U_1; x = t; t = c; c = d; d = U_1 + U_2;$$

(5) Compress a block and add it tothe hash value as of right now

$$I_0^{(v)} = z + I_0^{(v-1)}, I_1^{(v)} = r + I_1^{(v-1)}$$

$$I_2^{(v)} = y + I_2^{(v-1)}, I_3^{(v)} = s + I_3^{(v-1)}$$

$$I_4^{(v)} = x + I_4^{(v-1)}, I_5^{(v)} = t + I_5^{(v-1)}$$

$$I_6^{(v)} = w + I_6^{(v-1)}, I_7^{(v)} = u + I_7^{(v-1)}$$

Standard X.509 certificates serve as the foundation for fabric membership and the (ECDSA) Digital Signature Algorithm using Elliptic Curve key combines an algorithm for Digital signatures (DSA) and (ECC) Cryptography using Elliptic Curve. The intractability of the ECDLP Discrete Logarithm Problem with an Elliptic Curve is the foundation for the elliptic curve cryptosystem's security.

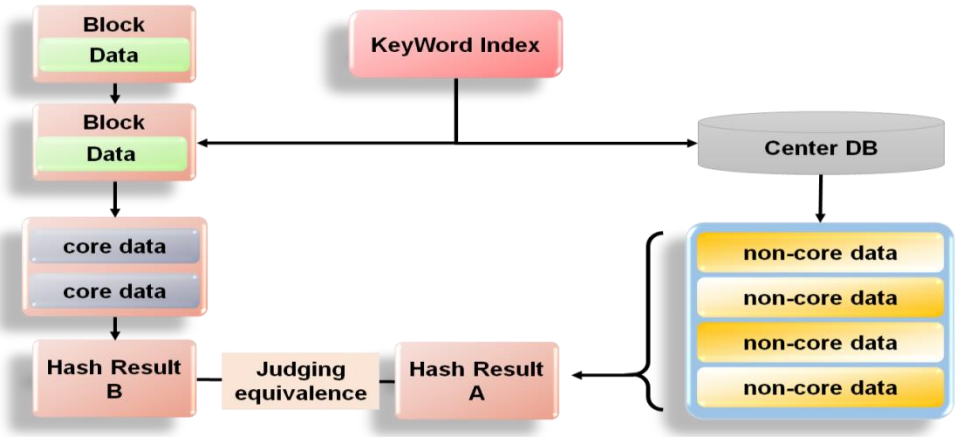

Figure 2. The method of doing a query over the divided stored data (Source: Author)

The Gossip protocol is limited to nodes in the channel that have the same Managed Service Provider (MSP).

The procedure for signing is as follows:

- Choose a base point A and an elliptic curve $Ft(x, y)$.
- Using the base point A, get the public key $N = vg$ by selecting the private key N ($v <$ n, where n is the order of (A).
- Determine the location $S = w A$ by creating a random number, w ($w < n$).
- Computing Hash = SHA1 (original data, a, b), where the coordinate values of the point S and the original data are used as arguments.
- Determine the document-required $Z \equiv s{-}Hash{*}k(\text{mod } n)$;
- The values for the signature are sand z. If either r or s is zero, repeat step 3

Verification process

- The receiver carries out the following actions upon obtaining the signature value and the message (m) (s, z).
- Determine that $zA + I(m) Q = (a1, b1), s1 \equiv a1 \text{ mod } q$.
- Equation of verification $s1 \equiv s \text{ mod } q$
- Accept the signature if the equation holds true; if not, it is invalid.

Chain Code and Data Structures

Following data entry, the administrator has the option to verify specific fields, like the central domain. Editor Time, which is a date and time used to store the most recent specifics as well as editor, which is the administrator in charge of the system, are two fields that can be used to verify that the data has changed. Data histories act as a data trace back by documenting any modifications to the data. Only when a transaction is endorsed in line with the endorsement tactics is it considered legitimate. The associate is guided in determining if the transaction has been approved by using the endorsement technique. As part of the transaction validation process, a peer that receives to determine if a transaction is legitimate, it queries the (VSCC) Chain code for Verification System connected to the transaction's Chain code. Figure 3 shows the structure of the Redundant Byzantine Fault Tolerance (RBFT). Sending 2+ 1 to a node in the network suffices as a request; sending a message to every node is not necessary. The node will spread the message to other nodes so they are aware of the request message after it receives it from the client. Following receipt of the request by each primary node, the node will have sufficient information to accept the plan that issue a message of commit after receiving the PREPARE messages and the PRE-PREPARE message. 2+1 sorting and adding commit messages to the ledger is possible.

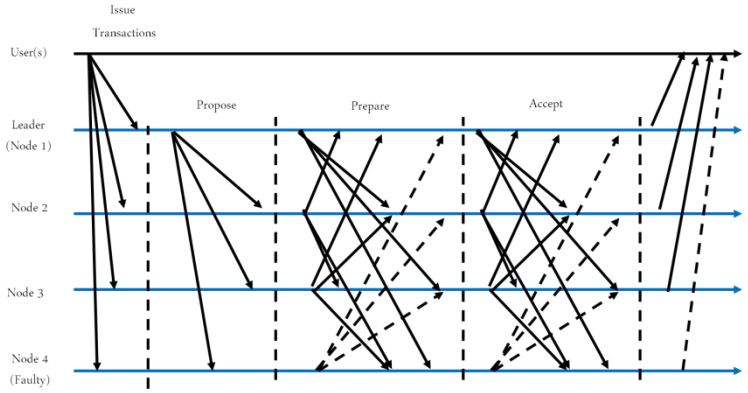

Figure 3. Redundant Byzantine Fault Tolerance structure (Source: Author)

3. Analysis and Outcomes Of The Research

To confirm that our suggested strategy of dividing and keeping information is in fact suitable for large-scale handling of data platforms, such as PIM, we created a prototype apparatus built on the hyper ledger fabric. The system employs a My SQL Ver. 8.0 simulation central database and it is powered by a Core (TM) Intel(R) it470HQ CPU @ 2.50 GHz processor, 6 GB RAM and an Ubuntu 17.04 (64-bit) virtual machine.

The response time for adding data is depicted in Figure 4 as the volume of data on the block chain grows. It is evident that cutting back on data can shorten storage response times. Because unique saved information must store data in the local system and the digital ledger, respectively, in situations where there is minimal data, its reaction time will be longer than if it weren't separated storage. This indicates that storing all of the data in the block chain network. Node data transfer and consensus verification are not necessary when using a local database to store data. The benefits of independent storage become more apparent as data volumes rise.

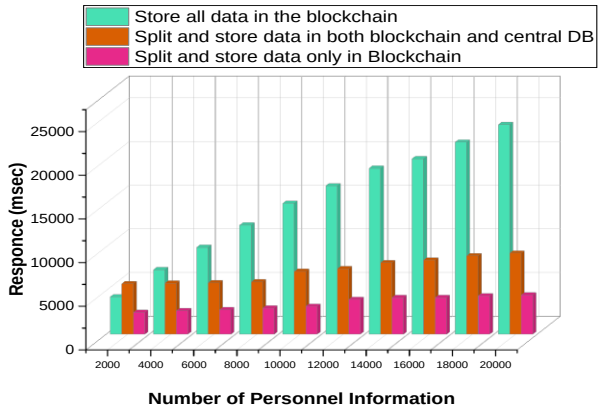

Figure 4. The response time of the data quantity on chain and the storage data's connection (Source: Author)

Figure 5 illustrates how query response times vary with data volume. Similar to storage, query time can be decreased by minimizing the amount of data. A comparison and performance analysis of the two approaches storing data on/off-chain and storing all data in block-chain is shown in Figure 6. Figures 4 and 5 show unique information retention performs better on writes and reads than non-separated archiving of data in application scenarios like managing staff data, which requires storing a lot of data. This approach strikes a balance between cutting-edge and antiquated technologies, while it is not as safe as data storage on a distributed ledger.

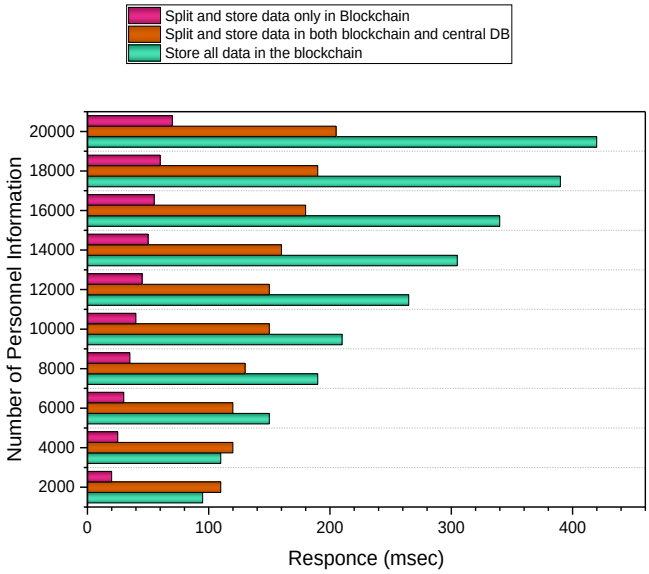

Figure 5. The Connection between the Quantity of Data on the Chain and the Storage Data Response Time (Source: Author)

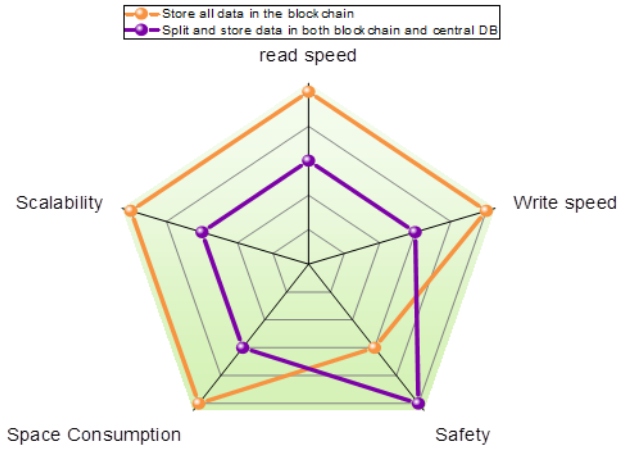

Figure 6. Comparison of the two methods' respective performances (Source: Author)

Given that the digital ledger system houses almost all the data, even though some of it is

kept in a regional database, overall protection is more elevated because, in accordance with the process that we created, the data is hashed and kept on file in the blockchain.

4. Conclusion

The study highlights how information management could undergo a radical change due to block chain technology. In the context of block chain-based big data management, the study analyses data manipulation and security in a thorough manner. An appropriate solution is provided by the improved data storage model that is presented in this research. The created prototype shows how block chain technology can be applied to manage employee data in real-world settings. As block chain technology gains traction globally, attempts are made to incorporate it into a variety of business, including identity management, logistics and healthcare. As a result, our understanding of information management and security has changed, bringing in a new era of efficiency, openness and trust. Since the block chain is limited by internal bottlenecks like finite data capacity, it is not extensively employed. The technology is in its initial stages of verification and lacks large-scale application scenarios, particularly in the big data industry. The potential of block chain technology to transform information security is a significant factor influencing the direction of the digital world, despite on-going obstacles and regulatory concerns.

References

1. Demirkan S, Demirkan I, McKee A. Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics. 2020 Apr 2;7(2):189-208. https://doi.org/10.1080 /232 70012.2020.1731721.
2. Cali U, Fifield A. Towards the decentralized revolution in energy systems using blockchain technology. Int. J. Smart Grid Clean Energy. 2019 May;8(3):245-56.https://doi.org/10.12720/sgce.8.3.245-256.
3. Le Nguyen B, Lydia EL, Elhoseny M, Pustokhina I, Pustokhin DA, Selim MM, et al. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Computers, Materials & Continua. 2020 Jan 1;65(1):87-107. Computers, Materials & Continua, 65(1), pp.87-107.https://doi. org/10.32604/cmc.2020.011599.
4. Krishnan A. Blockchain empowers social resistance and terrorism through decentralized autonomous organizations. Journal of Strategic Security. 2020 Jan 1; 13(1):41-58. https://doi.org/10.5038/1944-0472.13.1.1743.
5. Al-Zaqeba M, Jarah B, Ineizeh N, Almatarneh Z, Jarrah MA. The effect of management accounting and blockchain technology characteristics on supply chains efficiency. Uncertain Supply Chain Management. 2022;10(3):973-82. http://dx.doi.org/10.5267/j.uscm.2022.2.016.
6. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing. 2021 Jun 19:1-4.https://doi.org/10.1007/s007729-021-015259.
7. Dey K, Shekhawat U. Blockchain for sustainable e-agriculture: Literature review, architecture for data management, and implications. Journal of Cleaner Production. 2021 Sep

20; 316:128254. https:// doi.org /10.1016/j.jclepro.2021.128254.

8. Liu Z, Chi Z, Osmani M, Demian P. Blockchain and building information management (BIM) for sustainable building development within the context of smart cities. Sustainability. 2021 Feb 16;13(4):2090. https://doi.org/10.3390/su13042090.
9. Upadhyay N. Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management. 2020 Oct 1; 54:102120.https://doi.org/ 10.1016/ j.ijinfomgt5.2020.102120.
10. Khan AA, Laghari AA, Gadekallu TR, Shaikh ZA, Javed AR, Rashid M, et al. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Computers and Electrical Engineering. 2022 Sep 1; 102:108234.https://doi.org/10.1016/j.compeleceng.2022.108234.
11. Jain D, Dash MK, Kumar A, Luthra S. How is blockchain used in marketing: a review and research agenda. International Journal of Information Management Data Insights. 2021 Nov 1;1(2): 100044. https:// doi.org/10.1016/j.jjimei.2021.100044.
12. Dwivedi SK, Amin R, Vollala S. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. Journal of Information Security and Applications. 2020 Oct 1; 54:102554.https://doi.org/10.1016/j.jisa.2020.102554 102554.
13. Attaran M. Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management. 2022 Jan 2;15(1):70-83. https://doi.org/10.1080/20479700.2020.1843887.
14. Kim K, Lee G, Kim S. A study on the application of blockchain technology in the construction industry. KSCE Journal of Civil Engineering. 2020 Sep; 24(9):2561-71.https://doi.org/10.1007/s12205-020-0188x.
15. Fu Y, Zhu J. Operation mechanisms for intelligent logistics system: a blockchain perspective. IEEE Access. 2019 Oct 2; 7:144202-13. https://doi.org/10.1109/ACCESS.2019.2945078.