International Journal of Basic and Applied Sciences, 14 (SI-1) (2025) 332-337

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/a53ajt05
Research paper

Blockchain Technology in Scientific Data Management: Security and Efficiency Perspectives

K. N. Raja Praveen [1] *, Deepak Bhanot [2], Amritpal Sidhu [3], Dr. Trapty Agarwal [4], Dr. Shashikant Patil [5], Sanjay Kumar Jena [6], Dr.L. Lakshmanan [7]

[1] Assistant Professor, Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Ramnagar District, Karnataka, India
[2] Center of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India
[3] Chitkara Center for Research and Development, Chitkara University, Himachal Pradesh, India
[4] Associate Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India
[5] Professor, uGDX, ATLAS SkillTech University, Mumbai, India
[6] Assistant Professor, Department of Computer Science and Engineering, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India
[7] Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India
**Corresponding author E-mail: p.raja@Jainuniversity.ac.in*

Received: May 2, 2025, Accepted: May 31, 2025, Published: October 31, 2025

Abstract

Blockchain is a decentralized architectural model that creates an immutable ledger in a distributed manner for recording all transactions. Typically, blockchain is a protected and decentralized data store where all the records are positioned in order, as well as events called blocks. All types of data that are apparent to the nodes are recorded in the blockchain-driven system. Meanwhile, it is the apparent, distributed, and open ledger that effectively records every transaction between two parties in an enduring and verifiable way. Once the information is stored, the information present in the blockchain does not get changed unless a record is inserted. In cryptocurrencies, each user has a precise ledger in the network domain, ensuring the complete agreement of users or nodes in the blockchain currencies. The characteristics of blockchain, including transparency, security, and immutability, facilitate the recording and verification of transactions, rendering it appropriate for secure document management, identity verification, maintaining record integrity, and obviating the necessity for third-party intermediaries in transaction verification. The blockchain-based access control technique was devised to enhance security. Consequently, the access control management system stipulates that the total characteristics must be inferior to the number of users.

Keywords: *Blockchain; Data Management; Security and Efficiency.*

1. Introduction

The advent of new technologies, like the Internet of Things (IoT) and wearable devices, offers healthcare professionals both significant opportunities and substantial challenges [3]. The interconnection of smart devices generates a wealth of data related to our health and well-being [7]. It might even play your favorite tunes to lift your spirits and prepare a meal if you've ordered one. Experts believe that in the coming years, we'll see significant changes in how our living spaces are designed, proving that IoT is more than just a trendy term. The Internet is gradually taking over many real-world applications [2].

Copyright © K. N. Raja Praveen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

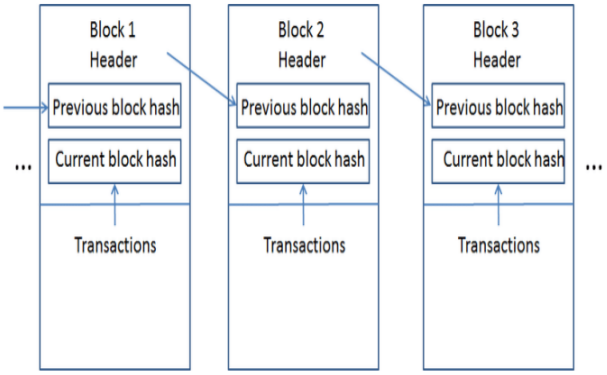


Fig. 1: Blockchain Transactions.

The goal of an optimal architecture should be to create a solution that makes system and application integration easier [5] [15]. Several basic IoT specifications are unique to IoT devices and their enabling environments, such as specific requirements that stem from the compact size and limited resources of these devices [11]. For instance, many specifications arise from the constraints of form factors and resources available to IoT devices. Other specifications come from how these devices are manufactured and used [4]. The approaches resemble traditional digital product concepts more than current Internet applications [9]. It's essential to understand and consider a collection of standard best practices for server-side and Internet connectivity. Below are some key criteria for which various categories are necessary [12]. In the context of blockchain platforms, Ethereum provides an open-source, decentralized environment that allows for customizable smart contracts but faces scalability issues and higher energy consumption [17] [20]. In contrast, Hyperledger is designed for enterprise-level blockchain solutions with a more focused use case and superior scalability but may lack the decentralization that Ethereum offers [18] [21]. The selection between these platforms frequently hinges on application requirements, with Ethereum chosen for public decentralized networks and Hyperledger favored for private, permissioned systems. Cryptographic techniques, like homomorphic encryption and zero-knowledge proofs, are essential for safeguarding data while maintaining anonymity. Homomorphic encryption facilitates computations on encrypted data, but zero-knowledge proofs guarantee data integrity without disclosing sensitive information. These methods have varying trade-offs in terms of computational efficiency and scalability, as demonstrated by Tariq (2024) and Huang (2024).

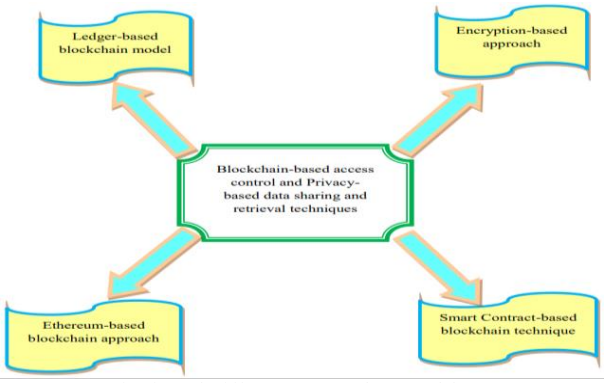


Fig. 2: Categorization of Different Approaches Used for Access Control.

2. Materials and Methods

This can include wearable low-powered IoT devices like smartwatches and mobile phones, or even electric vehicles that are connected to the Internet, which we generally refer to as IoT. In this thesis, we explore two use cases of mobile IoT: one involves individuals wearing smart devices to track various parameters within a specific geographic area, while the other focuses on IoT that operates without limits [6]. The first scenario is less complex due to its limited mobility, whereas the second presents more challenges because of its high mobility, making it the primary focus of our work [1]. With the rising number of vehicles on the road, the need for efficient transport networks has significantly increased. The growing urban population has made traffic management more challenging, complicating efforts to address serious traffic issues. Moreover, factors like road conditions, traffic congestion, and inadequate public transportation are all critical challenges that need to be addressed. Cities adopting a smart city approach will also require traffic control systems to assist municipal administrations and support new car ownership initiatives [13].

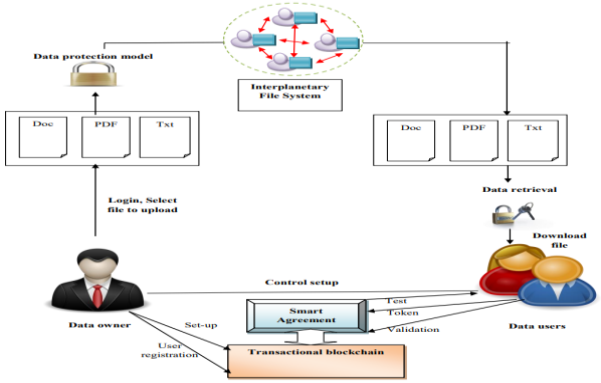


Fig. 3: Blockchain IoT Interactions.

As a result, smart services will only come to life through innovative technological solutions, making their importance vital for both road authorities and driver satisfaction. Historically, transportation management systems have relied on Vehicular Ad-hoc Networks (VANETs) to provide various applications and services. The abundance of data and improved connectivity provided by the Internet of Things (IoT) render this IoT method increasingly pertinent [8].

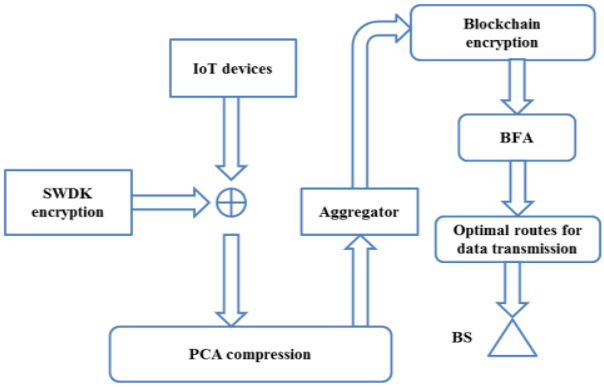


Fig. 4: Proposed System Model.

The physical layer remains consistent with the OSI definition, which is crucial for the standard model to keep up with all the technological advancements in the reference model [14]. The top layer is where all the different applications in the networking stack come together. The linking layer deserves special attention to tackle the diversity in networking architectures that we often see in the IoT landscape. While there are some variations, most networks typically rely on standard connectivity schemes and protection solutions [10]. This layer needs to embrace diversity to ensure IoT systems can achieve full interoperability and support for various architectures, along with strong protection measures. At the same time, it should provide standard interfaces for the upper layers, functioning similarly to the corresponding OSI stack [16]. Additionally, this layer must incorporate a standard connectivity model that accommodates all potential networking solutions, enabling global manageability, interoperability, and scalability.

3. Results and Discussion

A network consisting of 50x50 sensor nodes has been created and assessed using the user-friendly software MATLAB. We employed SWDK to formulate a multifaceted security protocol, with compression methodologies and a blockchain-based storage system that integrates homomorphic encryption [19] [22]. Furthermore, we assessed the expenses related to storage, transmission, network efficiency, and the validation of individual texts. Figure 5 illustrates the storage costs associated with the proposed transmission method.

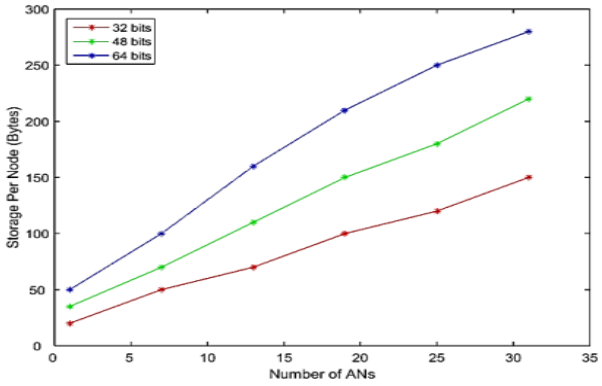


Fig. 5: Storage Costs vs. Access Nodes.

The study involves the selection of security key sizes of 32, 48, and 64 bits. In assessing the outcomes, we also adjust the selection of Access Nodes (ANs). To calculate the storage cost, we multiply the number of keys by the SWDK key size. The graph below demonstrates that an increase in key size correlates with a substantial increase in storage costs.

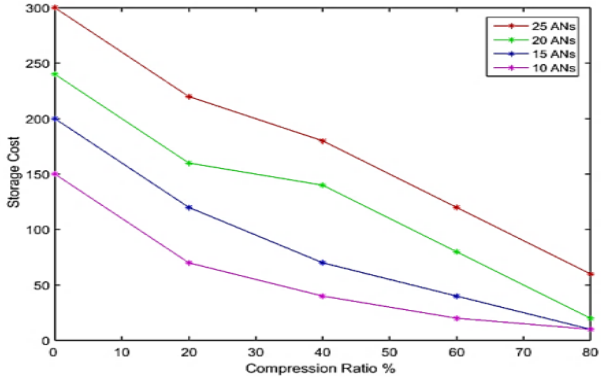


Fig. 6: Compression Ratio vs. Storage Cost - Various Ans.

Fig. 6: This figure illustrates the trade-off between compression ratio and storage cost in IoT networks. Increasing the compression ratio reduces storage costs but can negatively impact data retrieval times, which are critical in real-time IoT applications.
While larger key sizes can complicate things for attackers trying to breach the node, it's always a good idea to opt for these bigger keys, even if they come with a higher storage cost. The image illustrates that an augmentation of Access Nodes (ANs) in the network leads to increased storage expenses. The proposed method incorporates security measures at two separate stages, and the use of security keys during data transfers further escalates costs.

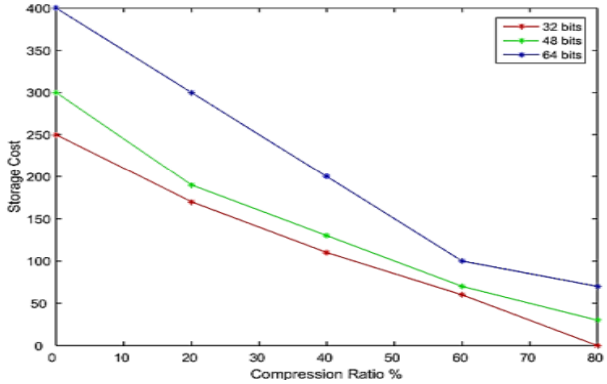


Fig. 7: Compression Ratio vs. Storage Cost - Various Key Sizes.

Fig. 7: This graphic illustrates the effect of enlarging the encryption key size on both storage expenses and security levels. Increased key sizes enhance security by complicating unauthorized access, while they incur greater storage and processing expenses. These trade-offs are essential for establishing the ideal configuration in IoT contexts, where security and storage efficiency are paramount.
To implement the data sharing procedure on the cloud platform, only authorised users must have access to the cloud data. When the data owner needs to share their data with a certain group, they send the encryption key to each group member. Furthermore, any member of the group can obtain the encrypted material from the cloud, after which decryption is performed using the key. Therefore, the group member requires no intervention from the data owner.

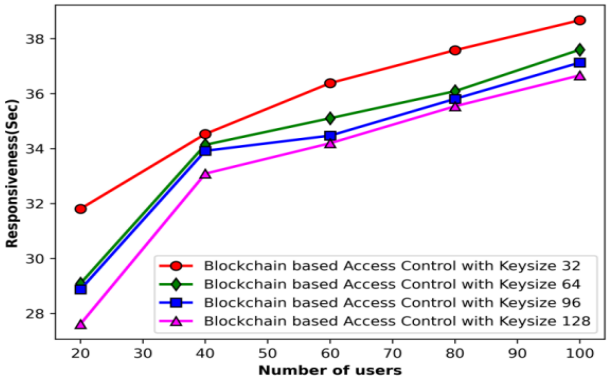


Fig. 8: Performance Analysis of Responsiveness with Blockchain Size 100.

The data is transmitted by converting the original data into privacy-secured data to enable a safe transmission method. Furthermore, the approach employed privacy and utility parameters to regulate the essential data. Upon request for encrypted data stored on the cloud platform, the Cloud Service Provider evaluates the availability of the requested data in storage and its compliance with the defined index terms using a data retrieval mechanism. In data retrieval, the original data is recovered from secure sources.
We examine the security and efficiency trade-offs of Ethereum and Hyperledger to improve the comparison of blockchain platforms. Ethereum, a decentralized public blockchain, encounters scalability challenges attributed to its proof-of-work consensus mechanism, which

is energy-consuming and restricts transaction capacity. Conversely, Hyperledger, a permissioned blockchain, provides expedited transaction processing with reduced energy usage, rendering it more appropriate for enterprise applications. Homomorphic encryption facilitates computations on encrypted data while preserving privacy, and zero-knowledge proofs provide rapid validation without disclosing sensitive information. As highlighted by Huang (2024) and Tariq (2024), these trade-offs are critical when evaluating blockchain for IoT applications, where privacy, scalability, and efficiency are paramount.

Despite its potential, blockchain faces several challenges when applied to IoT. A primary limitation is scalability. Contemporary blockchain platforms face challenges in managing the substantial data volume produced by IoT devices, leading to heightened latency and transaction expenses. The energy consumption linked to blockchain networks, especially those utilizing proof-of-work consensus, is a challenge for low-powered IoT devices. These constraints pose significant challenges for the feasibility of the proposed framework, especially in resource-limited IoT environments that require energy-efficient and scalable solutions.

4. Conclusion

This model is specifically crafted for IoT applications. Before diving into the development of this blockchain security model, we introduce the "Lightweight Security Framework for IoT-Enabled Tracking of COVID-19 and its Variants" as part of the first framework. During a global pandemic like COVID-19, when travel is rampant, safeguarding human health becomes paramount. A substantial effort has been made to improve healthcare and monitoring via IoT devices. Nonetheless, the present capabilities of these devices are inadequate for countering significant security concerns. This deficiency arises from the constrained resources of IoT devices, the absence of stringent standards, and weaknesses in hardware and software design. Blockchain technology is proposed to tackle these difficulties by ensuring safety while enabling billions of IoT devices to deliver secure, transparent, and efficient health assistance to patients and healthcare professionals. Unlocking the complete potential of the IoT revolution might profoundly impact numerous sectors of society and the economy. The proposed framework delineates a blockchain-based IoT architecture that considers the resource constraints of various IoT devices while addressing critical privacy and security issues. The paradigm, although demonstrated in the realm of remote health monitoring and tracking, is relevant to other IoT configurations within multi-tiered networks. Future research should address the scalability issues inherent in blockchain networks, particularly for large-scale IoT systems. Key areas for exploration include the development of lightweight blockchain protocols that are optimized for IoT environments with limited computational resources. Additionally, integrating blockchain with artificial intelligence (AI) could enable enhanced decision-making capabilities in healthcare IoT applications, such as predictive health monitoring and secure patient data management. These developments will address existing deficiencies in blockchain technologies and facilitate the development of more efficient, secure, and scalable IoT solutions.

References

[1] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering, 30*(7), 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227.

[2] Iskamto, D., &Juariyah, L. (2023). Blockchain technology challenge in the future: Data security and efficiency. *International Journal of Law, Policy, and Governance, 2*(2), 65–76. https://doi.org/10.54099/ijlpg.v2i2.708.

[3] Huang, J. (2024). Impact of non-performing corporate assets on shareholder's equity and return on the application of AI and blockchain technologies. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(3), 412–423. https://doi.org/10.58346/JOWUA.2024.I3.027.

[4] Paik, H.-Y., Xu, X., Bandara, H. D., Lee, S. U., & Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance. *IEEE Access, 7*, 186091–186107. https://doi.org/10.1109/ACCESS.2019.2961404.

[5] Im, A., Rahmadika, S., Lee, Y. H., Kim, B., & You, I. (2022). A note on enactment of blockchain for HACCP-based cooperative model. *Journal of Internet Services and Information Security, 12*(1), 44–56.

[6] Zheng, X., Zhu, Y., & Si, X. (2019). A survey on challenges and progresses in blockchain technologies: A performance and security perspective. *Applied Sciences, 9*(22), 4731. https://doi.org/10.3390/app9224731.

[7] Krishnan, H., Santhosh, Vijay, & Yasmin, S. (2022). Blockchain for health data management. *International Academic Journal of Science and Engineering, 9*(2), 23–27. https://doi.org/10.9756/IAJSE/V9I2/IAJSE0910.

[8] Singh, S., Sharma, S. K., Mehrotra, P., Bhatt, P., &Kaurav, M. (2022). Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives. *Materials Today: Proceedings, 62*, 5042–5046. https://doi.org/10.1016/j.matpr.2022.04.998.

[9] Kong, Y., Suntrayuth, S., & Lin, F. (2024). Construction of cross-border e-commerce supply chain of agricultural food products based on blockchain technology. *Natural and Engineering Sciences, 9*(2), 145–163. https://doi.org/10.28978/nesciences.1569226.

[10] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., &Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography, 3*(1), 3. https://doi.org/10.3390/cryptography3010003.

[11] Akila, A., Nandhini, S., Pavithra, M., Suman, K., &Madhorubagan, E. (2023). Enhancing data storage security using blockchain technique in cloud computing. *International Journal of Advances in Engineering and Emerging Technology, 14*(1), 77–86.

[12] Kurkin, A. V., Giraev, A. V., &Medzhidov, Z. U. (2021). Corporate database management on the basis of cloud technologies, blockchain technologies and technologies of big data processing: Effectiveness and security. In *State and corporate management of region's development in the conditions of the digital economy* (pp. 79–83). https://doi.org/10.1007/978-3-030-46394-6_14.

[13] Ganesan, E., Agarwal, T., Sidhu, J., Goyal, S., Deepak, S., MR, E. J., & Sahu, P. K. (2025). Improving Security in 5G and Next-Generation Networks Through Blockchain Integration. *National Journal of Antennas and Propagation*, *7*(2), 44-50. https://doi.org/10.31838/NJAP/07.02.09.

[14] Uvarajan, K. P. (2025). Machine Learning-Based EEG Analysis for Early Detection of Alzheimer's Disease in Aging Populations. *Frontiers in Life Sciences Research*, 38-43.

[15] Sindhu, S. (2025). Mathematical Analysis of Vibration Attenuation in Smart Structures Using Piezoelectric Layers. *Journal of Applied Mathematical Models in Engineering*, 26-32.

[16] Salabi, L., & Mdodo, K. L. (2023). Food Safety Challenges in Informal Markets: A Microbiological Assessment of Fresh Produce. *National Journal of Food Security and Nutritional Innovation*, *1*(1), 25-32.

[17] Cao, H., He, H., & Tian, J. (2022). A scientific research information system via intelligent blockchain technology for the applications in university management. *Mobile information systems*, *2022*(1), 7512692. https://doi.org/10.1155/2022/7512692.

[18] Tariq, M. U. (2024). Revolutionizing health data management with blockchain technology: Enhancing security and efficiency in a digital era. In *Emerging technologies for health literacy and medical practice* (pp. 153–175). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-1214-8.ch008.

[19] Deepa, N., Pham, Q.-V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., Maddikunta, P. K. R., Fang, F., & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Generation Computer Systems, 131*, 209–226. https://doi.org/10.1016/j.future.2022.01.017.

[20] Vo, H. T., Kundu, A., &Mohania, M. K. (2018). Research directions in blockchain data management and analytics. In *Proceedings of the International Conference on Extending Database Technology (EDBT)* (pp. 445–448).
[21] Huang, S., Wang, G., Yan, Y., & Fang, X. (2020). Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems*, *54*, 361-371. https://doi.org/10.1016/j.jmsy.2020.01.009.
[22] Kishnani, U., Madabhushi, S., & Das, S. (2023, July). Blockchain in oil and gas supply chain: a literature review from user security and privacy perspective. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 296-309). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-38530-8_24.
[23] Rocha, G. D. S. R., Mühl, D. D., Chingamba, H. A., de Oliveira, L., & Talamini, E. (2023). Blockchain, Quo Vadis? Recent Changes in Perspectives on the Application of Technology in Agribusiness. *Future internet*, *15*(1), 38. https://doi.org/10.3390/fi15010038.
[24] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and ubiquitous computing*, *28*(1), 59-72. https://doi.org/10.1007/s00779-021-01583-8.
[25] Liu, Y., Peng, S., Zhang, M., Shi, S., & Fu, J. (2024). Towards secure and efficient integration of blockchain and 6G networks. *Plos one*, *19*(4), e0302052. https://doi.org/10.1371/journal.pone.0302052.
[26] Iliev, K. (2022). Philosophical views on the procedure for regulating the norms of Blockchain technologies in the context of future prospects for the development of the meta-universe. *Futurity Philosophy*, *1*(1), 30-41. https://doi.org/10.57125/FP.2022.03.30.03.