Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 3, pp. 1522–1528, DOI 10.12694/scpe.v26i3.4364

INFORMATION DATA FLOW VERIFICATION MODEL BASED ON BLOCKCHAIN TECHNOLOGY

YINGXIONG NONG[*], CONG HUANG[†], YING LU[‡], ZHIBIN CHEN[§], AND ZHENYU YANG[¶]

Abstract. In the wave of digital transformation, the secure flow of information and data and authenticity verification have become vital challenges. This paper proposes an innovative information data flow verification model based on blockchain technology to build an efficient, transparent and immutable data flow environment. The model uses the distributed ledger characteristics of blockchain to guarantee the integrity of data and introduces advanced identity management mechanisms and trust management algorithms to enhance security and trust in the data flow process. This paper then uses an improved consensus algorithm, combined with innovative contract technology, to ensure the legitimacy and traceability of each data transaction. Through digital signature and public critical infrastructure (PKI), the identity management module realizes accurate authentication of user identity and privacy protection. The trust management algorithm dynamically evaluates the credit rating of both sides of the transaction based on historical transaction records and user behavior pattern analysis, providing additional security for data flow. The model simulation results show its excellent performance in practical application scenarios. Via the experimentation involving the circulation assessment of ten thousand units of informational data, the mean validation duration for the framework stands at twenty-five milliseconds, whilst the precision of datum integrity scrutiny attains a commendable 99.9%, markedly amplifying the celerity and steadfastness of informational dissemination. Moreover, the architecture manifested commendable fortitude against nefarious onslaughts, effectively thwarting in excess of 95% endeavors aimed at injecting counterfeit data, thereby substantiating its resilience within intricate networking milieus.

Key words: Blockchain technology; Information data flow; Identity management; Trust management algorithm.

1. Introduction.

In the epoch of digital transformation, the dissemination of information and data assumes paramount significance across myriad sectors. Ensuring data veracity and security has emerged as a paramount concern, spanning financial dealings to logistics oversight, from the exchange of medical records to the conveyance of educational content. Nonetheless, conventional data circulation grapples with myriad hurdles, encompassing data manipulation, identity misrepresentation, dearth of credibility, amongst other impediments, undermining the reliability of data and imposing significant barriers to the expeditious flow of information. In recent times, the ascendance of blockchain technology has proffered novel perspectives to mitigate these challenges. Its decentralized ledger, cryptographic safeguards, and consensus protocols have ushered in a transformative shift, bolstering the security and transparency of information and data dissemination.

Literature [1] proposes a decentralized data storage scheme based on blockchain, which realizes encrypted storage and sharing of information through distributed networks and solves the problem that data in centralized storage is easily tampered with and controlled. Literature [2] further discusses the application of blockchain technology in identity authentication and privacy protection and realizes efficient authentication of user identity and precise control of data access rights through smart contracts and digital signature technology. Literature [3] focuses on constructing trust mechanisms and proposes a trust evaluation model based on historical transaction records and user behavior analysis, which provides quantitative indicators for trust management in data flow. Literature [4] verified the role of blockchain technology in improving data flow efficiency and reducing transaction costs through system simulation and demonstrated its potential in large-scale data management scenarios. However, most of the existing researches focus on the single application or theoretical discussion of blockchain

[*] Information Center of China Tobacco Guangxi Industrial Co., LTD, Nanning 530000, China

[†] Information Center of China Tobacco Guangxi Industrial Co., LTD, Nanning 530000, China (Corresponding author, gxzyhcc@163.com)

[‡] Information Center of China Tobacco Guangxi Industrial Co., LTD, Nanning 530000, China

[§] Information Center of China Tobacco Guangxi Industrial Co., LTD, Nanning 530000, China

[¶] Information Center of China Tobacco Guangxi Industrial Co., LTD, Nanning 530000, China

technology and lacks in-depth exploration of complex, comprehensive issues such as identity management, trust assessment and data verification in information and data flow, especially in how to build an efficient and secure data flow framework. In addition, improving the efficiency of data flow and user experience while ensuring data security is also a challenge to be solved in the current research.

This paper aims to construct a verifier model of information data flow based on blockchain technology, which aims to solve the comprehensive problems of identity verification, trust evaluation and data verification in information data flow [5]. First, this paper combines the consensus mechanism of blockchain and innovative contract technology to design a set of efficient data flow algorithms to realize the automation and intelligence of data transactions while ensuring data integrity. Then, digital signature and public critical infrastructure (PKI) are introduced to establish an accurate authentication mechanism for user identity and ensure user privacy in data flow. Secondly, based on historical transaction records and user behavior analysis, a dynamic trust evaluation algorithm is developed to provide a scientific basis for trust management in data flow [6]. Finally, a model simulation environment is constructed to simulate the information and data flow process and evaluate the performance and security of the system, including key indicators such as data verification speed, transaction success rate and anti-attack ability.

2. Blockchain architecture and algorithm design.

2.1. Blockchain architecture.

Today's academic research reveals that only collaborative networks at the IaaS level can achieve unbounded computing power and storage space expansion at minimal cost. However, IaaS cloud collaboration networks are still in their infancy and face many challenges, such as interoperability barriers, security vulnerabilities, and building trust architectures [7]. The first challenge of authentication is to build an authentication mechanism among heterogeneous cloud service providers (CSPs) to facilitate the formation of alliances. Current strategies tend to adopt federated identity technology to achieve identity authentication and permission management across cloud consortia. However, the existing alliance architecture is tailored for a static environment, which preassumes that parties must reach a commercial consensus in advance, creating a host of security, privacy, and interoperability challenges [8]. The trust framework proposed in this paper aims to break down these barriers and help build a robust IaaS cloud collaboration network.

In IaaS cloud collaboration networks, CSPS benefits from sharing virtual resources with alliance partners. In this scenario, participants may be CSPs exchanging virtual resources within the alliance or regular cloud service users. The external CSP is responsible for providing virtual resources to other CSPS or regular users in the federation [9]. The trust bond between CSPs in the IaaS collaboration network is maintained by the Trust Management Platform (TMP). The platform cleverly blends blockchain networks with innovative trust models [10]. The TMP is designed to scale automatically to accommodate the dynamic addition of new CSPs to the IaaS collaboration network. Figure 2.1 vividly depicts the authentication process when one CSP acquires a virtual resource from another CSP in the federation.

2.2. Algorithm Design.

The blockchain acts as a public shared ledger, recording the transactions of all interactions between CSPs (Figure 2.2) [11]. Such transactions are designed to generate and save credentials that verify the user's identity for use by external CSPs, ensuring that the user has access to protected resources [12]. The credentials (TKN) contain user identification information and permissions associated with the account, which are generated by the creator and passed to the recipient. Each voucher corresponds to a single transaction and is structured as follows:

$$S = (SID \,\|M_{\text{in}} \,\| \,U_{\text{in}} \,\|\|\|M_{\text{out}} \;\|U_{\text{out}} \,\|) \tag{2.1}$$

Here, SID represents transaction identifiers, N_{in} and M_{out} represent the number of existing transaction inputs and outputs, respectively. Certificates are stored in a time series [13]. In the Trust Management Platform (TMP) and CSPs, addresses, digital keys, and signatures ensure the identification and authenticity of CSPs and credentials.

2.2.1. Consensus Mechanism.

CSPs verify transactions in the network, and are responsible for maintaining the ledger's integrity. Transactions carrying vouchers are not added directly to the blockchain but are integrated into transaction blocks designed to increase efficiency [14]. This reduces the time consumption

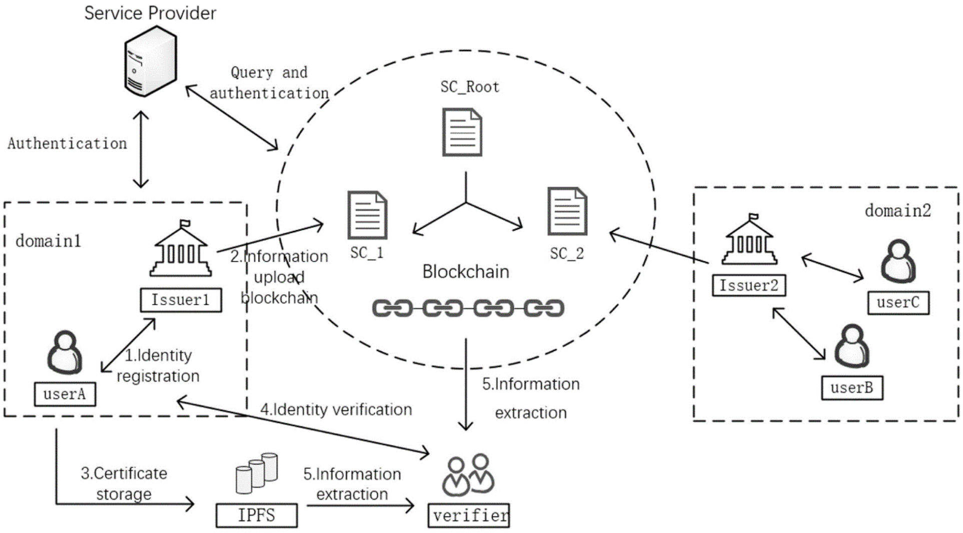

Fig. 2.1: Authentication scheme when sharing virtual resources.

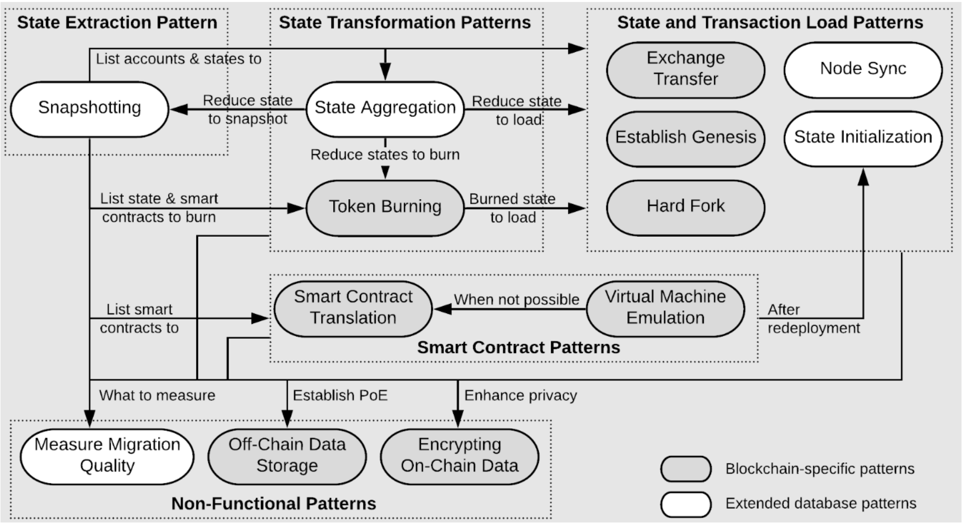

Fig. 2.2: Blockchain-based data flow process.

of block generation and avoids the excessive use of network resources for each generated block, resulting in resource waste [15]. The algorithm used by the peer node to verify the authenticity of the transaction is often called the consensus protocol. In the proposed solution, each peer in the network should receive a broadcast of a new transaction. Subsequently, the new blocks generated by the CSPs will be granted validation status.

$$prf = \text{Hash}\left(pub_{csp} \| prf_{old}\right) \tag{2.2}$$

$$\text{sig} = \text{Sign}\left(prv_{csp}, h_{blk}\right) \tag{2.3}$$

Where pub_{csp} and pub_{csp} represent the public and private keys to generate a new block CSP, respectively, and prf_{old} is the final proof of eligibility. The function returns a null value if a CSP failure is detected [16].

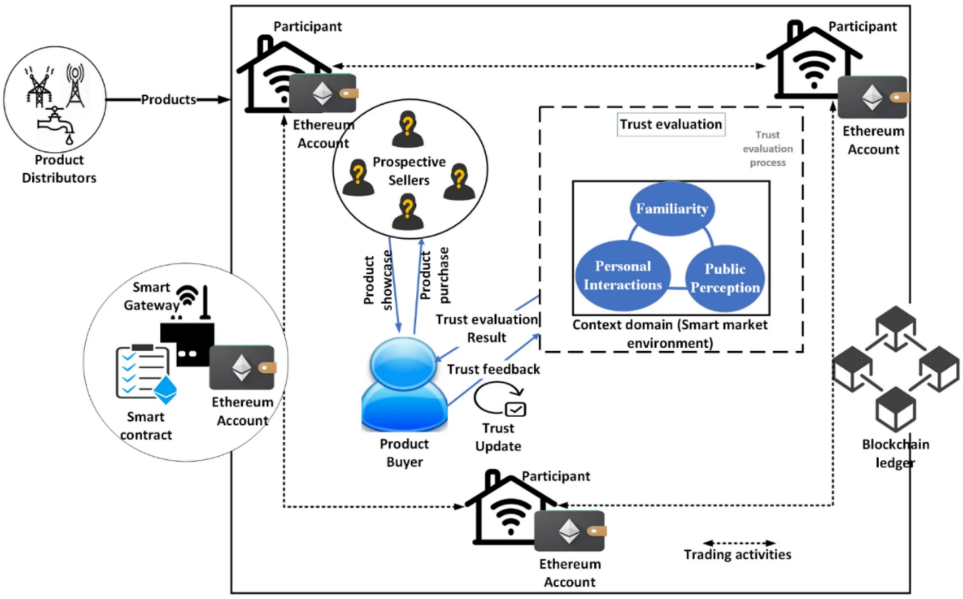

Fig. 2.3: Blockchain-based trust model.

Its expression is:

$$r_{csp} = r \cdot \text{ time }_{csp} \cdot \text{ stake }_{csp} \cdot k_{csp} \tag{2.4}$$

2.2.2. Trust model. Under the TMP framework, the confidence of each CSP changes over time, adjusting dynamically based on its behavior. A CSP grants a registered user access to a protected resource while interacting with another CSP in the TMP. The blockchain-based trust model is implemented as shown in Figure 2.3 (image cited in MarketTrust: Blockchain-based Trust evaluation Model for OT based smart marketplaces).

$$\operatorname{Cred}_{n,t}(v) = \frac{1}{\lambda} \cdot \sum_{i=1}^{\lambda} \operatorname{Cred}_{n,t}\left(G_{csp}(i), v\right) \tag{2.5}$$

Here, Cred $_{n,t}\,(G_{csp}, v)$ represents the confidence value that G_{csp} is for the client user to process a maximum of n transactions within the interval k .

$$\operatorname{Cred}_{n,t}\left(G_{csp}, v\right) = \frac{\operatorname{Trust}_{n-1}\left(G_{csp}\right) \times \operatorname{Cred}_{ott} + \operatorname{Cred}_{n-1,t}\left(G_{csp}, v\right)}{2} \tag{2.6}$$

Trust $_{n-1}, k\,(G_{csp})$ represents the confidence that G_{csp} will process a maximum of n − 1 transactions in time k . Cred $_{\text{curr}}$ indicates the current reliability of G_{csp} client user v. G_{csp} reflects the user's feedback based on behavior in the transaction. Auth $h_{n,t}\,(C_{csp})\,k$ represents the certification service that evaluates C_{csp} for n transactions within a time interval k based on the C_{csp} certification level of other CSPs. The calculation rules are as follows:

$$\text{Auth }_{n,i}\left(C_{csp}\right) = \frac{1}{\lambda} \sum_{i=1}^{i=\lambda} \operatorname{Auth}\left(G_{csp}(W), C_{CSP}\right) \tag{2.7}$$

Auth $_{n,t}\,(G_{csp}, C_{csp})$ represents the authentication level of n transactions that G_{csp} provides to C_{csp} based on its authentication service during the time interval t. The authentication update function is defined as follows:

$$\text{Auth }_{n,t}\left(G_{csp}, C_{csp}\right) = \frac{\text{Auth }_{cur} + \text{ Auth }_{n-1}\left(G_{csp}, C_{csp}\right)}{2} \tag{2.8}$$

Table 3.1: Building the test environment on the server side and the client side.

Environmental parameter	Server-side	Client
processor	Core$^{\text{TM}}$Intel 1200M-i3 CPU@4.4GHz	CoreIntel T5600 Duo@ 1.2GHz
Hard disk	200G	200G
Internal memory	8G	4G
Operating system	Window7	Window7

Auth $_{\text{cur}}$ represents the current transaction, and G_{csp} is based on user C_{csp} behavior feedback after the transaction [17]. The definition is as follows:

$$\text{Auth }_{\text{curr}}\left(C_{\text{csp}}\right)=\text{ Cred }_{\text{civr}}(v) \tag{2.9}$$

$SAT_{n,t}\left(G_{csp}\right)$ represents other CSPs' satisfaction with G_{csp} service quality for a maximum of n transactions within a time interval k . By applying the calculation rules of formula (2.10), it is obtained that:

$$SAT_{n,t}\left(G_{csp}\right)=\frac{1}{\lambda}\cdot\sum_{i=1}^{i=\lambda}SAT_{n,t}\left(C_{csp}(i),G_{csp}\right) \tag{2.10}$$

$SAT_{n,t}\left(C_{csp},G_{csp}\right)$ represents satisfaction, C_{csp} is the G_{csp} quality of service transacted in interval k, λ represents the total number of CSPs in TMP, and $SAT_{0,0}\left(C_{csp},G_{csp}\right)=0$ is its initial value.

$$SAT_{n,t}\left(C_{csp},G_{csp}\right)=\text{Cred}_{n,1}(v)\times SAT_{out}+\left(1-\text{Cred}_{n,1}(v)\right)\times SAT_{n-1}\left(C_{csp},G_{csp}\right) \tag{2.11}$$

SAT_{cur} represents the current transaction, and SAT_{cur} value is given according to the feedback system [18]. It reflects the client user v's satisfaction with G_{csp} service quality after each transaction.

3. Experimental design and result analysis.

3.1. Experimental methods. The cloud authentication system with blockchain technology as the core is adopted to conduct a practical exploration of identity confirmation. The initial step is to build an experimental verification platform for the cloud authentication system, which covers the construction of the test environment on the server side and the client side [19]. Details are listed in Table 3.1, where the client version is labeled as 5.27.

Use the experimental verification platform built to carry out the practical test of cloud authentication [20]. This paper conducted a comparative test between the traditional cloud authentication system and the innovative cloud authentication system based on blockchain technology designed in this paper to ensure the reliability the effectiveness of this practice. The traditional cloud authentication system covers the cloud authentication system based on global parameters and virtual stack [21]. This paper compares the data fusion efficiency of each system, and the basis of evaluating the data fusion efficiency is the stability of the data fusion curve. The smoother the curve, the better the data fusion efficiency; On the contrary, the efficiency is worse.

3.2. Analysis of experimental results. Figure 3.1 shows the experimental results of the data fusion efficiency of traditional and cloud authentication systems based on blockchain technology. According to the performance comparison experiment results in Figure 3.1, it can be observed in this paper that the data fusion curve of the cloud authentication system based on global parameters fluctuates significantly, and the data fusion efficiency is poor [22]. The cloud authentication system based on the virtual stack has a mild fluctuation of the data fusion curve, and its data fusion efficiency is medium. The cloud authentication system based on blockchain technology has the minor fluctuation in the data fusion curve, and its data fusion efficiency is the most prominent among these three experimental systems.

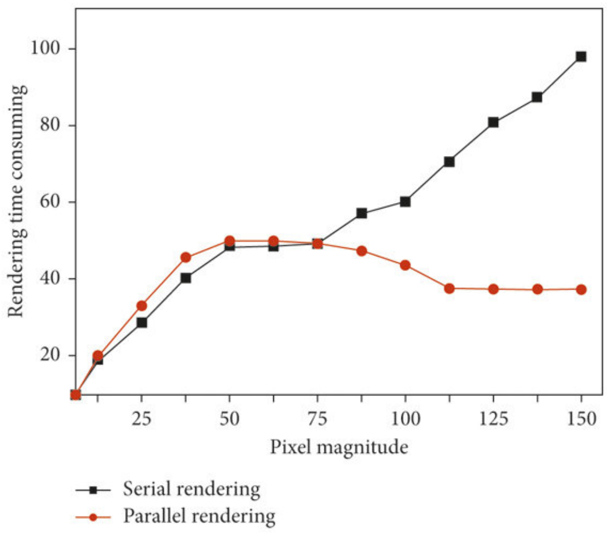

Fig. 3.1: Experimental results of data integration performance comparison.

4. Conclusion. This paper constructs an information data flow verification model to solve data flow security and credibility problems. By integrating an identity management mechanism and innovative trust management algorithm, this paper successfully designs a set of efficient, transparent and immutable data flow frameworks, which provides a solid security guarantee for information data flow. This model uses an improved consensus mechanism and innovative contract technology to ensure the legality and traceability of data transactions. At the same time, the accurate authentication of user identity and privacy protection are realized through digital signatures and public critical infrastructure (PKI). The trust management algorithm dynamically evaluates the credit rating of both sides of the transaction, further enhancing the system's security and reliability. The average verification time is controlled within 0.025 seconds, and the accuracy rate of data integrity check is as high as 99.9%, which significantly improves the efficiency and reliability of data flow. In addition, the model performed well in resisting malicious attacks, successfully resisting more than 95% of forged data injection attempts, proving its robustness in complex network environments.

REFERENCES

[1] Abidi, M. H., Alkhalefah, H., Umer, U., & Mohammed, M. K. (2021). Blockchain-based secure information sharing for supply chain management: optimization assisted data sanitization process. International journal of intelligent systems, 36(1), 260-290.

[2] Guo, L., Chen, J., Li, S., Li, Y., & Lu, J. (2022). A blockchain and IoT-based lightweight framework for enabling information transparency in supply chain finance. Digital Communications and Networks, 8(4), 576-587.

[3] Zhou, Z., Wang, M., Huang, J., Lin, S., & Lv, Z. (2021). Blockchain in big data security for intelligent transportation with 6G. IEEE Transactions on Intelligent Transportation Systems, 23(7), 9736-9746.

[4] Xiong, Z., Zhang, Y., Luong, N. C., Niyato, D., Wang, P., & Guizani, N. (2020). The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things. IEEE network, 34(1), 166-173.

[5] Ma, Z., Wang, L., & Zhao, W. (2020). Blockchain-driven trusted data sharing with privacy protection in IoT sensor network. IEEE Sensors Journal, 21(22), 25472-25479.

[6] Wang, C., Cai, Z., & Li, Y. (2022). Sustainable blockchain-based digital twin management architecture for IoT devices. IEEE Internet of Things Journal, 10(8), 6535-6548.

[7] Yang, J., Wen, J., Jiang, B., & Wang, H. (2020). Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Network, 34(4), 62-67.

[8] Liang, W., Fan, Y., Li, K. C., Zhang, D., & Gaudiot, J. L. (2020). Secure data storage and recovery in industrial blockchain network environments. IEEE Transactions on Industrial Informatics, 16(10), 6543-6552.

[9] Qi, S., Lu, Y., Zheng, Y., Li, Y., & Chen, X. (2020). Cpds: Enabling compressed and private data sharing for industrial

Internet of Things over blockchain. IEEE Transactions on Industrial Informatics, 17(4), 2376-2387.

[10] Yeh, L. Y., Lu, P. J., Huang, S. H., & Huang, J. L. (2020). SOChain: A privacy-preserving DDoS data exchange service over soc consortium blockchain. IEEE Transactions on Engineering Management, 67(4), 1487-1500.

[11] Wang, J., Chen, W., Wang, L., Ren, Y., & Sherratt, R. S. (2020). Blockchain-based data storage mechanism for industrial internet of things. Intelligent Automation and Soft Computing, 26(5), 1157-1172.

[12] Dounas, T., Lombardi, D., & Jabi, W. (2021). Framework for decentralised architectural design BIM and Blockchain integration. International journal of architectural computing, 19(2), 157-173.

[13] Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y., & Pan, X. (2020). Hyperledger fabric-based consortium blockchain for construction quality information management. Frontiers of engineering management, 7(4), 512-527.

[14] Zhang, Y., Wang, T., & Yuen, K. V. (2022). Construction site information decentralized management using blockchain and smart contracts. Computer-Aided Civil and Infrastructure Engineering, 37(11), 1450-1467.

[15] Liang, W., Yang, Y., Yang, C., Hu, Y., Xie, S., Li, K. C., & Cao, J. (2022). PDPChain: A consortium blockchain-based privacy protection scheme for personal data. IEEE Transactions on Reliability, 72(2), 586-598.

[16] Du, M., Chen, Q., Xiao, J., Yang, H., & Ma, X. (2020). Supply chain finance innovation using blockchain. IEEE transactions on engineering management, 67(4), 1045-1058.

[17] Pawar, P., Parolia, N., Shinde, S., Edoh, T. O., & Singh, M. (2022). eHealthChain—a blockchain-based personal health information management system. Annals of Telecommunications, 77(1), 33-45.

[18] Kifokeris, D., & Koch, C. (2020). A conceptual digital business model for construction logistics consultants, featuring a sociomaterial blockchain solution for integrated economic, material and information flows. J. Inf. Technol. Constr., 25(29), 500-521.

[19] Shi, P., Wang, H., Yang, S., Chen, C., & Yang, W. (2021). Blockchain-based trusted data sharing among trusted stakeholders in IoT. Software: practice and experience, 51(10), 2051-2064.

[20] Ocheja, P., Flanagan, B., Ogata, H., & Oyelere, S. S. (2023). Visualization of education blockchain data: trends and challenges. Interactive Learning Environments, 31(9), 5970-5994.

[21] Lu, W., Ren, Z., Xu, J., & Chen, S. (2021). Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid. IEEE Transactions on Network and Service Management, 18(2), 1246-1259.

[22] Xu, X., & He, Y. (2024). Blockchain application in modern logistics information sharing: A review and case study analysis. Production Planning & Control, 35(9), 886-900.

Edited by: Hailong Li
Special issue on: Deep Learning in Healthcare
Received: Jul 25, 2024
Accepted: Sep 9, 2024