International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 8, pp 62-70, August-2024

https://doi.org/10.47001/IRJIET/2024.808008

The Blockchain in Secure and Efficient Data Sharing: A Review

[1]Kanaan J. Brakas, [2]Mafaz Alanezi

[1]General Directorate of Kirkuk Education, Kirkuk, Iraq. E-mail: kjbbaby@gmail.com
[2]ICT Research Unit, Computer Center, University of Mosul, Mosul, Iraq. E-mail: mafazmhalanezi@uomosul.edu.iq

***Abstract* - Blockchain technology has received a lot of attention since its very beginning due to its unique characteristics such as decentralization, immutability, smart contracts, and consensus procedures. Today's digital systems and data exchange systems face several obstacles in the era of digital collaboration in all economic, financial, commercial, scientific, and other fields. Blockchain technology offers the ability to address a wide range of difficulties associated with digital data sharing, such as data management, security, and privacy. This assessment of data sharing based on blockchain technology includes various research publications published in prominent scientific journals between 2022 and 2024. We employ the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) and its surrounding region. This study uses articles' databases: Elsevier, Springer, IEEE Xplore, Web of Science, and MDPI. This study comprised 36 studies. We discovered that authors attempted to use blockchain technology to enable consumers and other organizations to share data, information, experiences, and process data, as well as to include various entities. Our study examines the impact of using different methods of storing data with blockchain technology on the security of that data and what depends on choosing the best method of storing data between on-chain and off-chain storage, with the aim of solving many problems such as access control, data security, and privacy that are overlooked in traditional systems.**

Keywords: Blockchain technology, Blockchain-based data sharing, Blockchain technology review, Efficient Data Sharing, Data Sharing review.

I. INTRODUCTION

Blockchain technology enables numerous users to share data stored in a ledger without the need for a centralized administrator. Many independent users create a sophisticated technological ledger that ties data items to their owners, and each node verifies the encoded data before accepting and sharing it. As a result, the all-in consensus process preserves the data state that all nodes agree on [1]. Because of the unique features of blockchain technology, there are two separate approaches to using resources to store data. For example, blockchain technology does not handle large volumes of data. The first option is on-chain storage, which stores data in a block on the blockchain. An alternate method is to use external resources, such as the cloud or IPFS. The characteristics of using the two methods will be the primary focus of this study [2]. There are three major types of blockchain technologies: private, public, and hybrid, which are used and classified based on the ability to access the data contained inside them. Because data on public blockchain technology is accessible to all participants, access is restricted to specified participants only, using private blockchain technology. The hybrid technology combines the advantages of private and public blockchain systems [3].

The remainder of this work focuses on the following areas: Section No. 2 clarifies the research methods; Section No. 3 provides background information on blockchain technology; Section No. 4 focuses on previous work using blockchain technology to share data; and Section No. 5 discusses previous works in terms of the mechanism for using blockchain technology and storage types. The conclusion is in Section 6, and the references are in Section 7.

1.1 Method of Research

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement was first released more than ten years ago [4]. The (PRISMA) method is intended to assist authors in properly reporting systematic reviews and meta-analyses. Data sharing in IoT, smart cities, supply chains, health, and other decision makers see systematic reviews as an important resource for information that has been gathered in a systematic and transparent way [5]. Some (PRISMA) components provided a comprehensive, methodical, and scientific investigation of blockchain-based applications for data exchange in healthcare. The literature survey in Figure 1 includes the most recent research on blockchain technology for data exchange. The activities listed below influenced the results of the systematic survey [6].

1.1.1 Questions of Research

This study's research questions:

1. What problems does the data-sharing system have?
2. What are blockchain's main data-sharing benefits?
3. What blockchain architecture models, types, and methods exist?
4. How does on-chain or off-chain storage affect data sharing systems and when should it be used?

1.1.2 Strategy of Search

The databases used were Web of Science, Springer, IEEE, Scopus, and MDPI. After reviewing scholarly publications, reviews, and surveys on developing topics like blockchain-based data exchange, these databases were chosen. Google Scholar searches for papers containing "(blockchain-based data sharing OR blockchain technology with data sharing) AND (decentralized data sharing OR secure data sharing OR data management OR smart contract)".

1.1.3 Selection of Study

We selected articles for our final review using the inclusion and exclusion criteria below after receiving the papers. This study includes papers based on inclusion criteria. The results reflect the number of papers used in this review.

A) Including Criteria

The inclusion requirements are, the studies are published in English. Only journal publications, reviews, conferences, and open-source surveys publish studies. The main contribution of this research is blockchain-based data exchange. The blockchain-based data sharing research study covers architecture, system design, use cases, framework, platform, scheme, model, method, transaction location, and model storage. Studies 2022–2024.

B) Excluding Criteria

Studies are not published in the English language. Excludes proceedings, book chapters, periodical articles, and theses. Discard duplicate papers.

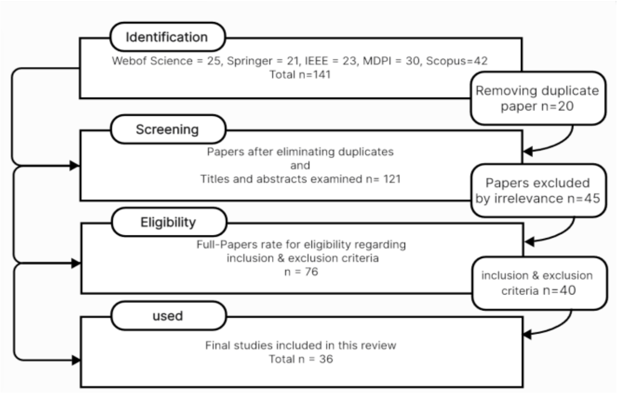
Identification
Webof Science = 25, Springer = 21, IEEE = 23, MDPI = 30, Scopus=42
Total n=141
Removing duplicate paper n=20
Screening
Papers after eliminating duplicates
and
Titles and abstracts examined n= 121
Papers excluded by irrelevance n=45
Eligibility
Full-Papers rate for eligibility regarding
inclusion & exclusion criteria
n = 76
inclusion & exclusion criteria n=40
used
Final studies included in this review
Total n = 36

Figure 1: flow diagram for selecting

C) Result

After deleting duplicated and irrelevant publications, the final survey included 36 articles. Figure 1 shows the preferred reporting items for systematic reviews and meta-analyses (PRISMA). Figure 1 shows the flow diagram for selecting articles.

II. BACKGROUND OF BLOCKCHAIN TECHNOLOGY

Multiple blockchain versions have been created since Bitcoin's inception. Blockchain was used for digital data in finance transactions [7]. One of the most promising subjects is data sharing [8]. Blockchain technology is redefining data governance and management in data-sharing apps. This is due to its adaptability and unique ability to encrypt, segregate, and distribute data and services [9]. Blockchain drives many data-sharing advances. Real-world systems exchange IOT, health, and other data but are not consistent with external systems [10]. Data suggests that integrating these networks into various networked, high-quality institutions and enterprises has many benefits, including connecting informatics and information security researchers and organizations [11]. Business and management must effectively manage and safeguard the huge amounts of data exchanged between firms during daily operations, transaction processing, and service supply. Most data transferred is inaccessible, unreliable, and hard to understand, manage, and distribute [12]. Sharing data is a security issue. Most firms store sensitive data in a centralized area vulnerable to malware and other attacks owing to legacy IT architecture. Blockchain technology may help maintain, process, share, secure, and evolve digital data [13]. Many businesses and agencies are also building infrastructure, computer programs, and key technologies to safely, securely, and reliably combine data sets [14]. This part discusses blockchain basics to help you comprehend the rest of the study. [15] To securely store data, a blockchain uses digital ledger types copied concurrently across numerous peer-to-peer networks. Blockchains are specialized distributed ledger technology (DLT) that describes any database maintained in several locations [16]. Each data block in the blockchain has a pointer to the previous block, represented by a hash address.

2.1 Blockchain Benefits

This article goes into detail about the characteristics of blockchain. These qualities were also described in other study publications; however, some of these features led to other specific characteristics, allowing the list to be reduced.

ISSN (online): 2581-3048
Volume 8, Issue 8, pp 62-70, August-2024
https://doi.org/10.47001/IRJIET/2024.808008

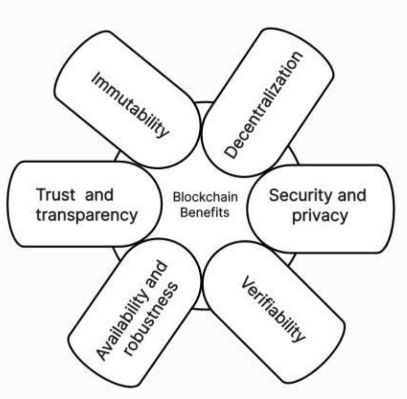

Figure 2: Blockchain Benefits

2.1.1 Decentralization

Decentralized networks are maintained by nodes. It is essential to blockchain technology. Traditional centralized systems are limited by central transaction permission. Unlike centralized systems, blockchain requires no third parties. Consensus methods ensure network data consistency. Blockchain is an open, decentralized ledger. Open ledgers allow anyone to view transactions. Blockchain transactions are uncontrolled. Every network connection copies the ledger [17].

2.1.2 Immutability

Blockchain technology's immutability prevents data alteration, making it attractive. Blockchain technology is renowned for its immutable network and permanence. Blockchain data is unchangeable and requires node approval before being added to a block, providing safe transactions. Mining improves security and privacy by adding and validating block transactions [18].

2.1.3 Availability and Robustness

Genuine miners can easily validate transactions and reject invalid ones. Blockchain transactions are irreversible. Uneven block transactions are readily noticeable. Any transaction or block in a chain is confirmed, making the data permanent and traceable. Bitcoin has one ledger viewable from all nodes, ensuring a complete cash trail and preventing double-spending [19].

2.1.4 Trust and Transparency

Chain transactions require only the recipient's ID, ensuring anonymity for all parties. Users communicate with the blockchain using created addresses to hide their identities. Due to its limitations, the blockchain cannot guarantee privacy [20].

2.1.5 Verifiability

Blockchain data is protected through authentication, integrity, and precision, allowing for verification without complete access to entries. This capability is useful in health care for authenticating records, such as pharmaceutical supply chain tracking and insurance claim processing. Digital ledger technology makes healthcare information reliable and accessible to all network users, allowing for multiple sharing among blockchain nodes. Blockchains maintain data integrity and file synchronization by self-updating at predetermined intervals [21].

2.1.6 Privacy and Security

Blocks of transaction data are protected from internal, peripheral, hostile, or unintentional threats via "blockchain" technology. Security and IT services, regulations, and technologies are used to identify, prevent, and respond to threats. Blockchain privacy allows a stakeholder or group to isolate themselves from other data and communicate in an identifiable manner. Transactions can be made without revealing personal information. Users can also disclose to ensure compliance [22].

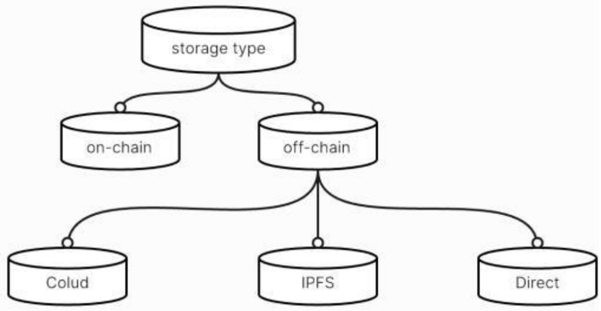

Figure 3: Blockchain Data storage classification

2.2 Consensus Mechanism

Blockchain consensus methods ensure that all network participants accept the distributed ledger's state. It increases blockchain network resilience by trusting anonymous individuals in distributed computing. The consensus operations ensure that each new blockchain block represents the only truth agreed upon by all parties.

Proof of Work (PoW) Satoshi Nakamoto proposed a paper on Bitcoin Proof of Work (PoW) in 2008. Today, most cryptocurrencies adopt the Proof of Work consensus. A 1999 book by Markus Jakobsson and Ari Juels introduced "proof of work." Mathematical problems can be difficult. Validating the solution is simple. The next block generation is decided by this consensus algorithm. The Bitcoin consensus algorithm is PoW. The program seeks a simple solution to a difficult mathematical problem. This puzzle demands a lot of processing power; thus, the first node to solve it mines the next block. [24].

Practical Byzantine Fault Tolerance (PBFT) Miguel Castro and Barbara Liskov proposed PBFT in the late 1990s. Asynchronous systems are designed for PBFT efficiency. The minimum overhead time is the target. Byzantine fault tolerance methods exist, but they are problematic. It's used in blockchain and distributed computing. Energy efficiency, transaction finality, and minimal reward variance are benefits. Sybil attacks, scaling weaknesses [25].

Proof of Stake (PoS) Most people use it instead of PoW. Ethereum's consensus algorithm is PoS. Consider staking validator money. From there, everyone certifies blocks. Validators bet on blocks worth adding to the chain. Taking into account all validators, stakes increase proportionally with blockchain block additions. A fresh block validator is chosen using an economic stake in the network. Incentives help validators reach consensus in POS [26].

Proof of Capacity (PoC) Validators should use hard drive space to promote PoC consensus instead of buying expensive hardware or burning coins. Validators with more hard drive capacity are more likely to mine the next block and obtain the reward [15].

2.3 Smart Contract

Smart contracts are computational programs that facilitate the execution of agreements between many parties. Blockchain technology eradicates intermediaries in transactions. Its ability to automate and secure multi-domain transactions has made it popular. They employ non-standard software life cycles, which may generate security and user issues. Smart contract frameworks are available on Ethereum, Counterparty, Stellar, Monax, and Lisk. Traditional software has wider measurement ranges than smart contracts. They enable decentralized, secure agreement execution without intermediaries [23].

III. BLOCKCHAIN-BASED DATA SHARING

Sharing data between companies, commercial, scientific, and health institutions, and regulatory authorities is a necessary and very important matter, especially after the developments taking place in the digital world, as data needs security services to ensure the integrity of the data during sharing and faces various challenges such as data theft, forgery, data spying, and others. Blockchain technology, by its nature, is built on providing many of these security services that help facilitate the data sharing process, according to many previous studies, which are summarized in our study.

3.1 Storage Used in Blockchain-Based Data Sharing

Previous studies have used a variety of storage techniques for data sharing based on blockchain technology, including on-chain, cloud, direct storage, and the InterPlanetary File System (IPFS). Each storage technology has properties that distinguish it from the others. Here are some previous studies on each:

3.1.1 On-Chain

RCDS verifies data rights using symbol mapping coding (SMC) and blockchain. By L. Wang et al., symbol mapping coding (SMC) encodes each party's digital identification into the byte sequence of shared data, allowing content-independent data rights declaration for any type and volume of information. Blockchain technology lets data-sharing entities cooperatively monitor data delivery and access, validating data rights [27]. To protect IoT data providers' privacy, BP2P-FL uses peer-to-peer federated learning and model sharing. Miao et al. suggested using blockchain technology to record every training procedure to ensure data sources provide high-quality information [28]. A blockchain-based solution to supply chain business information sharing issues. A blockchain-based supply chain architecture for industrial institutions provides a hierarchical paradigm for blockchain supply chain information. Hsiao &Sung propose registering supply chain information blocks using a multi-resource data structure and analysis. It recommends a multi-resource data analysis center [29]. A bloom filter-based ITS data search that reduces data and computing expenses by selecting a low-frequency phrase. The protocol tags each identifier-keyword pair to finish the search in one trip while maintaining confidentiality. It allows dynamic data record addition and deletion. Jiang et al.'s security model treats blockchain nodes and ITS data owners as potentially malicious and improves multi-keyword search searches with new data structures [30]. Yele et al. Use IoT devices to capture supply chain data and upload it to the blockchain network for verification and storage to increase blockchain technology integration with RFID technology. Food is tracked throughout the supply chain using RFID technology. The food supply chain is transparent and traceable since each product has a QR code, and a blockchain-based ledger records transactions and alterations [31]. A secure blockchain-based IoT publish-subscribe access control technique. The ledger preserves data events and permits cross-domain information access, while fully homomorphic encryption ensures anonymity. Z. Liu et al.'s approach was carefully evaluated for correctness and security. A prototype system is tested on two PCs to measure performance. Collusion and spoofing resistance are theoretically investigated in the method's security. The scheme's performance and security are carefully tested on two PCs [32].

3.1.2 Off-Chain

Using data storage sources outside the blocks of blockchain technology is necessary, especially in the case of large data. Many external storage resources were used, including the following:

- **Cloud**

Zhang et al. propose a consortium blockchain for medical data exchange. Patients pick who can view their records, and requesters have traits. Access policies are blockchain-based, but records are off-chain encrypted. Tencent Cloud uses Quorum. Hash functions and smart contracts are discussed. The Authorize contract provides authorization interfaces. Access requests are accepted if they match the criteria. The center and owners are trustworthy, and opponents are weak [33]. A blockchain-based cross-user auditing method. Users can delegate auditing jobs to a third-party auditor and share the auditing process with others using Li et al.'s method, ensuring privacy and efficiency. Functionality, theoretical analysis, and application are compared to other methods to assess their efficacy [34]. A blockchain-based system for anonymous data sharing on the IoT that uses ring signatures, linkable ring signatures, and Signature of Knowledge (SoK) to enable anonymity, data privacy, accountability, and authenticity. Wu et al.'s analysis shows the scheme's safety and effectiveness in the random oracle model, and experiments confirm its computing complexity, communication operation cost, and blockchain use [35]. Hasan et al. developed a blockchain-SDWBAN architectural framework for safe healthcare data sharing. It addresses data confidentiality, user-centric design, integrity, and privacy in SDWBANs. The proposed system uses smart contracts for access control. Compared to standard cloud-based solutions, experimental results are promising [36]. How crucial EMR management and sharing are in e-healthcare. Lin et al. offer proxy re-encryption (PRE) for safe EMR sharing with access control. Blockchain-based technologies address privacy and security problems by exploiting the blockchain's decentralization and re-encryption key secrecy. Smart contracts on the blockchain enable accurate and complete ciphertext-searching results [37]. An architecture that uses blockchain and SDWBANs to securely share Isaja et al. To provide health data owners with full control, a smart contract-based access control mechanism is being developed. Only the block hash is added to the blockchain from off-chain storage. High throughput and minimal latency distinguish the paradigm from traditional cloud-based systems [38]. Feng et al. described a blockchain-based medical data sharing system with privacy and access management. LDP and SE protect identity and data privacy. Blockchain and cloud server storage enable fine-grained access control and collusion prevention. New secure medical data exchange ideas. It also described a blockchain-based distributed verified healthcare data sharing system in an untrustworthy environment [39].

- **InterPlanetary File System (IPFS)**

Na & Park offers a decentralized oracle and multi-signature accident access control system. Distributed file systems store and communicate video data. Estimating vehicle distance is approximate. Create, upload, and encrypt dashcam videos. The blockchain aggregates transactions. To assure video data accuracy, Na & Park propose a V2V network and multi-signature access control mechanism based on GPS distance-based grouping [40]. Jaberzadeh et al. proposed a system that uses data trust in federated learning, IPFS, blockchain, and smart contracts to enable secure and mutually beneficial data sharing with incentives, access restrictions, and consequences for dishonesty. The smart contract system controls data sharing, compensation, and access and needs a collateral deposit to prevent fraud. Participants who provide accurate data receive the forfeited deposit. IPFS allows federated learning models to be trained on users' devices rather than centralized storage [41]. Athanere and Thakur propose a blockchain-IPFS data sharing system. Changes to blocks are logged on the chain, making them difficult to hide. IPFS secures encrypted files uploaded by data owners with hash codes. Owner-set data access permissions. It uses two-level key management. Blockchain technology addresses consumers, eliminates failures, and cuts costs [42]. Ullah Khan et al. suggested a blockchain-based IOWST authentication, data sharing, and non-repudiation method. Used a consortium blockchain to identify lawful nodes. Coordination smart contracts provide sensor node authentication, data exchange, and non-repudiation. Artificial intelligence-based IPFS stores node ambient data. A stellar consensus protocol boosts network capacity. Large simulations support the suggested method, which has reduced transaction latency compared to a POW-based model (Ullah Khan et al., 2023). Zhang et al. proposed a blockchain-based approach for storing anomalous cereal and oil video surveillance data. A deep learning algorithm detects unusual photographs in surveillance data. Data is hashed and stored on a blockchain for security. IPFS is a secondary database that reduces storage needs. The experiment uses FISCO BCOS and WeBASE to deploy blockchain and activate smart contracts.[44]. S. Liu & Zheng suggests a blockchain-IPFS court evidence storage strategy. A storage module for IPFS-stored court evidence, a permission module for authority and privacy, and a smart contract module for blockchain connectivity make up the scheme architecture. The article utilizes the FISCO BCOS blockchain network, which provides high TPS and distributed big service storage capabilities. [45]. Tong et al. proposed an industrial Internet of Things data exchange and privacy method. They use a weighted threshold secret sharing strategy to improve data sharing. Use non-interactive zero-knowledge proof technologies to construct a lightweight identity proof system. The InterPlanetary File System encrypts shared files. Using theoretical and experimental methodologies, the technique's computing overhead is studied [46].

- **Direct Storage**

Liu et al. presented a fair, private, auditable, and general blockchain system. Data transport is safe and fair with adaptor signatures and zero knowledge. The protocol works with several blockchains. Experimental results on an Ethereum test network suggest that the protocol is practical and helpful. Data access rights and security are tracked using blockchain technology. Adaptor signatures and zero-knowledge proofs reduce threats. Python implementations of the design using specified encryption methods show its practicality and performance [47].

IV. CONCLUSION

Blockchain applications have increased in popularity and need to be improved to solve many problems. Thus, blockchain technology will become big data-based, scalable, efficient, and secure. When viewed on its own, its functions and much of its technology are familiar. However, its combination of features makes it suitable for many applications, indicating high demand. The study evaluated blockchain data-sharing research and applications. We identified search topics and reduced the reviewed articles to 36 studies using the predefined process. We searched five databases for 2022–2024 publications. Further analysis follows. This paper describes key data-sharing applications where blockchain technology can have a significant impact. This paper discusses several blockchain data exchange requirements and solutions. According to the articles, we have identified a mechanism for selecting the type of blockchain technology and on-chain or off-chain data storage that best suits data sharing applications based on data volume, security, trust, and system node size. It is preferable to use on-chain storage if the data to be shared is of small size and is not affected by the limited block size according to blockchain technology, as well as preventing tampering with or modifying that data after it is actually stored on the chain. When sharing large amounts of data, it is preferable to store it off-chain to avoid problems with the limited size of the block.

ACKNOWLEDGEMENT

We are grateful for all the support the Computer Science Department/ University of Mosul/ Iraq provides.

REFERENCES

[1] M. M. Taha and M. Alanezi, “Cryptocurrencies in Blockchains Environment: The Verification Trip,” in 4th International Conference on Current Research in Engineering and Science Applications, ICCRESA 2022, Institute of Electrical and Electronics Engineers Inc., 2022.

[2] Y. P. Tsang, C. K. M. Lee, K. Zhang, C. H. Wu, and W. H. Ip, “On-Chain and Off-Chain Data Management for Blockchain-Internet of Things: A Multi-Agent Deep Reinforcement Learning Approach,” J Grid Comput, vol. 22, no. 1, p. 16, Mar. 2024.

[3] M. M. Taha and M. Alanezi, “The Blockchains Technologies for Cryptocurrencies: A Review,” in 2022 International Conference for Natural and Applied Sciences, ICNAS 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 101–106.

[4] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, “How to properly use the PRISMA Statement,” Systematic Reviews, vol. 10, no. 1. BioMed Central Ltd, Dec. 01, 2021.

[5] M. M. Albhirat et al., “The PRISMA statement in enviropreneurship study: A systematic literature and a research agenda,” Clean Eng Technol, vol. 18, p. 100721, Feb. 2024, doi: 10.1016/j.clet.2024.100721.

[6] S. A. Bennacer, K. Sabiri, A. Aaroud, K. Akodadi, and B. Cherradi, “A comprehensive survey on blockchain-based healthcare industry: applications and challenges,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 30, no. 3, pp. 1558–1571, Jun. 2023.

[7] A.Mercik, T. Słoński, and M. Karaś, “Understanding crypto-asset exposure: An investigation of its impact on performance and stock sensitivity among listed companies,” International Review of Financial Analysis, vol. 92, p. 103070, Mar. 2024.

[8] Y. Sun, R. Jia, A. Razzaq, and Q. Bao, “Social network platforms and climate change in China: Evidence from TikTok,” Technol Forecast Soc Change, vol. 200, p. 123197, Mar. 2024.

[9] K. Thapliyal, M. Thapliyal, and D. Thapliyal, “Social Media and Health Communication,” in Emerging Technologies for Health Literacy and Medical Practice, Emerging Technologies for Health Literacy and Medical Practice, 2024, pp. 364–384.

[10] Y. Yue and J. Z. Shyu, “A paradigm shift in crisis management: The nexus of AGI-driven intelligence

fusion networks and blockchain trustworthiness," Journal of Contingencies and Crisis Management, vol. 32, no. 1, Mar. 2024, doi: 10.1111/1468-5973.12541.

[11] S. Kumari and M. Eknath Patil, "International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Academic and Commercial Circles in Block Chain Secure Privacy and Scalability at Block Chain Technologies."

[12] S. Asaithambi, L. Ravi, M. Devarajan, A. S. Almazyad, G. Xiong, and A. W. Mohamed, "Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platform for SMEs," Egyptian Informatics Journal, vol. 25, p. 100444, Mar. 2024.

[13] H. Prasad Josyula, L. T. Reddi, S. Parate, and A. Rajagopal, "International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING A Review on Security and Privacy Considerations in Programmable Payments," 2023.

[14] A.Kharche, S. Badholia, and R. K. Upadhyay, "Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India," Blockchain: Research and Applications, p. 100188, Jan. 2024, doi: 10.1016/j.bcra.2024.100188.

[15] A.Sharma, S. Kaur, and M. Singh, "A secure blockchain framework for the internet of medical things," Transactions on Emerging Telecommunications Technologies, vol. 35, no. 1, Jan. 2024.

[16] B. Sun, Q. Dang, Y. Qiu, L. Yan, C. Du, and X. Liu, "Blockchain Privacy Data Access Control Method Based on Cloud Platform Data," International Journal of Advanced Computer Science and Applications, vol. 13, no. 6, 2022, doi: 10.14569/IJACSA.2022.0130602.

[17] K. K. Vaigandla, R. Karne, M. Siluveru, and M. Kesoju, "Review on Blockchain Technology: Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications," Mesopotamian Journal of Cyber Security, pp. 73–85, Mar. 2023, doi: 10.58496/MJCS/2023/012.

[18] K. Kottursamy, B. Sadayapillai, A. A. AlZubi, and A. K. Bashir, "A novel blockchain architecture with mutable block and immutable transactions for enhanced scalability," Sustainable Energy Technologies and Assessments, vol. 58, p. 103320, Aug. 2023.

[19] J. Aslam, A. Saleem, and Y. B. Kim, "Blockchain-enabled supply chain management: integrated impact on firm performance and robustness capabilities," Business Process Management Journal, vol. 29, no. 6, pp. 1680–1705, Oct. 2023, doi: 10.1108/BPMJ-03-2023-0165.

[20] V. Singh and S. K. Sharma, "Application of blockchain technology in shaping the future of food industry based on transparency and consumer trust," Journal of Food Science and Technology, vol. 60, no. 4. Springer, pp. 1237–1254, Apr. 01, 2023. doi: 10.1007/s13197-022-05360-0.

[21] M. Zhou, Z. Yang, H. Yu, and S. Yu, "VDFChain: Secure and verifiable decentralized federated learning via committee-based blockchain," Journal of Network and Computer Applications, vol. 223, p. 103814, Mar. 2024.

[22] S. Kayikci and T. M. Khoshgoftaar, "Blockchain meets machine learning: a survey," J Big Data, vol. 11, no. 1, p. 9, Jan. 2024.

[23] F. AyotundeAlaba, H. A. Sulaimon, M. Ifeyinwa Marisa, and O. Najeem, "Smart Contracts Security Application and Challenges: A Review," Cloud Computing and Data Science, vol. 5, 2024.

[24] S. Fahim, S. Katibur Rahman, and S. Mahmood, "Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV," International Journal of Mathematical Sciences and Computing, vol. 9, no. 3, pp. 46–57, Aug. 2023, doi: 10.5815/ijmsc.2023.03.04.

[25] J. Liu, W. Feng, M. Huang, S. Feng, and Y. Zhang, "Grouped Multilayer Practical Byzantine Fault Tolerance Algorithm: A Practical Byzantine Fault Tolerance Consensus Algorithm Optimized for Digital Asset Trading Scenarios," Sensors, vol. 23, no. 21, p. 8903, Nov. 2023.

[26] Z. Du, L. Liu, M. Huang, Y. Fu, and W. Zhang, "Bulwark: A proof-of-stake protocol with strong consistency and liveness," Computer Networks, vol. 242, p. 110245, Apr. 2024.

[27] L. Wang, S. Huang, L. Zuo, J. Li, and W. Liu, "RCDS: a right-confirmable data-sharing model based on symbol mapping coding and blockchain," Frontiers of Information Technology and Electronic Engineering, vol. 24, no. 8, pp. 1194–1213, Aug. 2023.

[28] Q. Miao, H. Lin, J. Hu, and X. Wang, "An intelligent and privacy-enhanced data sharing strategy for blockchain-empowered Internet of Things," Digital Communications and Networks, vol. 8, no. 5, pp. 636–643, Oct. 2022.

[29] S. J. Hsiao and W. T. Sung, "Blockchain-Based Supply Chain Information Sharing Mechanism," IEEE Access, vol. 10, pp. 78875–78886, 2022, doi: 10.1109/ACCESS.2022.3194157.

[30] S. Jiang, J. Cao, H. Wu, K. Chen, and X. Liu, "Privacy-preserving and efficient data sharing for blockchain-

ISSN (online): 2581-3048
Volume 8, Issue 8, pp 62-70, August-2024
https://doi.org/10.47001/IRJIET/2024.808008

based intelligent transportation systems," Inf Sci (N Y), vol. 635, pp. 72–85, Jul. 2023.

[31] S. Yele and R. Litoriya, "Blockchain-based secure dining: Enhancing safety, transparency, and traceability in food consumption environment," Blockchain: Research and Applications, p. 100187, Jan. 2024.

[32] Z. Liu et al., "A Blockchain-Based Privacy-Preserving Publish-Subscribe Model in IoT Multidomain Data Sharing," WirelCommun Mob Comput, vol. 2022, 2022, doi: 10.1155/2022/2381365.

[33] D. Zhang, S. Wang, Y. Zhang, Q. Zhang, and Y. Zhang, "A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain," Security and Communication Networks, vol. 2022, 2022, doi: 10.1155/2022/2759787.

[34] A.Li, G. Tian, M. Miao, and J. Gong, "Blockchain-based cross-user data shared auditing," Conn Sci, vol. 34, no. 1, pp. 83–103, Dec. 2022, doi: 10.1080/09540091.2021.1956879.

[35] T. Wu et al., "Blockchain-Based Anonymous Data Sharing With Accountability for Internet of Things," IEEE Internet Things J, vol. 10, no. 6, pp. 5461–5475, Mar. 2023, doi: 10.1109/JIOT.2022.3222453.

[36] K. Hasan, M. J. M. Chowdhury, K. Biswas, K. Ahmed, Md. S. Islam, and M. Usman, "A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks," Computer Networks, vol. 211, p. 109004, Jul. 2022, doi: 10.1016/j.comnet.2022.109004.

[37] G. Lin, H. Wang, J. Wan, L. Zhang, and J. Huang, "A blockchain-based fine-grained data sharing scheme for e-healthcare system," Journal of Systems Architecture, vol. 132, Nov. 2022.

[38] M. Isaja et al., "A blockchain-based framework for trusted quality data sharing towards zero-defect manufacturing," Comput Ind, vol. 146, Apr. 2023, doi: 10.1016/j.compind.2023.103853.

[39] T. Feng, L. Chen, and R. Ma, "BTMDS: Blockchain Trusted Medical Data Sharing Scheme with Privacy Protection and Access Control," 2024, [Online]. Available: https://ssrn.com/abstract=4668770

[40] D. Na and S. Park, "Blockchain-Based Dashcam Video Management Method for Data Sharing and Integrity in V2V Network," IEEE Access, vol. 10, pp. 3307–3319, 2022, doi: 10.1109/ACCESS.2022.3140419.

[41] A.Jaberzadeh, A. K. Shrestha, F. A. Khan, M. A. Shaikh, B. Dave, and J. Geng, "Blockchain-Based Federated Learning: Incentivizing Data Sharing and Penalizing Dishonest Behavior," in Blockchain and Applications, 5th ed., vol. 778, Springer, Cham, 2023, pp. 186–195.

[42] S. Athanere and R. Thakur, "Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 4, pp. 1523–1534, Apr. 2022.

[43] A.Ullah Khan, • Nadeem Javaid, • Muhammad, A. Khan, and I. Ullah, "A Blockchain Scheme for Authentication, Data Sharing and Nonrepudiation to Secure Internet of Wireless Sensor Things."

[44] Y. Zhang et al., "Research on Blockchain-Based Cereal and Oil Video Surveillance Abnormal Data Storage," Agriculture (Switzerland), vol. 14, no. 1, Jan. 2024, doi: 10.3390/agriculture14010023.

[45] S. Liu and Q. Zheng, "A Study of a blockchain-based judicial evidence preservation scheme," Blockchain: Research and Applications, p. 100192, Feb. 2024, doi: 10.1016/j.bcra.2024.100192.

[46] W. Tong, L. Yang, Z. Li, X. Jin, and L. Tan, "Enhancing Security and Flexibility in the Industrial Internet of Things: Blockchain-Based Data Sharing and Privacy Protection," Sensors, vol. 24, no. 3, Feb. 2024.

[47] Z. Liu, A. Yang, H. Zeng, C. Jiang, and L. Ma, "A Generalized Blockchain-Based Government Data Sharing Protocol," Security and Communication Networks, vol. 2023, 2023.

AUTHORS BIOGRAPHY

Kanaan J. Brakas is a teacher at Mandali Boys' Middle School General Directorate of Kirkuk Education, Kirkuk, Iraq. And works as a lecturer at Kirkuk University, Faculty of Computer Science and Information Technology, Iraq. He obtained M.Sc. Degree in computer science (Information Security), at Osmania University, Hyderabad, India. His research interests are in Cybersecurity, Artificial Intelligence, Networks.
Email: kjbbaby@gmail.com

Prof. Dr. Mafaz Alanezi is a Cybersecurity full time professor at the University of Mosul, Iraq. She obtained her Ph.D. degree in Computer Science in the field of Computer and Network Security from University of Mosul, Iraq in 2012. Her M.Sc. degree was also in Computer Science in the field of Image Processing from the University of Mosul/ Iraq in 2003. Her research interests are in Cybersecurity, Artificial

Intelligence, Networks, Data Science and Bioinformatics.

Citation of this Article:

Kanaan J. Brakas, & Mafaz Alanezi. (2024). The Blockchain in Secure and Efficient Data Sharing: A Review. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 8(8), 62-70. Article DOI https://doi.org/10.47001/IRJIET/2024.808008

****