RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 07, Issue 04 April

Check for updates

http://dx.doi.org/10.47392/IRJASH.2025.035

Block Chain Applications in Healthcare: A Secure and Transparent Method for Data Sharing

Archana K[1], Sheela D V[2]

[1]Research scholar, School of applied science, Sapthagiri NPS university, Bangalore, Karnataka, India.

[2]Assistant professor, School of applied science, Sapthagiri NPS university, Bangalore, Karnataka, India.

Emails: *Sheela.sims.cs@gmail.com[2]*

Article history

Received: 06 March 2025
Accepted: 17 March 2025
Published: 08 April 2025

Keywords:
Block chain; Health care system; Data sharing; Data security;

Abstract

Medical data includes several patient records that are crucial for further study and therapy. To preserve the privacy of the data, it must be shared and maintained securely. Blockchain's tamper-proof and decentralised properties make it a popular choice for managing healthcare data. This research assesses blockchain from a number of angles in order to investigate its evolution in the healthcare industry. We examine blockchain-based strategies in various application contexts. These comprise blockchain and the Internet of Medical Things, blockchain-based federal learning, and blockchain-based electronic medical record sharing. These comprise blockchain and the Internet of Medical Things, blockchain-based federal learning, and blockchain-based electronic medical record sharing. The results show how naturally beneficial in the domain of medical data are tamper-proof and traceable blockchain and smart contracts. In order to propel the healthcare industry forward, the difficulties and potential paths of blockchain technology are finally examined.

1. Introduction

Blockchain technology presents notable possibilities in addressing the security-related issues and the serious challenge of massive and very varied data in healthcare systems. A digital ledger, peer-to-peer network, and distributed, decentralised database, blockchain. The blockchain may link several computers through nodes, and it doesn't require transactions to generate a new block that facilitates the safe transfer of information between individuals. The client has access to all authorized and verifiable medical data over an encrypted blockchain. Anybody can choose transactions and add new chains to the block. The hash function, which is a blockchain's master key, allows the blockchain to generate unique IDs for cryptocurrencies that include data. Security and privacy of health care data also cause other issues. For instance, patients must undergo a new examination each time they visit a different hospital for security reasons. Both money and energy are wasted by this behaviour. Medical advancement is hindered by the prohibition of sharing medical data with scientific entities to safeguard patient privacy. These have led to a search for safe ways to transmit and store data, and blockchain is popular for sharing medical data because to its decentralised and impenetrable nature[1]. Innoplexus uses blockchain technology and artificial intelligence to continuously scan life science data worldwide. Pharmaceutical businesses and research organisations receive data from the system. One platform that has been

effectively applied in practical settings is BlockRx. The platform integrates iSolve's cutting-edge digital ledger technology with blockchain technology. Medical data from research and biomedical institutions is integrated into the platform. BlockRx has advanced significantly since it was implemented in real-world applications. Stakeholders are reluctant to work together and cooperate for the exchange of health information since existing systems based on electronic health records and personal health records have not been able to handle privacy and security-related concerns. Both individuals and healthcare providers are greatly burdened by the rising expense of healthcare as a result. These days, experts and governments are looking to blockchain technology to address these trust-related issues. By developing a decentralized infrastructure for the interchange of electronic health data and enhancing healthcare management systems, blockchain is expected to significantly alter the healthcare sector, according to IBM and numerous other top healthcare organisations [2]. It is projected that the blockchain technology market would generate over USD 500 million by 2022. Despite the fact that there have been numerous studies on blockchain in the healthcare sector, the body of current literature is insufficient to paint a complete picture of the application areas. As a result, a thorough investigation of the potential uses of blockchain technology in the healthcare sector is unavoidable. With mobile devices and numerous applications, a vast amount of medical data can be created and transmitted weekly or daily in this era of internet services. The existing healthcare system can address a number of issues, including individual behavioural constraints on treatments, economic and tactical restrictions, and the need to maintain uniformity [3]. The most recent technological advancements in the supply chain aren't always utilised by healthcare system providers, nevertheless. For instance, they do not properly utilise the recently acquired and dispersed medical supplies. Indeed, according to a Healthcare Finance research, needless supply management and operations cost close to USD 25.7 billion annually.

2. Block Chain

A block chain is a decentralized node network that stores data. This technology is excellent for protecting sensitive data within the system. Important data can now be sent privately and safely because to this technology[4]. For securely storing all pertinent papers in one location, it is the perfect tool. Blockchain speeds up the process of identifying individuals who fit certain trial conditions by using a single patient database. The Blockchain is a decentralized peer-to-peer (P2P) network of individual computers, called nodes, that logs, stores, and maintains transactional or historical data. It continuously records past and present events and enables reliable collaboration because all network users store and share information. This technology can shed light on the importance of individualized care by integrating many networks. Thus, blockchain is well-known for its security and immutability. Blocks, nodes, and miners are the three main ideas of blockchain. Blockchain doesn't keep all of its data in one location. Instead, a computer network replicates and distributes the Blockchain. Figure 1 shows Block Chain Technology

Figure 1 Block Chain Technology

An immutable ledger that records data inputs in a decentralised fashion is what blockchain is. It enables communication between entities even in the absence of a central, trustworthy third party. An ever-growing collection of data entries organized into data blocks is tracked by the blockchain[5]. These blocks are linked by cryptographic protocols to both previous and subsequent blocks when they are added to the blockchain. These data records/blocks are readable, writable, and impenetrable by everyone in the original form of blockchain technology. For example, this enables

decentralised data administration and transactions. These characteristics have drawn a lot of interest in blockchain for a variety of uses[6]. Additionally, smart contracts—self-executing agreements that do not require a central authority—are made possible by blockchain. The largest blockchain smart contract facilitator at the moment is Ethereum.

2.1. Characteristics of Block Chain

Decentralisation is a fundamental feature of blockchain technology; anything posted to the blockchain is not governed by a central authority. Rather, a variety of consensus protocols are used in a peer-to-peer network to decide which entries should be sent to the blockchain. Persistence is another essential feature of blockchain technology. After an entry is accepted, it is almost impossible to remove it from the blockchain due to the distributed ledger, which is stored across multiple nodes[7]. Additionally, the potential for anonymity (or pseudonymity) is a desirable feature that is employed in numerous blockchains. By incorporating the hash of the previous block into a new block, blockchains provide audit and traceability by creating a chain of blocks. Every leaf value (transaction) in the blocks' transactions may be traced back to its known root in a Merkle tree. By just keeping the tree's root on the blockchain, this allows the tree structure to confirm the accuracy of the data.

2.2. Types of Block Chain

Blockchains are primarily categorized into three types: public (permissionless), consortium (public permissioned), and private blockchains. Every blockchain variant produces different operational features that affect accessibility together with data governance procedures and consensus procedure participation rules[8]. At present each entry in public blockchains remains clear to everybody who participates within the system. Individuals may register for the network, propose transactions, and engage in the consensus mechanism, typically employing Proof of Stake (PoS) or Proof of Work (PoW) methodologies. These blockchain systems operate without centralized authority making them the backbone of cryptocurrency technologies. The major digital currencies Bitcoin and Ethereum execute their operations through open blockchain structures without permissions. Consortium blockchain networks operate under the management of pre-specified entity nodes and organizations since these systems fall under public permissioned categories. Special entities control both network entry and the consensus procedures which form part of the blockchain access system. Consortium blockchains achieve appropriate decentralization while incorporating controlled features which enables them to serve business collaborations that involve trusted but not fully trusted participants[9]. The management and upkeep of private blockchains rests with a single entity which operates them. The systems operate under permissioned rules which limit node engagement to preauthorized entities for accessing and modifying data records. Private blockchains gain advantages from distributed blockchain architecture however they face criticism because of their centralized nature as well as limited transparency. The need for development in the healthcare industry is growing at ever-increasing rates. Contemporary medical facilities require advanced and superior technologies. In this instance, blockchain would be pivotal in transforming the healthcare sector. Moreover, the healthcare system is transitioning to a patient-centered model that prioritizes two fundamental components: consistently available healthcare resources and readily accessible treatments[10]. The arduous and repeated process of health information sharing, which inflates healthcare expenses, can be efficiently addressed by the implementation of this technology. Blockchain technology enables citizens to engage in health research initiatives. Moreover, enhanced research and data on public health will augment care for diverse populations. The entire healthcare system and its organizations are governed by a singular database. Thus far, the primary challenges in population health management have been interoperability, data sharing, and safeguarding. Blockchain technology offers a dependable resolution to this particular problem. When effectively implemented, this technology enhances security, data exchange, interoperability, integrity, and real-time updating and accessibility. Data security constitutes a significant concern, especially within the realms of wearables and personalized treatment. Blockchain technology is employed to resolve these issues, as patients and healthcare professionals want straightforward and secure methods for recording, transmitting, and accessing data across networks without concerns regarding safety.

Table 1 Overview of Block Chain Types

Property	Public Blockchain	Consortium Blockchain	Private Blockchain
Consensus Control	All network participants	A designated group of nodes	A single organization
Access to Data	Open to everyone	Public or restricted	Public or restricted
Data Alteration	Highly resistant to change	Can be modified to some extent	Can be modified to some extent
Performance	Lower efficiency	Higher efficiency	Higher efficiency
Control Structure	Fully decentralized	Partially centralized	Fully centralized
Consensus Mechanism	Open participation	Restricted participation	Restricted participation

3. Smart Contracts

Digital protocols embedded in blockchain environments execute self-executing codes which verify and enforce agreement terms between parties[11]. The automated agreements execute through blockchain environments without utilizing third-party mediators thus optimizing trust relationships while minimizing transaction expenses. After deployment smart contracts establish permanent existence as they maintain absolute transparency to permit a thorough logging of all transactions. Automatic execution powered by smart contracts performs predefined tasks autonomously thus becoming effective for secure applications that require efficiency and reliability standards. Smart contracts eliminate need for centralized control thus creating a tamper-immune system which processes decentralized transactions. Table 1 shows Overview of Block Chain Types Figure 2 shows Smart Contracts

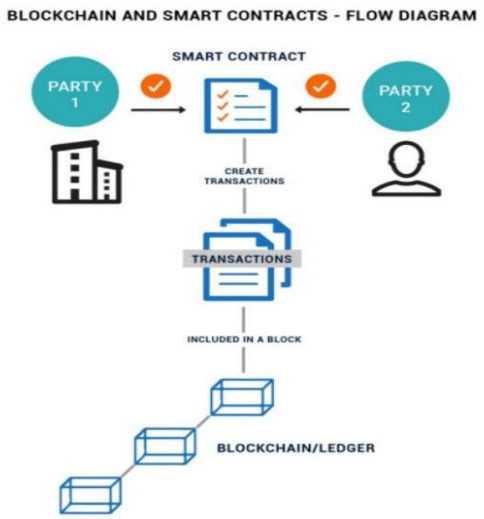

Figure 2 Smart Contracts

4. Review Analysis

4.1. Storage and Data Security by Block Chain Technology

The utilization of blockchain technology serves diverse medical data exchange needs which has resulted in three distinct types developed from different application situations. Grid Access Storage is the first blockchain application for data protection and access. Together with IOMT exists the second model of IOMT and blockchain integration. The third use of blockchain technology involves its implementation as a replacement for the federal learning center. Healthcare data management improved substantially with Electronic Medical Records (EMRs) but this advancement introduced new privacy and security concerns to patient data. Medical information sharing without restrictions remains dangerous because centralized systems have naturally occurring weak points. Blockchains have inspired multiple propositions for decentralized frameworks which boost data privacy safeguards while keeping data integrity intact[12]. Medichain represents a standout blockchain model that uses blockchain tracing mechanisms to store fully detailed patient medical histories. Records in the system undergo hashing before the generated hash values rest in Merkle trees to both guarantee data preservation and protect healthcare data from unauthorized modifications thus reducing clinical errors during treatment. In addition to supporting various data formats and sources medical data is integrated into a ‘hyperfield’ which simplifies storage across the blockchain architecture. The innovative system design encounters two fundamental issues regarding scalable storage

costs and data storage within the blockchain infrastructure[13].The research of Wu delivered a privacy-protecting access control system for health care operations which prioritizes patient privacy. The secure information storage platform depends on blockchain technology while standard cryptographic algorithms secure data transmission between systems. Security of privacy information relies on file authorization contracts. Through fine-grained access control the model provides separate access permissions for users based on their role assignment. Healthcare institutions store their EMR data in cloud databases which third-party service providers operate together with blockchain-stored hash values. The chain enables hash value comparison which detects unauthorized modifications in cloud-stored data. The implemented consensus algorithm named Proof of Work (PoW) operates at high computational cost together with low efficiency[14]. The authors [15] established a blockchain model with proxy re-encryption capabilities which enables secure medical information exchange between different healthcare facilities. Data integrity is maintained by collision-resistant hash functions and security increases because of an upgraded delegated Proof-of-Stake (DPoS) consensus algorithm. The system operates through a special disease-matching functionality which enables authenticated users to establish information sharing connections with others who share their medical condition. Private blockchains in this model provide quick transaction processing yet reduce the decentralization capability that prevents their widespread use within extensive healthcare systems such as networks (Farouk et al., 2020). Yu et al. proposed a hybrid framework combining decentralized chains to manage sensitive EMR data integrated through the shared and private (federated) aspect of the chain together with public chain non-sensitive information storage to balance privacy and scalability needs. Medical researchers along with institutions have public-record access to conduct studies and make institutional advancements through a system run by licensed users. The storage system follows an off-chain approach by storing data hashes on the blockchain while maintaining data integrity through this method. Smart contracts implement automation to handle patient data requests together with approvals and usage procedures. Despite its innovation, the model employs coarse-grained access control, lacking attribute-based differentiation. [16] present a blockchain structure which addresses fork in the chain issues and implements a trust-based consensus method that combats Byzantine faults. Healthcare institutions obtain trust points from sustaining mining operations to eventually acquire access to electronic medical records. The reputation-based system uses many processing assets which leads to elevated energy usage.

4.2. Block Chain Integration with the Internet of Medical Things (IOMT)

Physiological data collection for patient examination in real time happens through the connected medical devices network known as the Internet of Medical Things (IoMT). The technology improves disease control through early warning of abnormal health indicators which enables doctors to provide prompt medical assistance [17]. The IoMT environment has numerous clinical benefits however it faces major security threats because medical devices lack unified regulatory standards. Blockchain technology brings an effective resolution to security issues through its decentralized management system which protects sensitive health data from IoMT devices. Blockchain implements data integrity protocols and encryption tools with smart contracts through its features to provide IoMT ecosystems with enhanced transparency and privacy [18]. Figure 3 shows Block Chain Integration with the Internet of Medical Things (IOMT)

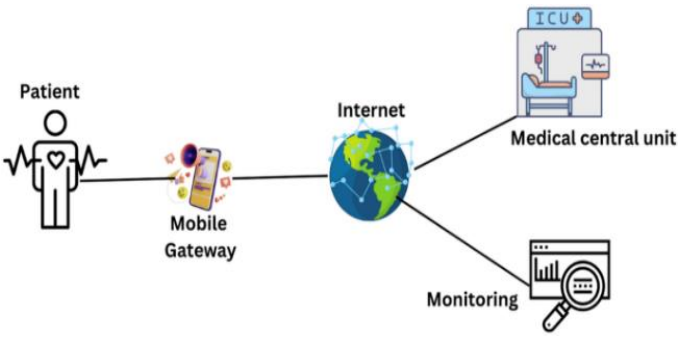

Figure 3 Block Chain Integration with the Internet of Medical Things (IOMT)

4.3. Block Chain in Medical Federated Learning

The efficacy of data-driven machine learning is hindered by healthcare data privacy. Federated

learning is an innovative artificial intelligence approach that protects data privacy in the creation of AI models. Federated learning enables collaborative model training across numerous nodes, transmitting only gradients and losses instead of the actual data. This method is efficient in protecting the data [19]. Nonetheless, the data must be relayed by the nodes to the central institution for additional computation. Blockchain technology can supplant the central institution, so alleviating the dishonesty inherent in the central framework. Table 2 shows Comparison Table of Methods in Review

Table 2 Comparison Table of Methods in Review

S. No.	Authors	Title	Source	Year	Key Contributions
1	McGhin, Choo, Liu, He	Blockchain in Healthcare Applications: Research Challenges and Opportunities	J. Netw. Comput. Appl., 135	2019	Comprehensive review of blockchain's role in healthcare, discussing challenges, opportunities, and future directions. Highlights issues related to scalability, interoperability, and privacy.
2	Yue, Wang, Jin, Li, Jiang	Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control	J. Med. Syst., 40(10)	2016	Introduces a privacy-risk control model using blockchain to enable intelligent healthcare data gateways with enhanced privacy.
3	Hölbl, Kompara, Kamišalić, Nemec Zlatolas	A Systematic Review of the Use of Blockchain in Healthcare	Symmetry, 10(10)	2018	Systematic review of existing blockchain applications in healthcare; categorizes applications based on data sharing, access control, and interoperability.
4	Farouk, Alahmadi, Ghose, Mashatan	Blockchain Platform for Industrial Healthcare: Vision and Future Opportunities	Comput. Commun., 154	2020	Proposes a blockchain framework tailored for industrial healthcare use with secure access and data provenance features. Discusses vision and technical gaps.
5	Ekblaw, Azaria, Halamka, Lippman	MedRec: A Case Study for Blockchain in Healthcare	IEEE Open & Big Data Conf., Vol. 13	2016	Presents "MedRec", a blockchain prototype for managing EMRs and research data using smart contracts for access control and auditing.
6	Dhillon, Metcalf, Hooper	Blockchain in Healthcare	Blockchain-enabled Applications, Apress	2021	Discusses practical use cases, implementation strategies, and industry-specific blockchain adoption in healthcare settings.
7	Dimitrov	Blockchain Applications for Healthcare Data Management	Healthcare Informatics Research, 25(1)	2019	Explores blockchain's potential in enhancing security, privacy, and patient empowerment in healthcare data management.

The blockchain supplants the central gradient aggregator. The hash of the encrypted global model is stored in the blockchain for subsequent sharing after aggregation is completed. Malicious FL nodes may introduce toxic models, thereby biasing the training data. A monitoring system is established to verify the legitimacy and history of the training process. Malicious nodes can be identified. The reputation score can be utilized to reduce the quantity of malicious nodes. An optimal situation involves the exchange of computational resources and data among nodes; however, achieving this in practice is fraught with difficulties. Because the computational capacity and data among nodes are not uniform. Achieving consensus among unprofitable nodes is tough. Distributing tokens based on the workload of nodes is more egalitarian. The authors propose a unique, entirely decentralized healthcare architecture. The blockchain and MEC-based technology is utilized to enable the sharing of distributed EMR among federal institutions. A novel decentralized electronic medical record (EMR) storage system was created using multi-access edge computing (MEC) servers, leveraging the InterPlanetary File System (IPFS) framework to enable EMR sharing. A blockchain-based smart contract was utilized to create an access authentication method that verifies access at the network's peripheral without requiring a central authority. During each iteration of the consensus phase, a restricted number of miners are selected for Byzantine protocol validation. This strategy reduces overhead but increases the risk of an assault [20]. The authors propose a blockchain-based system for smart healthcare utilizing federated learning. This model governs the entire training process. An adaptive differential privacy technique is proposed to augment FL's security. Figure 4 shows Federated Learning in Healthcare

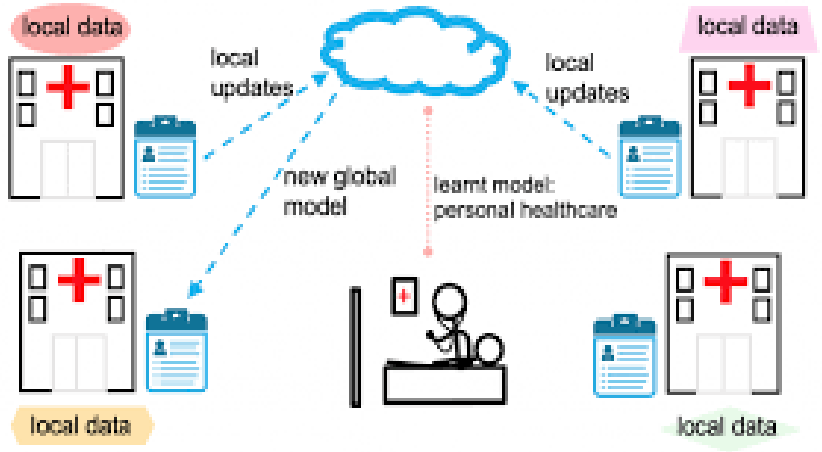

Figure 4 Federated Learning in Healthcare

Conclusion

The aim of this study was to perform a thorough assessment, survey, and classification of relevant research publications on blockchain and its integration into various healthcare applications. The study also sought to identify specific literary patterns. The distribution of blockchain platforms and the diverse sorts of blockchain methodologies utilized or suggested in the analyzed articles were evaluated. The blockchain platform facilitates the development of decentralized apps where data transmission patterns are not governed by any third-party entity. The data transactions of the entities are recorded in a decentralized database in a verifiable, secure, immutable, and transparent way, accompanied by a timestamp and other pertinent information. This paper provides a concise

overview of three healthcare data sharing application scenarios and contrasts them with conventional methods. The blockchain-based model is more intelligent and secure than the traditional cryptography-based model due to the significant role of smart contracts. Nevertheless, blockchain technology is experiencing a variety of challenges, such as inadequate scalability and low throughput. The development of blockchain in healthcare data exchange has been restricted by these factors. Sharding, cross-chain, and consensus algorithms are technologies that require attention in the future.

References

[1]. Chanchaichujit, J., Tan, A., Meng, F., & Eaimkhong, S. (2019). Blockchain technology in healthcare. In Healthcare 4.0 (pp. 37–62). Palgrave Pivot, Singapore.

[2]. Chelladurai, U., & Pandian, S. (2021). A novel blockchain-based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing.

[3]. Dhillon, V., Metcalf, D., & Hooper, M. (2021). Blockchain in healthcare. In Blockchain-enabled Applications (pp. 201–220). Apress, Berkeley, CA.

[4]. Dimitrov, D.V. (2019). Blockchain applications for healthcare data management. Healthcare Informatics Research, 25(1), 51.

[5]. Ekblaw, A., Azaria, A., Halamka, J.D., & Lippman, A. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In IEEE Open & Big Data Conference, Vol. 13, p. 13.

[6]. Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications, 154, 223–235.

[7]. Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470.

[8]. Kassab, M.H., DeFranco, J., Malas, T., Destefanis, G., & Neto, V.V. (2019). Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Transactions on Emerging Topics in Computing, 1–1.

[9]. Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences, 9(9), 1736.

[10]. Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., & Ylianttila, M. (2018). Blockchain utilization in healthcare: Key requirements and challenges. In 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom), pp. 1–7.

[11]. Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5.

[12]. McGhin, T., Choo, K.K.R., Liu, C.Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62–75.

[13]. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), pp. 1–3.

[14]. Moona, G., Jewariya, M., & Sharma, R. (2019). Relevance of dimensional metrology in manufacturing industries. MAPAN, 34, 97–104. https:// doi.org /10.1007/s12647-018-0291-3

[15]. Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing

via blockchain. Applied Sciences, 9(6), 1207.

[16]. Tripathi, G., Ahad, M.A., & Paiva, S. (2020). S2HS – A blockchain-based approach for smart healthcare system. Healthcare, 8, 100391.

[17]. Varshney, A., Garg, N., Nagla, K.S., et al. (2021). Challenges in sensors technology for Industry 4.0 for futuristic metrological applications. MAPAN, 36, 215–226. https://doi.org/10.1007/s12647-021-00453-1

[18]. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Computing and Applications, 1–6.

[19]. ue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 1–8.

[20]. Zhang, P., Schmidt, D.C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In Advances in Computers, Vol. 111, pp. 1–41. Elsevier.