Performance Analysis of a Hyperledger-Based Medical Record Data Management Using Amazon Web Services

Mohammed K Elghoul[1*], Sayed F. Bahgat[2], Ashraf S. Hussein[3], Safwat H. Hamad[4]
Scientific Computing Department, Faculty of Computer and Information Sciences, Ain-Shams University, Egypt[1, 2, 3, 4]
King Salman International University, South Sinai, Egypt[3]
Saint Mary's College of California, Moraga CA 94575, USA[4]

***Abstract*—Recently, there's been growing excitement around the innovative capabilities of blockchain technology, especially for enhancing security, privacy, and transparency. Its application in various sectors, like finance and logistics, is intriguing, but its potential in healthcare stands out. Specifically, in the realm of medical data management, blockchain can transform how we protect patient data. Our study unveils a cutting-edge approach to handle digital health records by harnessing the power of Amazon Web Services (AWS). This pioneering, serverless model is not only cost-effective, with charges only for used resources, but also offers heightened security and for blockchain network access. We build a private, permissioned blockchain network with Hyperledger Fabric to control access while ensuring transparency. The paper demonstrates the prowess of this new system is validated through rigorous tests on speed, network prowess, and multi-user handling, complete with a detailed cost analysis for implementation. The paper further demonstrates the use of the Gatling open-source library to design various experiments for performance measurement.**

Keywords*—Hyperledger; blockchain; healthcare; data management

I. Introduction

Distributed ledger technology, commonly referred to as blockchain, facilitates the sharing of data between peer-to-peer networks [1]. Its first application was seen in 2008 with the Bitcoin cryptocurrency [2]. The main appeal of blockchain is its low cost, speed, improved security, and direct peer-to-peer transactions without relying on a central third party.

In today's technological age, the increasing reliance on accurate data calls for new methods of storing and analyzing information. Ensuring that data is immutable, secure, and maintains its integrity has become an important part of modern systems. Especially since the implementation of Bitcoin in 2008, blockchain has stood out as an emerging solution [3]. The rapid growth of medical data [2] coupled with the rise of blockchain suggests the need for a new framework. As electronic medical records (EMRs) increase in size and scope [4], modern systems struggle to keep up. Maintaining and securing EMR data is essential, especially given the fragility of patient information and the complexity of sharing such information across locations, and traditional databases often fail to meet these challenges accurate [5]. Moreover, the integration of blockchain technology could offer a robust solution to these issues, providing a decentralized, secure, and transparent platform for managing and sharing EMR data.

Considering blockchain's inherent properties such as data immutability, decentralized ledger, and strong security, it appears to be a powerful solution for EMR management [6]. The immutable and transparent nature of blockchain ensures that once data is stored, it remains untouched [7]. This could significantly reduce the risks of data tampering and unauthorized access, which are common concerns in traditional EMR systems.

Four key characteristics define blockchain: decentralization, immutability, audibility and traceability, and data integrity. This ensures that any transactions or records on the network remain unchanged [8]. Blockchain operates without a central governing body, instead using consensus mechanisms to support data and network peers. Correlations are verified using a Merkle tree-like structure [9], which supports data integrity.

There are basically three types of blockchain: public, federated, and private. Like Bitcoin and Ethereum, public versions are open source. In contrast, confederation block chains limit access to a particular group, and although they are confined to private blocks, they are managed by a single entity. Given the breadth of blockchain applications, there is rarely a universal definition. Table I provides an in-depth comparison of these three types.

This paper explores a comprehensive review of a cloud-centric approach to securing data management systems through blockchain technology, specifically through AWS. The article begins with an overview that emphasizes the need to address security challenges in EMRs. The paper then describes the proposed system architecture, clarifies external components such as the Hyperledger blockchain grid, and specific AWS applications. Additionally, a diagram of the sequence of reactions is provided. Reinforcing the background, the paper presents an experimental performance measure of the system.

In conclusion, the paper recounts his major publications and contributions. In the final sections, it discusses the development of the system and potential efficiencies, demonstrating a progressive research focus and the ability to continuously refine and modernize the system.

*Corresponding Author.

TABLE I. TYPES OF BLOCKCHAINS [2], [9]

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

II. RELATED WORK

Asma Khatoon [10] investigated in detail the integration of blockchain-enabled smart contracts in the healthcare industry. His proposal includes a medical system built on smart contracts and blockchain, demonstrating the benefits of decentralization for healthcare services. Key objectives include reducing transaction costs, streamlining administrative tasks, and bypassing intermediaries.

MedChain, a blockchain system designed for the privacy of medical data, was introduced by Daraghmi et al. [11]. Their platform provides patients, healthcare providers and those who value patient privacy with reliable health records. Short-term smart contracts, with sophisticated encryption, are used to manage transactions and promote data security. Additionally, it is recommended that incentives be developed for health professionals to maintain and develop updates.

Through their research, Zhang et al. [12] examined the synergies between blockchain and smart contracts in healthcare, highlighting its effectiveness in solving many healthcare challenges. Furthermore, they shed light on the obstacles faced when integrating blockchain into healthcare.

Kumar and his team [13] examined various applications of blockchain in the healthcare system. They acknowledge the barriers to integration but point to smart contracts as a logical solution in a blockchain-based healthcare system.

Sial and others [14] highlighted the benefits of integrating blockchain with smart contracts to improve healthcare services. They point to blockchain's ability to prevent loss and prevent data manipulation by storing data safely on a ledger. The potential of Hyperledger Fabric for storing medical records was the focus of Daisuke et al. [15], who aimed to transfer medical data from smartphones to the Hyperledger blockchain system.

Aiming to address the obstacles of a permissive and open blockchain system, Rouhani and his team [16] turned to a Hyperledger system to empower patients with suggestive autonomy of their health data to develop a new system developed by Sukhpal Gill [17] to enable cloud maintenance, serverless, Combining quantum computing and blockchain, the management layer covered the IoT devices in a service layer that manages resources and communicates with IoT devices, while the service side performs computing tasks through Serverless FaaS architecture.

Bhati et al. [18] supported the adoption of blockchain in healthcare, especially in the management of EHRs. Their goal was to increase the accessibility and relevance of EHRs by leveraging blockchain's improved security, with the introduction of streamlined access guidelines. Their design also includes external data storage to address scalability issues, ensuring security, and flexibility.

Finally, Anurag and his team [19] compiled the literature on its role in healthcare and delved into the potential of blockchain to manage healthcare intelligence.

A. Blockchain Technology Limitations

When it comes to storing large amounts of data, blockchain faces two important challenges: scalability and privacy. The data stored on the blockchain is visible to all authorized users, which could be a concern for healthcare organizations that need to store sensitive patient information. Additionally, storing a patient's complete medical history, records, visits, lab results, and other reports in the blockchain can cause significant strain on its storage [20].

Blockchain technology is still not fully understood by many, as it is a relatively new field and is constantly evolving. This lack of knowledge and understanding can complicate the adoption of blockchain in healthcare. Additionally, the transition from traditional EHR systems to blockchain will require significant effort, as hospitals and healthcare organizations need to change their systems to take advantage of this new technology.

As blockchain technology is still relatively new and evolving rapidly, there is no established standard for it. This means that implementation in the healthcare industry requires additional time and effort. To ensure the safe and secure use of blockchain, international authorities should develop standardized guidelines to assist in the standardization of this technology.

III. PROPOSED SOLUTION

A. Implementation

Fig. 1 illustrates the system architecture diagram, illustrating the use of the Hyperledger blockchain network for storing and processing medical records.

Each participant in this network operates through a unique client application, which connects them to the blockchain and allows them to access medical data.

Member A, who is the embodiment of the patient only has the right to view his/her own medical history and other ability to change his/her address information On the other hand, member B which refers to the health reputation has the right to do detailed medical information and edits for individual or multiple patients and may also include patient access instructions Conversely, Member C on behalf of the regulatory agency may request and select records a can be adopted for research purposes.

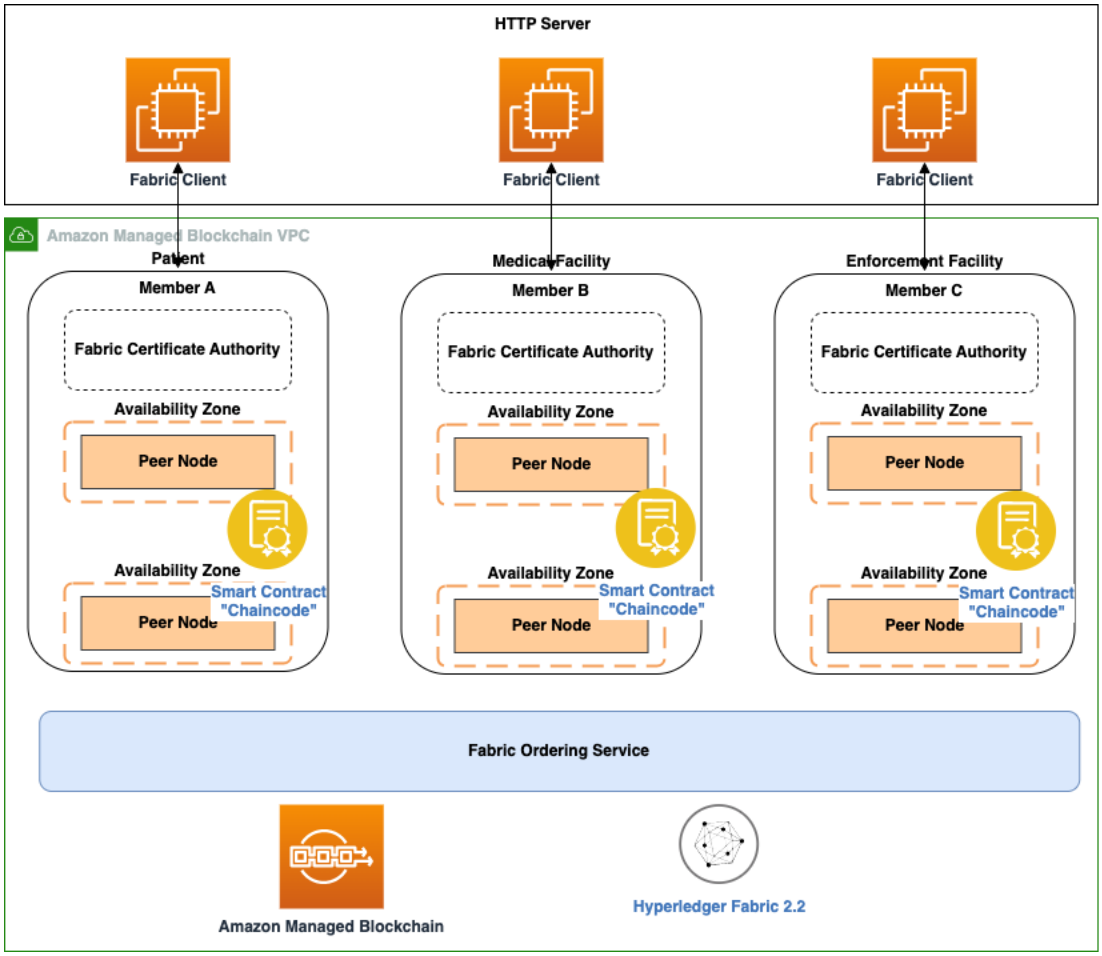

Fig. 1. High level system architecture diagram [21].

Arvind et al. [20] utilized IBM cloud and Kubernetes containers to execute their approach. In contrast, our suggested method employs Amazon Web Services (AWS) and the principle of serverless computing. This strategy allows us to avoid paying for inactive resources and offers the flexibility to adjust our scale according to traffic demands. As we will observe in the results section, this results in substantial performance improvements.

Integrating ownership and authorization protocols is key to maintaining the purity and resilience of the Hyperledger blockchain network. This ensures that only authenticated users can access it, thus protecting the network from inappropriate access or threats. Authentication focuses on supporting the identity of the user or device, while authorization is about defining what activities are allowed for a user or device in the network Using these safeguards reduces the chance of a there is greater access to unauthorized networks or potential security breaches.

In the described Hyperledger framework, authentication and authorization are seamlessly integrated into the client software. As a result, the specific client applications used by network participants come equipped with built-in mechanisms to authenticate and direct users, enabling secure and regulated transactions with the blockchain.

The infrastructural layer of our Hyperledger network is built on the Amazon Managed Blockchain, essentially following version 2.2 of the framework. Notably, Amazon Web Services (AWS) provides two different versions of the said network: 'Starter' and 'Standard'. Given the budget constraints, our decision wanted to utilize the capabilities of the 'starter' version.

TABLE II. MACHINE TYPES SUPPORTED BY AMAZON MANAGED BLOCKCHAIN STARTER EDITION

Machine Type	Member cost	Peer node	Hourly cost	Daily cost
bc.t3.small	$0.30	$0.034	$0.334	$8.0
bc.t3.medium	$0.30	$0.067	$0.367	$8.8

Delving into the specifics, "Table II", enumerates the varies of current compatible device configurations, providing a comparative analysis of their economic implications for general understanding, consider a hypothetical scenario of a network composed of three member groups. The table describes the total cost of this three-member network and breaks down the hourly computation costs for each member next to a peer node It should be noted that a maximum storage

fee of $.20 is charged on, and writing work the cost matrix of this amount is directly proportional to the requirement of identical nodes on the monthly cadence.

B. Sequence Diagram and Transaction Flow

Extending the complexity of the transaction process within our blockchain framework, “Fig. 2”, presents a complete sequence of diagrams describing the entire course of a transaction [21]. This diagram carefully describes a multifaceted level integral to the progress of a transaction. Starting at the point of user interaction, the sequence flows normally, through each level, and finally ends up in the Hyperledger system's integral sequence annotation services once processed in Hyperledger, the feedback reconfigures a route, which reaches the user to the destination. Through this approach, a comprehensive understanding of the complex behavioral journey is gained by emphasizing the interactions between each level within the larger behavioral ecosystem.

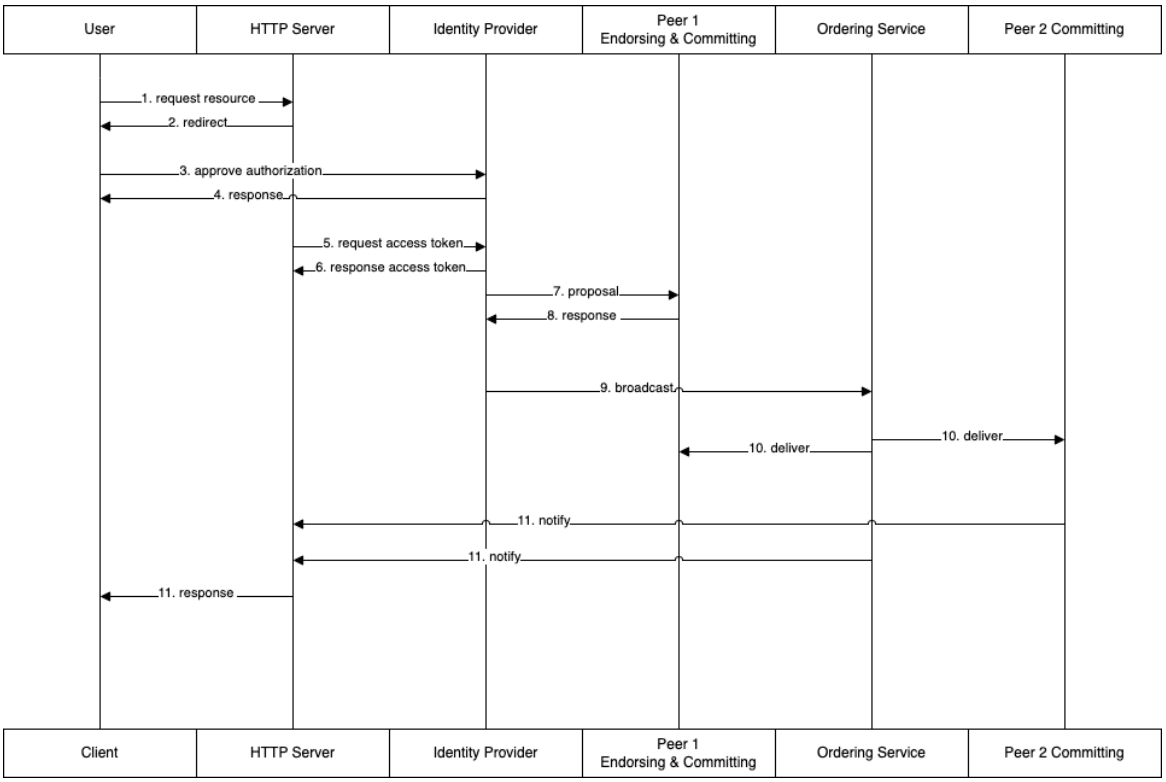

Fig. 2. Transaction flow and sequence diagram.

HTTP and License Phases When a user initiates a request to the server, the server immediately checks the user's license credentials. Based on this authentication, the server grants access or denies the user’s request. If the user credentials meet the required criteria and are considered valid, the server proceeds to communicate with the identity provider, requesting a token. After, the token and user request have been successfully received and validated, the server with the installed Fabric SDK carefully builds a transaction offer, ensuring that the appropriate certificate is included for authentication.

Detailed Steps

1. Initiation by the User
   a. The user sends a request to the server.
   b. The request is routed to a specific function based on the provided URI and HTTP method.
   c. The user embeds a valid token within the request header for authentication and authorization.
2. Token Verification
   a. The system verifies the validity of the embedded token.
   b. If the token is invalid or absent, the user is redirected to a login page.
3. Credential Input and Validation
   a. The user enters their authentication credentials on the login page.
   b. The credentials are validated.
4. Communication with Identity Provider

   A response is generated from the identity provider after validation.
5. Token Request by Server

   The server requests a token from the identity provider.
6. Token Receipt

   The identity provider issues a valid token for the ongoing request.
7. Transaction Proposal and Invocation

a. A transaction proposal is created using the Fabric SDK on the server.
b. The proposal is signed with the correct certificate and sent as an invoke request to the network.

Endorsement Phase

8. Endorser Verification
   a. The endorsing peer verifies that the client is authorized to invoke the chaincode.
   b. If authorized, the endorsing peer executes the chaincode and generates a response without changing the world state.
   c. The endorser signs the proposal with its identity and sends it to the client.
9. Endorsement Collection
   a. The client collects responses from multiple endorsers.
   b. The client verifies that the responses satisfy the endorsement policy.

Ordering Phase

10. Transaction Broadcast: The client broadcasts the endorsed transaction to the ordering service.
11. Block Creation
    a. The ordering service packages the transactions into blocks.
    b. The ordering service signs the blocks.
12. Block Delivery: The ordering service delivers the blocks to the leading peer nodes.

Validation & Committing Phase

13. Block Dissemination: The leading peers disseminate the blocks to all peers in the same channel and organization.
14. Block Verification: The peers verify the signature of the blocks.
15. Transaction Validation: The peers check all the transactions within the blocks.
16. Ledger Update: If all the transactions are valid, the blocks are appended to the ledger and the world state is updated.

Response Phase

17. Event Notification: The HTTP server is notified via the Channel EventHub listener once the target transaction has been committed to the ledger.
18. Response Formation:
    a. A registered callback function collects details of the event.
    b. The callback function forms a response in JSON format using the collected details.
19. Response Delivery: The response is sent back to the user via the client application.

C. Challenges and Limitations

Data migration poses a significant challenge in migrating existing medical records to blockchain-based systems due to format and data type compatibility issues. Careful design with data washing and validation process various uses are paramount to ensure a smooth and accurate transfer while maintaining data integrity and security Compliance with regulatory frameworks Not a trivial matter. The proposed system should not only leverage the advantages of blockchain technology but also strictly comply with these regulations.

User adoption depends on the active involvement of multiple stakeholders, including health care providers, patients, and regulatory agencies. Getting these organizations to thrive in the new system and ensure they are profitable is a difficult task. In terms of security and scalability, it is important to enforce strict security measures, especially when dealing with medical data. New systems should take full advantage of blockchain's inherent security features and add components when needed. It should also demonstrate adaptability to meet the growing demand for health care. From an economic perspective, setting up and maintaining a blockchain-related system to manage healthcare data can be expensive, considering ongoing infrastructure, development and operational costs. If designed such a wonderful implementation, will require skilled professionals with expertise in blockchain technology, security, and data management.

IV. Results and Discussions

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

In this section, we examine the results of our experiments and subsequent performance implications. Our test revolved around a sample dataset focused on the patient's medical record. We used the open-source Gatling library to facilitate these tests. This tool allowed us to perform simultaneous tasks, specifically designed to create, retrieve, modify, and purchase patient records. Test automation and quality assurance play an important role in monitoring test results because they reduce human effort and cost and improve the accuracy of results.

For our test parameters, we started with a modest ten users working simultaneously. Gradually we increased this, aiming for 2000 users, all within a short period of 100 seconds. Such a configuration has given us the ability to test our system, so that it serves 20 users at once, each performing one task.

The following images offer insights directly from Gatling. "Fig. 3", describes the sum of responses required to complete each request and the corresponding duration. Remarkably, not a single request experienced a failure, with each task taking just over 1.2 seconds to complete. Turning to "Fig. 4", it shows the flow of active users throughout the test phase, with a noticeable upward trend, rising to 1,706 users in a joint What last, "Fig. 5", provides a granular representation of the response time distribution, which shows how long the server needs to return a response.

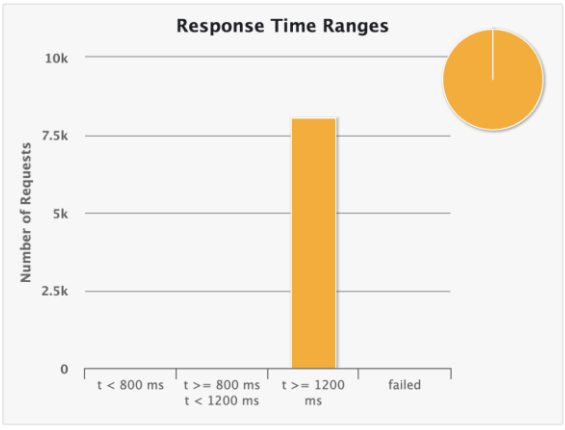

Fig. 3. Response time range and number of requests.

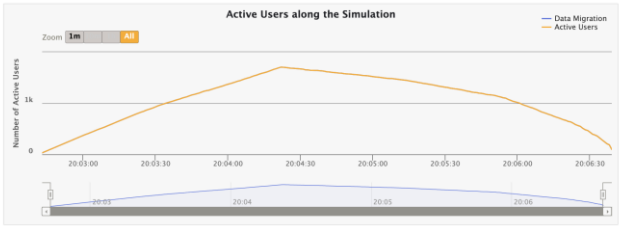

Fig. 4. Active users timeline.

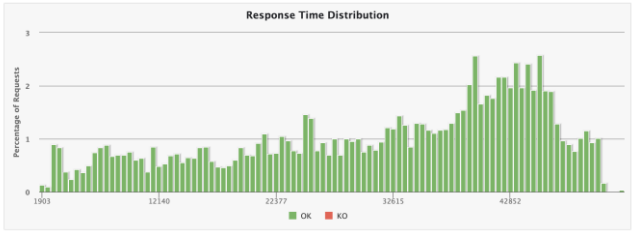

Fig. 5. Response time distribution.

The findings showed that the introduced solutions are efficient and mature in handling the requirements in real-world situations. What sets this platform apart is the efficient use of Amazon web services.

V. Conclusions and Future Work

This research presents a cloud-based approach, for storing and retrieving medical records on the Hyperledger blockchain network. We were able to transfer a volume of historical data consisting of approximately five million records and demonstrated that our system can handle daily traffic effectively. By utilizing the edition of Amazon Managed Blockchain, our solution seamlessly integrates with AWS ensuring adaptability for future data analysis. To ensure accuracy and efficiency we implemented testing with Gatling scripts to assess performance. Not does our system provide storage and analysis capabilities but it also paves the way for further advancements such, as integrating emerging technologies and enhancing security measures. This direction emphasizes how our system can adapt to the evolving demands of healthcare data management.

References

[1] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," Symmetry (Basel), vol. 10, no. 10, p. 470, Oct. 2018, doi: 10.3390/sym10100470.

[2] M. Elghoul, S. Bahgat, A. Hussein, and S. Hamad, "A Review of Leveraging Blockchain based Framework Landscape in Healthcare Systems," International Journal of Intelligent Computing and Information Sciences, vol. 0, no. 0, pp. 1–13, Oct. 2021, doi: 10.21608/ijicis.2021.75531.1095.

[3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.

[4] M. K. Elghoul, S. F. Bahgat, A. S. Hussein, and S. H. Hamad, "Securing Patient Medical Records with Blockchain Technology in Cloud-based Healthcare Systems," International Journal of Advanced Computer Science and Applications, vol. 14, no. 11, 2023, doi: 10.14569/IJACSA.2023.0141133.

[5] T. Benil and J. Jasper, "Cloud based security on outsourcing using blockchain in E-health systems," Computer Networks, vol. 178, p. 107344, Sep. 2020, doi: 10.1016/j.comnet.2020.107344.

[6] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," Healthcare, vol. 7, no. 2, p. 56, Apr. 2019, doi: 10.3390/healthcare7020056.

[7] A. Ali et al., "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography," Sensors, vol. 22, no. 2, p. 528, Jan. 2022, doi: 10.3390/s22020528.

[8] M. K. Elghoul, S. F. Bahgat, A. S. Hussein, and S. H. Hamad, "Secured Cloud-based Framework for Electronic Medical Records using Hyperledger Blockchain Network," Egyptian Computer Science Journal, vol. 46, no. 2, Sep. 2022.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[10] A. Khatoon, "A Blockchain-Based Smart Contract System for Healthcare Management," Electronics (Basel), vol. 9, no. 1, p. 94, Jan. 2020, doi: 10.3390/electronics9010094.

[11] E.-Y. Daraghmi, Y.-A. Daraghmi, and S.-M. Yuan, "MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management," IEEE Access, vol. 7, pp. 164595–164613, 2019, doi: 10.1109/ACCESS.2019.2952942.

[12] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Design of Blockchain-Based Apps Using Familiar Software Patterns with a Healthcare Focus," in Proceedings of the 24th Conference on Pattern Languages of Programs, in PLoP '17. USA: The Hillside Group, 2017.

[13] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, Sep. 2018, pp. 1–7. doi: 10.1109/HealthCom.2018.8531136.

[14] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," Cryptography, vol. 3, no. 1, p. 3, Jan. 2019, doi: 10.3390/cryptography3010003.

[15] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-Resistant Mobile Health Using Blockchain Technology," JMIR Mhealth Uhealth, vol. 5, no. 7, p. e111, Jul. 2017, doi: 10.2196/mhealth.7938.

[16] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery, and R. Deters, "MediChainTM: A Secure Decentralized Medical Data Asset Management System," Jan. 2019, doi: 10.1109/Cybermatics_2018.2018.00258.

[17] S. S. Gill, "Quantum and blockchain based Serverless edge computing: A vision, model, new trends and future directions," Internet Technology Letters, Feb. 2021, doi: 10.1002/itl2.275.

[18] N. S. Bhati, M. Khari, V. García-Díaz, and E. Verdú, "A Review on Intrusion Detection Systems and Techniques," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 28, no. Supp02, pp. 65–91, Dec. 2020, doi: 10.1142/S0218488520400140.

[19] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Implementing Blockchains for Efficient Health Care: Systematic Review," J Med Internet Res, vol. 21, no. 2, p. e12439, Feb. 2019, doi: 10.2196/12439.

[20] A. Panwar, V. Bhatnagar, M. Khari, A. W. Salehi, and G. Gupta, "A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake," Comput Intell Neurosci, vol. 2022, pp. 1–19, Apr. 2022, doi: 10.1155/2022/3045107.

[21] P. Yuan, K. Zheng, X. Xiong, K. Zhang, and L. Lei, "Performance modeling and analysis of a Hyperledger-based system using GSPN," Comput Commun, vol. 153, pp. 117–124, Mar. 2020, doi: 10.1016/j.comcom.2020.01.073.