International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-1, December 2022

Leveraging Blockchain-Based Electronic Health Record Systems in Healthcare 4.0

Manish Shashi

Abstract: ***Digitalization has become a crucial part of healthcare 4.0 by transforming systems such as electronic health records (EHR), electronic medical records (EMR), and electronic personal medical records (ePHR). Healthcare 4.0 is derived from industry 4.0 and aims to enhance collaboration, virtualization, coherence, and convergence, which helps transform modern healthcare into more personalized and predictive. Healthcare 4.0 also aims to develop digital enablers which will support coordination among various stakeholders and seamless information flow in the patient journey towards wellbeing. These systems enhance patient care through the timely sharing of patient data across different providers globally. Timely sharing helps, but it also makes the electronic system vulnerable to alteration and breaches. In healthcare, blockchain application is widely used in various areas, such as health information exchange, pharmaceutical counterfeit, clinical trials, health supply chain management, patient data management, insurance claims, and product recall in case of adverse events. This research paper aims to identify how blockchain technology can help enhance the privacy and security of electronic health record systems. This paper discusses various blockchain-based systems, which provide a more efficient and secure option than client-server architecture-based traditional EHR systems.***

Keywords: Healthcare, Digitalization, EHR, Blockchain, Sustainability.

I. INTRODUCTION

Healthcare 4.0 is derived from industry 4.0. Various digital enablers, such as cloud computing, machine learning, and artificial intelligence, were used to build the blockchain-based system to support real-time access to patient's clinical data. Industry 4.0 represents the industrial revolution and aims to integrate the physical system with information, process, and operational technology.

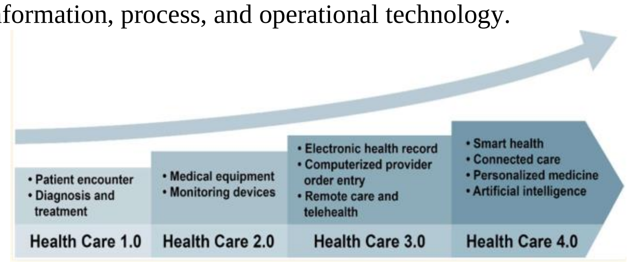

Fig. 1. Evolution of health care system (Li & Carayon, 2021) [7].

Manuscript received on 15 November 2022 | Revised Manuscript received on 18 November 2022 | Manuscript Accepted on 15 December 2022 | Manuscript published on 30 December 2022.
***** Correspondence Author
Dr. Manish Shashi*, College of Management, Walden University, Minneapolis, MN, USA. Email: manish.shashi@gmail.com

As depicted in fig.1, plenty of research and development work were already done in healthcare 3.0 pertaining to digitalization of EHR. Healthcare 4.0 is more like optimizing the effort and bringing humans, including patients, providers, and third parties such as clinics, insurance, and pharmacies, to the center of smart and connected healthcare. It is critical to consider their characteristics, abilities, needs, and constraints while designing and implementing interconnected and smart healthcare systems [7].

An electronic health record (EHR) contains the results of clinical and administrative encounters between a provider (physician, nurse, telephone triage nurse, and others) and a patient that occur during episodes of patient care [11]. Physicians can make prompt, smarter, and more efficient decisions with informed knowledge of a patient's health history, such as previous diagnoses, treatments, and tests. It will also be cost-effective and may save the cost of repeated tests and maximize the value of services delivered to patients. Most medical data transmission is still through mail or fax due to the lack of trusted and secure infrastructure and the mandatory requirement of privacy and sensitivity.

Security and privacy are the utmost critical factors in healthcare. Privacy refers to persons having the right to allow or disclose personal information to others, forcing providers and authorities to create agreed policies and procedures [16]. EHR can be utilized and maliciously exploited in two different ways. External agents like marketers can exploit patients' data for malicious purposes. EHR can also help make or break a diagnosis, such as avoiding injecting any substance a patient is allergic to. Safeguarding privacy includes access control of patients' information, security of patient data from unauthorized users, and the modification and destruction of stored data [16].

Blockchain holds great promise in healthcare and is believed to have more potential applications than any industry besides the financial industry. Blockchain is a list of records linked together using cryptography, a secure communication technique that allows only the sender and intended recipient of a message to view its contents [3]. Each block is unique, consisting of a specific algorithm of the previous block, transaction data, and timestamp [15]. Because a block is a byproduct of the previous block, data cannot be modified, allowing transactions to be recorded factually and with better security [15]. Blockchain allows users to have complete control of data and privacy without a central point of control, thus making it highly cost-effective and efficient for building applications for sharing EHR data [3].

II. PURPOSE AND PROBLEM STATEMENT

The purpose of this research paper is to evaluate healthcare organizations' readiness to adopt Blockchain technology for managing EHR systems. Patient records are scattered across different providers, and the current health care system needs to be equipped to create a lifetime record of a patient's health history. It is estimated that less than 10% of healthcare organizations regularly share medical information with providers outside their organization [1]. Lyu et al. (2017) surveyed 2,106 physicians to examine their perception of overtreatment as a cause of preventable harm and waste in health care problems [5]. The study indicates that 20.6% of overall medical care was unnecessary. The sources of waste include prescription medications (22%), tests (24.9%), and procedures (11.1%) [5]. Also, reasons for overtreatment include fear of malpractice (84.7%), patient pressure/request (59.0%), and difficulty accessing medical records (38.2%) [5].

III. LITERATURE REVIEW

The percentage of office-based physicians in the US with an EHR system has grown substantially between 2004 and 2022. In 2004, EHR adoption was just 20.8% in the US, and as of 2021, 88% of physicians have adopted an EHR solution, and 78% have adopted a certified EHR solution [9]. Most healthcare EHR system uses a client-server architecture, where a central authority has full access to the system, and lack of privacy or security flaws may lead to failure in the system, resulting in hackers potentially gaining access to patients' data [16].

Digitalization can be understood as using digital technology, leading to changes in value creation, business processes, and business models to provide new revenue and value-adding opportunities [13]. Digital technology in healthcare, such as blockchain, is an open, decentralized system that eliminates the intermediaries, does not requires multi-level authentication, and provides access to everyone who is part of the architecture [15]. Digitalization in healthcare facilitates the organization toward digital transformation by automating the processes for better outcomes [13]. Blockchain and smart contracts can also help trace drugs throughout life. Blockchain, as the underlying technology of financial bitcoin, has gained wider recognition as an innovation in healthcare and not only the financial area [15]. Blockchain technology can transform organizations' business processes and market inter-organizational activities. A connectivity platform using blockchain or distributed ledger technology (DLT) to address healthcare data accessibility, integrity, and security is a process solution to data collection [4]. Data collected using the blockchain is essential for processing and sharing by addressing speed, scale, and convenience concerns. Managers can use a central data repository integration strategy to develop further an intelligent ubiquitous communicative surveillance platform to simultaneously coordinate multiple devices, manufacturers, service providers, patients, and numerous protocols for processing data into insightful, proactive surveillance levers to reduce adverse medical events and revision costs [18]. Research completed by Dagher et al. (2018) indicated that the evolution of internet connectivity and applications such as blockchain has allowed managers to redesign the medical device surveillance process from a passive data collection system to a real-time data system [5].

Blockchains has unique features, including distributed ledger, consensus, immutability, blocks, and smart contract.

1. Distributed ledger: It facilitates immutability and transparency. it is a single decentralized database managed by participants who all updates it through mutual consensus. There is no central authority, and all participants follow specific rules.
2. Consensus mechanism: It ensures no duplication or fraud and is used to validate transactions. The most popular consensus mechanisms are proof work (PoW), Byzantine fault tolerant-based (BFT), and Proof of Stake (PoS) [12]. PoW is the most popular among the three and has better security. It validates a block by solving a complex computational puzzle. Solving a computational puzzle requires an immense amount of energy, and the significant amount of energy is a drawback to hackers from a cost perspective [12].
3. Blocks: A block is a recorded transaction linked to an irreversible chain. The genesis block is the first and only block with no reference to the previous block [12]. There is a consensus from the users, and only blocks are recorded and considered immutable. There is a nonce, hash from the previous block, data and time stamp, transaction list, and a unique number [12]. A secure Hash Algorithm (SHA) is the most common function used in the blockchain.
4. Immutability: it is the differentiation between blockchain database and traditional database storage. Any information added to the blockchain cannot be modified or deleted. However, sensitive information can be deleted from the chain to give patients the right to be forgotten by the security and privacy law [12].
5. Smart contracts are a computer code self-executing as criteria for blockchain transactions. Smart contracts eliminate the middle intermediaries and reduce red tape in the process. Completing any transaction must meet the smart contract's rules [12].

Blockchain type can be either public, private, hybrid, or consortium. All users have equal rights in a public blockchain, and there are no regulations to follow unless the platform asks about some safety precautions to maintain. The database is entirely decentralized. Bitcoin cryptocurrency is an example of a public blockchain. It is completely immutable. The private blockchain is not open to all participants, as the restricted network only allows access to selected users. It is partially immutable, as the administrator may delete some information. The private blockchain is considered faster and more efficient than the public. This model is useful in organizations that share sensitive data and does not want all to access their information. A hybrid blockchain is a combination of both private and public. Some functions remain accessible to the public, while others remain permissioned or private. It is considered flexible to the organizations.

Retrieval Number: 100.1/ijitee.A93591212122
DOI: 10.35940/ijitee.A9359.1212122
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A consortium blockchain is a variation of a private blockchain as access still requires permission, but the system includes multiple organizations instead of a single organization. Consortium further breaks down into four types: government-driven, dual-focused, technology-focused, and business-focused [10].

IV. DISCUSSION

Fig. 2 depicts a common scenario in the current healthcare system. Health provider A does have all the control. The provider handles all the tasks, including managing and maintaining the data. A can provide query access to users and another health provider B for a diagnosis. Health provider A only has edit access, and demand from other users and health providers raises serious concerns about data security, interoperability, and privacy [17]. Interoperability is the ability to access, exchange, integrate, and cooperatively use data in a coordinated manner within and across organizational and national boundaries to provide timely seamless information and improve the health of all individuals globally.

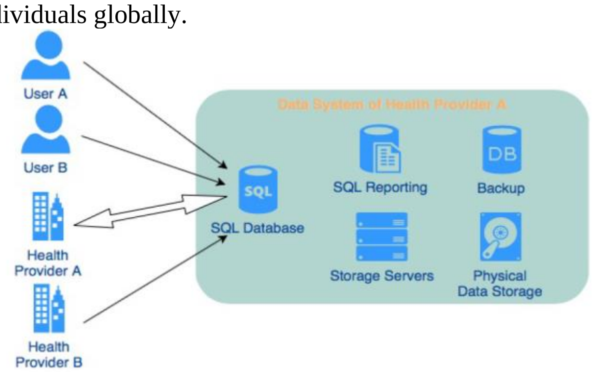

Fig. 2. Scenario in the current healthcare system (Yang et al., 2018) [17].

The primary issue in the model shown in fig 1 is fragmentation across different health providers. Every health providers maintain its system. Lack of integration between all providers stops the comprehensive overall of all records of a single user. It prompted several researchers to look for a decentralized electronic record system. Azaria et al. (2016) proposed Med Rec, a novel decentralized record management system to handle EHR efficiently. Med Rec blockchain implementation addresses the four major issues: fragmented, slow access to medical data; system interoperability; patient agency; improved data quality and quantity for medical research [2]. Med Rec is a *network* rather than a *service.* The advantage of this is that we can provide a cross-provider, patient-oriented interface and interaction mechanism [8].

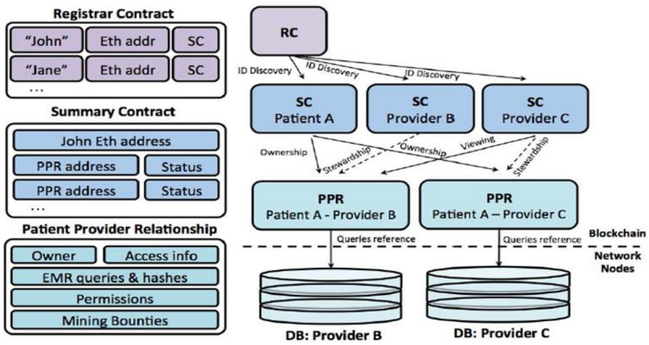

Fig. 3. MedRec smart contracts on the blockchain (Azaria et al., 2016) [2].

Fig 3 depicts the contract structures and relationships. Register contract (RC) maps participants' identification strings to their Ethereum public key identity. The RC also maps identity strings to an address on the blockchain, where a special contract called the smart contract is found. Patient-provider relationship (PPR) contract is issued between two nodes in the system when one node stores and manages medical records for others. The summary contract (SC) holds a list of references to PPRs representing all the participant's previous and current engagements with other nodes in the system. In Med Rec, the language is a set of contracts initiated by patients that define what entities or parties can access which records. The simplest asserts that entity B can access the records of patient A, and more complicated ones allow for intermediary healthcare proxies or allow a pharmacy to access all prescription records for patient A from any healthcare provider [8]. Lippman et al. (2018) utilized MedRec to build a model for successful operation [8]. As shown in fig 4, there are three participants in the network: Third parties such as research organizations, pharmacies, patients, and healthcare providers.

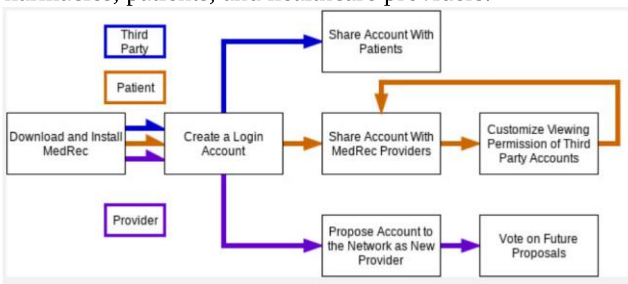

Fig. 4. Workflow for potential network constituents (Lippman et al., 2018) [8].

All users in the Med Rec network install Med Rec and create a login account. New healthcare providers propose special smart contracts for addition, and existing providers vote on whether to accept the proposal. Patients create relationships by sharing their account IDs with all healthcare providers. Patients can view the portion of the medical data stored by all the other providers once the relationship is formed. This network is semi-public. Anyone can join, but only providers authorize the contract and append it to the blockchain. Majority voting is required to immunize the system instead of trusting fully on providers. Tanwar et al. (2019) designed and proposed an efficient blockchain network-based EHR sharing system with enhanced security and privacy. We have four participants in the proposed system: patient, clinician, lab, and system administrator. Various smart contracts are defined in this architecture, such as Create Medical Record, Grant Access To Clinician, Grant Access To Lab, Revoke access, and Revoke Access to Lab [16]. As per simple workflow, participants register through the client application or SDK and request an enrollment certificate via an MSP to the certificate authority (CA). CA issues the certificate and new ID private key to enroll all participants. All transactions are distributed over the Hyperledger Fabric blockchain network.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

All participants have been given roles as per their access. Patients can use the client application to add records, invoking a chain code for committing a transaction to the network. The updated transactions are distributed over the network once the transaction is committed. It also ensures that each transaction is distributed to all participants in the network and cannot be deleted or modified by any users who are not authorized. The network is fully secured as the system allows new transactions to be added to the previous hash with a timestamp. Providers can add records to the EHR ledger network and access the data if patients grant access. This model helps optimize system performance by maintaining security using cryptography keys and smart contracts.

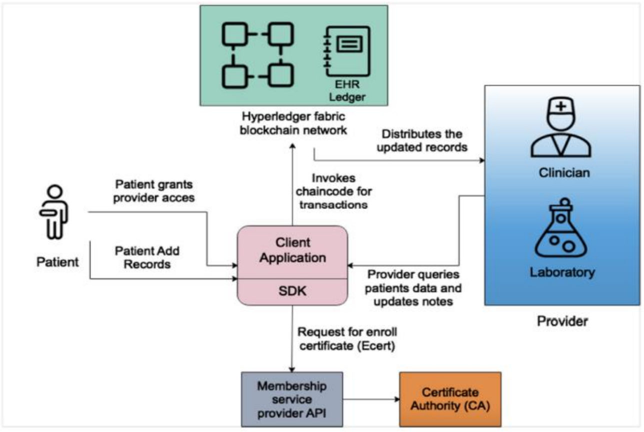

Fig. 5. Blockchain-based system architecture (Tanwar et al., 2019) [16].

I have discussed four different models in the study, including client-server architecture (fig 2), MedRec smart contracts on the blockchain (fig 3), Utilizing MedRec as a service (fig 4), and hyper ledger fabric blockchain network-based architecture (fig 5). Blockchain is an open decentralized system that eliminates the need for middlemen does not require multiple levels of authentication and provides access to anyone who is part of blockchain architecture [16]. These features in those models can help various challenges faced by the healthcare ecosystem, concluding all the evidence of blockchain utility in medical record management history.

V. CONCLUSION

Advancement in healthcare 4.0 digitalization, such as ambient listening from Siri and Alexa, telecare, and deep learning, has already transformed healthcare globally [6]. Recent breakthroughs in digital health technologies, such as electronic health records, health monitoring, and wearable devices, are not only transformative for reengineering care processes and improving health care outcomes such as care quality and patient safety but can also have a significant socio-economic impact, as almost 20% of the US GDP is dedicated to health expenditures [7]. The use of blockchain in healthcare can play a critical role by automating the data collection and verification process, correcting and aggregating data from various sources which are immutable, tamper-resistant, and provide secured temper proof data [16]. Any digital blockchain solution must also be sustainable, which contains social, environmental, and economic sub-dimensions [14]. EHR is the core of medical care. Medical institutions and practitioners must have access to patient's health histories to provide the correct diagnosis and best care possible. The infrastructure responsible for sharing and securing EHR between different medical entities is inadequate. There are severe consequences and risks to patients for their records not being accessible and compromised. There are significant strides in Digitalization using contemporary technologies, such as blockchain can help mitigate the problem. Sustainable development goals. Permission-based EHR system with cryptography key, design access control policy algorithm with smart contract achieves performance optimization of the system.

Emerging technology, such as blockchain, may play a vital role by improving all healthcare aspects- from clinical advances to communication and medical decision-making [6]. Blockchain is an ecosystem technology and works when technology is broadly adopted and only when physical systems work with it [15]. There are still roadblocks to proper strategies implementation, but the idea has yet to be posed. Researchers and industries are working tirelessly to develop the best solutions to current electronic health record problems.

REFERENCES

1. A. Siyal, A. 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 [CrossRef]
2. Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management." In Open and Big Data (OBD), International Conference on, pp. 25-30. IEEE, 2016, DOI: 10.1109/OBD.2016.11 [CrossRef]
3. Belcher, B. (2021). Blockchain: The way out into supply chain integrity. https://www.spiceworks.com/tech/innovation/guest-article/blockchain-the-way-out-into-supply-chain-integrity/
4. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, pp. 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014 [CrossRef]
5. H. Lyu et al. (2017), "Overtreatment in the United States," PLoS One, vol. 12, no. 9, Sep. 2017, DOI: 10.1371/journal.pone.0181970. [CrossRef]
6. Kritz, J. (2018). Beth Israel deaconess medical center launches health technology exploration center. https://www.bidmc.org/about-bidmc/news/2018/05/bidmc-launches-hte ch
7. Li, J., & Carayon, P. (2021). Healthcare 4.0: A vision for smart and connected healthcare. IISE Trans Healthc Syst Eng. 2021; 11(3): 171–180. DOI: 10.1080/24725579.2021.1884627 [CrossRef]
8. Lippman, A & Nachinda, N. Ratzepi, K., & Cameron, A. (2018). MedRec: Patient control of medical record distribution. https://blockchain.ieee.org/technicalbriefs/july-2018/medrec-patient-control-of-medical-record-distribution
9. Office of the National Coordinator for Health Information Technology, Office-based Physician Electronic Health Record Adoption," Health IT Dashboard - Quick-Stat #50, 2019. dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php. (accessed on 9th November 2022).
10. Pawczuk, L., Wiedmann, P., & Simpson, L. (2019). So, You've Decided to Join a Blockchain Consortium Defining the Benefits of Coopetition. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-cons-Blockchainconsortium.pdf
11. Pract, O., J. (2005). Electronic health records. National library of medicines, Volume 1 (2). DOI: 10.1200/jop.2005.1.2.57 [CrossRef]

12. Ribitzky, R., St. Clair, J., Houlding, D. I., McFarlane, C. T., Ahier, B., Gould, M., Flannery, H. L., Pupo, E., & Clauson, K. A. (2018). Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. Blockchain in Healthcare Today, (20180323). https://doi.org/10.30953/bhty.v1.24 [CrossRef]
13. Shashi, M. (2022). Digital Strategies to improve the performance of pharmaceutical supply chains. (Publication No. 28966332). ProQuest Dissertations and Theses Global
14. Shashi, M. (2022). The Sustainability Strategies in the Pharmaceutical Supply Chain: A Qualitative Research. International Journal of Engineering and Advanced Technology, Volume-11, Issue-6, August 2022 [CrossRef]
15. Shashi, M. (2022). Exploring Strategies to Leveraging the Blockchain in Pharmaceutical Supply Chains. International Journal of Research and Analytical Reviews, Volume-9, Issue-3, August 2022
16. Tanwar, S., Parekh, K., & Evans, R. (2019). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journals of information security and applications. https://doi.org/10.1016/j.jisa.2019.102407 [CrossRef]
17. Yang, G., Li, C., & Marstein, E. K. (2018). A blockchain-based architecture for securing electronic health record systems. The 10th IEEE International Conference on Cloud Computing Technology and Science (CloudCom, 2018). [CrossRef]
18. Zack, J. G. (2020). Strategies for reducing adverse medical events from implanted medical devices. ProQuest Dissertations and Theses Global.

AUTHORS PROFILE

Dr. Manish Shashi is a global supply chain, senior leader, and researcher. Dr. Shashi has more than 28 years of experience working globally in more than 12 countries, including APAC, Europe, EAMER, and the Americas geographies. Dr. Shashi earned a mechanical engineering degree from NIT, Surat, MBA from DBIM, India, a Lean Six Sigma Black lack belt from Villanova University, PA, USA, a master's in management from Saint Elizabeth, NJ, USA, and a doctorate from Walden University, MN, USA. Dr. Shashi is also associated with the digital transformation program at MIT, USA.