Chapter 8
The Desiderata of Blockchain and IoT in Medical and Pharmaceutical Enterprises

M. Manikandan, R. Subramanian, S. Nagajothi, S. Karthik, and Anand Paul

8.1 Introduction

Enterprises are typically known to be interpreting substantial data on an enormous scale which are made use of for heterogeneous processing. In the event of being extremely hard-pressed for time, conditioning voluminous records of patients locally and manually in a single node within an organization paves the way for less privacy and frequent chaos owing to the considerable hike in the number of patients in a hospital [1]. The demands for storage can be met with ease when the appropriate cloud computing service models are chosen as the solution for managing the workloads and computing instances of the respective enterprises. Cloud storage is regarded as the giant leap from the traditional way of handling IT resources. The expenditure on upgrading hardware and software and equipping data centers can be acutely minimized [2]. Cloud storage promotes remote access, data backup, and disaster recovery of indispensable information of the patient's data with enhanced

M. Manikandan (✉) · S. Nagajothi
Assistant Professor, Department of CSE, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India
e-mail: manikandanm@skcet.ac.in

R. Subramanian
Department of EEE, SNS College of Technology, Coimbatore, Tamil Nadu, India
e-mail: deaneee@snsct.org

S. Karthik
Department of CSE, SNS College of Technology, Coimbatore, Tamil Nadu, India
e-mail: deancse@snsct.org

A. Paul
Department of CSE, Kyungpook National University, Daegu, South Korea
e-mail: anand@knu.ac.kr

T. Choudhury et al. (eds.), *Blockchain Applications in IoT Ecosystem*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-65691-1_8

reliability than the formal methods of data storage as this data can be mirrored at multiple sites on the cloud provider's network. This article provokes how the amalgamation of cloud storage, blockchain, and IoT can render an unparalleled service to the pharmaceutical enterprise community to have a modicum of command over the sensitive data and transactions [3].

The blockchain technology promises to be bridging the gap between the establishments of a mutual conventional manner without any dispensary to rate the IoT transactions. It is predicted that many IoT services will extend its global reach across billions of devices. The current IoT ecosystems rely on centralized, brokered communication models [4]. The devices are authenticated and authorized via extremely robust servers that are capable of handling huge computations. Even after the confrontation of the prevailing pitfalls, cloud servers tend to turn out to be erroneous. Moreover, the alternating spectrum of ownership among devices and their respective cloud servers makes it too cumbersome to interact with their counterparts. Not all services offered by different organizations are neither completely interpretable nor portable to bring about the devices and their controls under a stand-alone roof [5]. But blockchain could effectively lend a straightforward infrastructure for devices to directly transfer paramount entities like money or data clustered with a secured and an enhanced time stamp. Utilizing the latter would also eliminate the need for centralized authority constraints to enable the autonomous functioning of smart devices resulting in a completely distributed worthwhile digital infrastructure [6].

Effectuating blockchain for IoT data yields new dimensions to automate healthcare processes among the medical and pharmaceutical enterprises without setting up a complex and expensive IT infrastructure [7]. The data protection in blockchain fosters a stronger working relationship with the partners and greater efficiency as enterprises take up the advantage of the information provided. Incorporating blockchain would be an eye-opener to settle vulnerability and privacy concerns in IoT. Single points of failure could be knocked out, and a more adaptable environment for the devices to run can be accomplished. Blockchain can keep track of unvarying reports of connected devices in the IoT network [8]. Blockchain holds an impeccable role in transforming the unadorned aspects of IoT into reality. This was made possible owing to its centralized authority and as the nodes in the blockchain do not extend the scope of validating and verifying the transactions to any other functional component.

Cloud storage has evolved to be one of the emanating technologies which primarily aid in storing data and eliminating storage constraints with an appreciable extent of security and privacy [9]. The ample responsibility of counteracting multiple storage requests and service discrepancies completely relies on the cloud service provider. The outcomes of the requests from the cloud server are typically shielded with a robust encryption schedule thereby turning out to be less erroneous than the existing data storage methodologies. Equipping a medical enterprise with a private cloud enables access to hosted services to a pre-assigned number of authorized people (doctors and other medical representatives) [10]. Cloud-based solutions also bring about opportunities for more portability and higher productivity

and efficiency for the physicians as everyone is assured access to the same updated information within a few mouse clicks.

The security attributes provided by the cloud service organizations naturally make the data ultimately devoid of cautionary threats. The transactions and security of the sensitive patient's data can be enhanced by implementing blockchain technologies [11]. Blockchain is an ingenious invention originally framed for crypto-currency, but it has now found many other applications in the world. Since the data held in a blockchain exists as a common and continually streamlined database, the medical reports added by a wide range of computers turn out to be verifiable with ease as the entire entity is backed up in a secure domain of space. The peculiar factor of a blockchain is that none could attempt to alter the data that was previously appended to the distributed ledger. The transactions stored in the nodes of the blockchain network cannot be falsified as attempting so would require the intruder's machine to overpower the entire network which is practically impossible.

8.2 IOT in Medical and Pharmaceutical Enterprises

8.2.1 Digitizing Patient's Records Using Blockchain with Electronic Health Records (EHR)

Electronic health records are regarded as a digital form of a patient's database. They are real-time monitored, patient-centered records that deliver information instantly and securely to physicians. They are usually composed of patients' medical history, medical transcriptions, diagnoses, radiology images, laboratory, and test results. The records stored in the EHRs can be effectively shared among other healthcare organizations which can avail access to evidence-based tools to conclude decisions about a patient's healthcare [12].

8.2.2 Precedence of Electronic Health Records (EHR) over Electronic Medical Records (EMR)

Electronic medical records are digitized structures of the patient's record in the physician's enterprise. An EMR comprises the medical history of the patients in due course of time. They keep track of data over time and identify the patients who are to undertake medical checkups. The quality of care within the practice can be delved into accordingly. In case of the requirement of a hard copy of a patient's record, it might be delivered to veteran physicians and other medical professionals of the care team. In that regard, EMRs cannot be handled with much ease than the traditional paper records, making it considerably less consistent [13].

Electronic health records, on the other hand, do satisfy all the parameters which the EMR failed. When EHR is chosen to undertake the patient's records, they could reach out beyond the healthcare enterprises that initially collect and record information. Electronic health records can be created, maintained, and shared by the concerned personnel across more than one medical enterprise.

The data is coordinated with the patient to the concerned representatives, the hospital, or even across the continents. Electronic health records are extremely handy when sharing medical and treatment records among associates and comprehending the levels of care undertaken by the individual.

The patient's records shared with encryption turns out to be powerful. The culminating value from the enterprises is an outcome of productive interaction of information from one recipient to another and the capability of interchanging the information to indulge in an interactive communication of the curative particulars which can only be accomplished by cloud storage and blockchain [19].

8.2.3 Advantages Associated with Electronic Health Records (EHR)

1. Individual patients can log on to his/her record and keep track of the laboratory results over their past arrivals, which can present a clear and concise picture of the medications that he/she takes in and the routines he/she maintains to keep up the scale [14].
2. At times of emergency, electronic health records (EHR) can reveal the patient's medical threats, so that medications and healthcare processes are adapted accordingly even if the patient is insensible.
3. Precise conclusions can be drawn from the previous test results by the specialists despite running duplicate tests to ensure the current status of the patient.
4. The physicians' descriptions from the patient's period of hospital stay can reveal the requisite details and pave the way for the portability of patients [14].

8.2.4 Incorporating Privacy and Security into EHR and IoT

Health information breaches can lead to a plethora of disastrous consequences. The data breaches might result in harming patients, downfall in finance, and degradation of an enterprise's reputation. It is rather indispensable for the healthcare records to be furnished with a considerable extent of privacy and security implications than making this sensitive information immune to destructive cyber threats. Encrypting patient privacy and seclusion of electronic health information is of paramount importance and is an arbitrary responsibility. Clinging to constructive security attributes greatly enhances trust among patients. The patient must trust the enterprise

that their sensitive medical records will remain confidential, accurate, and secure in safe hands [15].

This trust can sum up the patient's overall health, in a nutshell, paving the way to better-structured decisions. The advantages associated with the security of EHRs over voluminous paper records include encoding medical information, backup, and automated control. The privacy guidelines enable the patients to gain a modicum of control over their medical records and let them determine their ways of utilizations. This also provides safeguard measures that make the medical professionals and their fraternity to abide by these rules that are set by the patients. Blockchain's capability to keep an indestructible and decentralized log of all patient data makes it a technological ruse for potentially scalable security solutions. The delicacy of the medical records can be greatly preserved as the blockchain promotes the anonymity of the individual. This disseminated nature of the latter enables rapid exchange of healthcare records among the authorized medical professionals as well.

8.2.5 Impediments Involved in Implementing EHR and Blockchain

In the course of technological development, several incentives have been provided by the respective democracies to deploy electronic health records to improve and coordinate quality care across the healthcare environment. Cost prevails to be the subjective concern for the organizations that are yet to incorporate blockchain. To establish an EHR system regardless of whether in an enterprise or a medical environment is a high-priced and comprehensive process that demands an enormous amount of manual workload and monetary requirements. On the other hand, security vulnerabilities for digital and classified information remain to be the predominant cause for why the enterprises hesitate to adapt to blockchain technology [16].

8.2.6 Medical Transcription and EHR

Organizations equipped with EHR have always looked forward to getting deprived of the transcriptions and opting for electronic records from the lucrative generated from the transcriptions. This stereotype existed until the advent of EHR. It was then realized that traversing through the EHR was time-consuming when clustered with the concerns about the standards of the documentation, and minimization of errors in documentation allowed the veteran medical associates to acknowledge that there is still much more scope for such services to evolve. Medical transcriptions help in the accumulation of the medical narrative, which prevails to be the medical memorandum in the physician's aspect. This narrative is often regarded as the first-person perspective of the patient's medical history. This narrative

being circumstantial is impossible to replicate with the finest EHR testimonial features. These transcriptions furnish hassle-free and significant documentation which is the much-expected factor to the physicians in an EHR. However, highly compliant documentation tools are provided by transcription service companies for the physicians and the authorities [17].

8.3 Existing Model

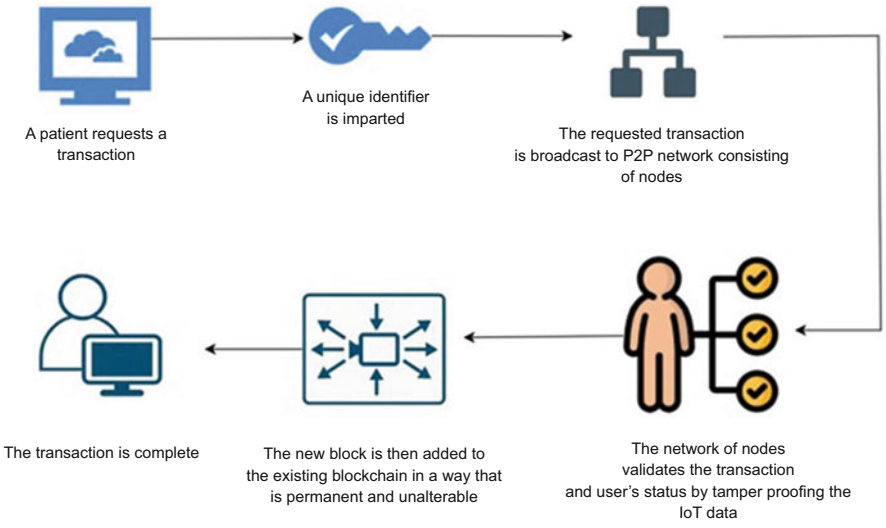
Electronic medical records (EMRs) also known as electronic health records (EHRs) are the foundational components of all healthcare systems. Despite the growing literature on boons of various EHR interoperabilities, there are proven potential banes accompanying this emanating technology. These include monetary loss, workflow chaos, and interim forfeiture of efficiency, security and privacy concerns, and various unprecedented aftermaths. Since the medical information is electronically exchanged extensively, the likelihood of violating a patient's privacy is at stake. A poorly designed EHR leads to elevated medical fallacies, disrupted misconceptions, and overdependence on technology [18]. Though geared with arbitrary security measures, the authorities must be trained in basic digital security to ensure they do not leave their organizations vulnerable to unauthorized access. Any discrepancy in the medical records eventually leads to shrunken efficiency thereby making tasks of ease to be tiresome. Yet another cause of shrunken efficiency relates to inadequate tutoring on the EHR infrastructure which emerges when a system is renovated or modernized. The EHR of each patient must be frequently updated to enhance the precision of their data, while non-frequent reconditioning can lead to misconceptions in diagnoses of the patients.

8.4 Proposed Model

The existing healthcare facilities are known to be still solely relying on traditional systems for maintaining medical and healthcare records and processing payments thereby making it extremely tedious for the healthcare professionals to diagnose as the records are locally stored. Yet another painstaking threat prevailing in the medical industry is the exchange of the patient health information. The records are more susceptible to the chances of impersonation and fraudulent monetary crimes as the patients don't own any control over their records/data. The availability of acutely handy devices had still not let the patients collect, analyze, secure, and exchange healthcare information seamlessly. Adopting a blockchain and IoT leveraged solution can help accomplish a smooth, transparent, economically efficient, and easily operable system combined with secure payment options. As far as healthcare is concerned, none of the enterprises were found to be possessing a universally recognized patient identifier. An intriguing factor is that a unique

patient identifier is capable of solving the disputes of mismatched EHRs (electronic health records) which have in the past led to numerous errors in patient care and increase the likelihood of patient harm. The medical and pharmaceutical industries are subjected to indispensably handle and store a colossal amount of data leading to potential security breach prospects. Patient records which are recorded and stored in a blockchain network are persistent and sturdy. Either to revamp or to refurbish the records in a block, it solely requires the prerogative of the patients, hence making them the owners of their respective medical information. The effectuation of blockchain also facilitates authentic and genuine payments through cryptocurrencies. The implementation of blockchain technology could mitigate these errors in the following ways:

1. A unique identifier is imparted to each patient thereby establishing a smart contract between patients and medical wellness enterprises. Doing so would not only ensure that the data shared is genuine and precise but also extend coherence with rapid diagnoses.
2. The courtesy of the inherent transparency of the blockchain technology guarantees hospitals that all patients' health records are "tamper-proof" while still ensuring the data's privacy. This would potentially eliminate the security hurdles that come along with IoT.
3. Enacting cryptocurrencies in place of cash or fiat money would ease bill processing automation and henceforth obliterate the third parties from the chain and increase the lucrative revenue of the organizations. Deploying such technologies would enable the tracking of each penny paid to the healthcare enterprise and verify that no errors are encountered.



Since healthcare is a convoluted system with miscellaneous structures, it necessitates a patient to share their healthcare records across the medical environment.

The abrupt increase in the number of patients had led to the need for intensified data management by medical enterprises. Thus, maintaining patient information within hospital premises would be a big deal.

Financial aspects of medical care are of paramount importance. This domain is usually clogged with inefficiencies which can be optimized by the utilization of blockchain. In the view of the establishment of smart contracts between medical care professionals and patients, the latter can be made use of in premium negotiating phases. Data which deals with current health status, types of medications intake, etc. entangled to the blockchain to evolving premiums, through smart contracts. The intrusion of too many mediators or intermediaries turns out the claim handling process to be enduring and burdensome for the end customer. Taking these counterproductive effects into account, few propositions had been employed into blockchain for billing claims management and broader financial aspects of care delivery. The Ethereum or Hyperledger framework used in streamlining claim management in medical care is known for its versatility in delivering the patients, providers, and the insurers together into one ecosystem for real-time insights into the patients' health journey and ease of health claims management.

The cluster of blockchain and IoT can hopefully replace cash or government-backed currencies. Innumerable nodes in a blockchain network utilize cryptographic strategy to establish an irreversible and collective record of all transactions that had ever taken place. Processing transactions with a decentralized currency provides added security and minimizes the erroneous instances of fraud. The transparent nature of the blockchain leads to a robust repository of databases and secure payments subsequently instituting falsification or corruption of records impossible. Healthcare organizations who had succeeded in administering this emanating technology would witness consequent ease of access to their billing and accounting thereby ignoring the fear of fraud being committed by employees of the enterprise or from the patients themselves.

8.5 Conclusion

Blockchain has the inherent knack to solve several disputes storming the medical care industry today. It poses a boundless dimension among various healthcare

stakeholders, namely, patients and providers. A blockchain which is a decentralized network may minimize stakeholder lock-in problems in healthcare. Despite the hype and the deal of interest circling over blockchain and IoT, its implication and effect on healthcare had been quite low and are still in the early days. Medical organizations and enterprises which have deployed blockchain applications are working with a limited user base. Yet a mammoth growth is anticipated with a significant positive impact of blockchain in healthcare in the future. Handling patients' records and the dome of secured payments is the key that blockchain holds which the existing entities are devoid of. The processes will not only be trustworthy and persistent, but also the quality of healthcare will be extended cost-effectively. The prioritization of data is allocated solely to the patients. The idea of an encrypted public ledger via cryptocurrency among medical agencies, patients, and networks brings about an intriguing future that could change the way data is used to treat patients. The transactions of both the enterprise and patients turn out to be more explicit after the successful effectuation of blockchain and cryptocurrency than maintaining incommodious physical records and ingenuine payments. By incorporating IoT with tampered-proof protocols, its security threats are eliminated, thereby paving the way for a smooth process curve, and the prioritization of data is allocated solely to the patients.

References

1. A. Firdaus, N.B. Anuar, M. Faizal, I.A.T. Hashem, S. Bachok, A. Kumar, Root exploit detection and features optimization: Mobile device and blockchain-based medical data management. J. Med. Syst. **42**(6), 1 (2018 June). https://doi.org/10.1007/s10916-018-0966-x
2. T. Bocek, B.B. Rodrigues, T. Strasser, B. Stiller, *Blockchains Everywhere – A Use-Case of Blockchains in the Pharma Supply-Chain* (2017 May). https://doi.org/10.23919/INM.2017.7987376
3. E. Chukwu, L. Garga, Systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. IEEE Access **8**, 21196 (2020 January 7)
4. WHO, *World Health Statistics 2018: Monitoring Health for the SDGs* (WHO, Geneva, 2018)
5. AAMC, Careers in medicine (2019). Accessed: Jan. 29, 2019. [Online]. Available: https://www.aamc.org/cim/specialty/exploreoptions/list/
6. P. Zhang, D.C. Schmidt, J. White, G. Lenz, Blockchain technology use cases in healthcare. Adv. Comput. **111**, 1–41 (2018 January)
7. X. Zheng, R.R. Mukkamala, R. Vatrapu, J. Ordieres-Mere, Blockchain-based personal health data sharing system using cloud storage, in *Proceedings of the IEEE 20th International Conference on e-Health Networking, Applications Services (Healthcom), September 2018*, (2018), pp. 1–6
8. X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in *Proceedings of the IEEE 28th Annual International Symposium on Personal, Indoor, Mobile Radio Communication (PIMRC), October 2017*, (2017), pp. 1–5
9. Y. Du, J. Liu, Z. Guan, H. Feng, A medical information service platform based on distributed cloud and blockchain, in *Proceedings of the IEEE International Conference on Smart Cloud (SmartCloud), September 2018*, (2018), pp. 34–39

10. C. Ananth, M. Karthikeyan, N. Mohananthini, A secured healthcare system using private blockchain technology. J. Eng. Technol. **6**(2), 42–54 (2018)
11. [49] G. Srivastava, A.D. Dwivedi, R. Singh, Automated remote patient monitoring: Data sharing and privacy using blockchain. arXiv:1811.03417 (2018). https://arxiv.org/abs/1811.03417
12. S. Rahmadika, K.-H. Rhee, Blockchain technology for providing an architecture model of decentralized personal health information, *Int. J. Eng. Bus. Manag.***10**, Art. no. 184797901879058 (2018 January)
13. A.K. Talukder, M. Chaitanya, D. Arnold, K. Sakurai, Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden, in *Proceedings of the IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud Big Data Computing, Internet People Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Oct. 2018, pp. 257–262*
14. Z. Shae, J.J. Tsai, On the design of a blockchain platform for clinical trial and precision medicine, in *Proceedings of the IEEE 37th International Conference on Distributed Computing System (ICDCS), June 2017*, (2017), pp. 1972–1980
15. A. Al Omar, M.S. Rahman, A. Basu, S. Kiyomoto, MediBchain: A blockchain-based privacy-preserving platform for healthcare data, in *Security, Privacy, and Anonymity in Computation, Communication, and Storage (Lecture Notes in Computer Science)*, (Springer, Cham, 2017)
16. T.-T. Kuo, L. Ohno-Machado, ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks, arXiv:1802.01746 (2018). [Online]. Available: https://arxiv.org/abs/1802.01746
17. T. Heston, A case study in blockchain health care innovation. Int. J. Curr. Res. **9**(11), 60587–60588 (2017)
18. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: Using blockchain for medical data access and permission management, in *Proceedings of the 2nd International Conference on Open Big Data (OBD), August 2016*, (2016), pp. 25–30
19. D. Ichikawa, M. Kashiyama, T. Ueno, Tamper-resistant mobile health using blockchain technology. JMIR Mhealth Uhealth **5**(7), e111 (2017 July)