SECURING HEALTHCARE:

LEVERAGING BLOCKCHAIN FOR DATA INTEGRITY IN HEALTHCARE SERVICES

Editors:
Mohit Angurala
Preet Kamal
Aryan Chaudhary
Rasmeet Singh Bali
Vijay Bhardwaj

Bentham Books

Securing Healthcare: Leveraging Blockchain for Data Integrity in Healthcare Services

Edited by

Mohit Angurala
Department of Computer Science
Guru Nanak Dev University College
Pathankot District - Pathankot
Punjab, India

Preet Kamal
Apex Institute of Technology-CSE, Chandigarh University
Mohali, Punjab, India

Aryan Chaudhary
Biotech Sphere Research, Ghaziabad, Uttar Pradesh, India

Rasmeet Singh Bali
Apex Institute of Technology-CSE, Chandigarh University
Mohali, Punjab, India

&

Vijay Bhardwaj
Apex Institute of Technology-CSE, Chandigarh University
Mohali, Punjab, India

Securing Healthcare: Leveraging Blockchain for Data Integrity in Healthcare Services

Editors: Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj

ISBN (Online): 979-8-89881-063-4

ISBN (Print): 979-8-89881-064-1

ISBN (Paperback): 979-8-89881-065-8

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA.

First published in 2025.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

We now find ourselves at the crossroads of two powerful forces: Blockchain technology, in a never-ending Renaissance landscape of the technology and healthcare industries, and the strong demand for increased integrity, security, and compliance in data stored in health systems. The idea of this book is to venture through this intersection, where immutability and decentralization provided by the blockchain will pave new ways to reshape our strategies to manage, secure, and interact with healthcare data. With greater detail, the content of this book begins with an introduction to blockchain and how it may revolutionize healthcare, followed by an in-depth discussion of its applications across a host of domains. The following chapters provide the entire discussion about the role of blockchain in data integrity and increased compliance with regulatory standards while at the same time protecting sensitive health information. The book itself goes into detail about how blockchain is reframing the healthcare industry through documented case studies, theoretical explorations, and implementation in real-life situations. For sure, the first few chapters make a good point in building a base for discussion on the basics of blockchain technology and its potential to provide solutions for some of the most important problems concerning data transparency, traceability, and security. This is also a way to show how interoperability for health information exchange can be safely achieved by using the blockchain, which drastically changes the way patient data is shared and consumed between different providers and various healthcare institutions.

In the following sections, we detail specific applications of blockchain technology in improving smart contracts' functionality within the healthcare compliance framework, building patient-centric data management systems, and detecting fraud in clinical trials. In each one of these cases, extensive case studies and real-life examples explain to the readers practical insights into the challenges and successes faced in the journey of adopting blockchain in healthcare. Later in this book, blockchain is woven with other emerging technologies, such as the IoT and AI, to illustrate the broad set of applied solutions that will take this a step beyond in upgrading security and efficiency within connected healthcare systems. The chapters also indicate that it will have the potential to enable an advanced data analytics capability ranging from monitoring patients outside the hospital to securely sharing health data across complex networks.

The last two are more future-facing, an indication of what could be the future of blockchain in healthcare. We then discuss the regulations that are in a state of flux, potential issues around scalability and interoperability, and blockchain as an enabler of novel business models and healthcare solutions. In view of these future trends, the book will lead the reader on a knowledgeable and foreseeing journey of the ongoing transformation in the healthcare industry.

While discussed from a more technical perspective in this book, it is an appeal to all healthcare professionals, technologists, policymakers, and researchers to recognize the potential of blockchain and work together to make the future healthcare ecosystem more secure, transparent, and efficient.

Mohit Angurala
Department of Computer Science
Guru Nanak Dev University College
Pathankot District - Pathankot
Punjab, India

Preet Kamal
Apex Institute of Technology-CSE
Chandigarh University, Mohali
Punjab, India

Aryan Chaudhary
Biotech Sphere Research
India

Rasmeet Singh Bali
Apex Institute of Technology-CSE
Chandigarh University, Mohali
Punjab, India

&

Vijay Bhardwaj
Apex Institute of Technology-CSE
Chandigarh University, Mohali
Punjab, India

List of Contributors

Anita Tanwar	Chitkara Business School, Chitkara University, Rajpura, Punjab, India
Ankita Gupta	Department of Computer Science and Engineering, C.T. Institute of Engineering, Management and Technology, Lambri, Punjab, India
Ambika Prakash Mani	Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Deep Mann	Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala, Punjab, India
Garima Sharma	Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Gurpreet Singh Panesar	Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, India
Kiran Deep Singh	Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Rajpura, Punjab, India
Keesara Sravanthi	Department of Information Technology, VNRVJIET University, Hyderabad, Telangana, India
Kamlesh Gautam	Department of Advance Computing, Poornima College of Engineering, Jaipur, India
Mandeep Kaur Sandhu	Department of Computer Science, Guru Nanak Dev University College, Pathankot, Punjab, India
Mohit Angurala	Department of Computer Science, Guru Nanak Dev University College, Pathankot, Punjab, India
Mushtaq Ahmad Rather	Department of CSE-IoT, Noida Institute of Engineering and Technology, Greater Noida, India
Meenakshi Mandola	Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Navneet Kumar Rajpoot	Department of Computer Science & Engineering, Graphic Era (Deemed to be University), Dehradun, India
Prabh Deep Singh	Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Pardeep Kumar Jindal	Department of Electronics and Communication, Chandigarh Engineering College, Mohali, Chandigarh, India
P. Prasant	Department of Computer Science, AIPH University, Bhubaneswar, Odisha, India
Riya Sharma	Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Rajbir Kaur	Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India
Rajeev Kumar Bedi	Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Jalandhar, India

Rohan Verma	Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Raminder Kaur Khattri	Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Saptadeepa Kalita	Department of Computer Science and Engineering, Sharda University, Greater Noida, India
Sharon Christa	Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune, Maharashtra, India
Sandeep Singh	Department of Computer Science Engineering, SGT University, Gurugram, Haryana, India
Sonal Rattan	Department of UCRD and Apex Institute of Technology, Chandigarh University, Mohali, Punjab, India
Vikas Kumar	Department of AI & DS, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India
Varinder Pabbi	Department of Computer Application, I. K. Gujral Punjab Technical University, Phagwara, Punjab, India

CHAPTER 1

Introduction to Blockchain Technology in Healthcare

Mandeep Kaur Sandhu[1,*] and **Mohit Angurala**[1]

[1] *Department of Computer Science, Guru Nanak Dev University College, Pathankot, Punjab, India*

Abstract: Blockchain technology is rapidly gaining traction across various sectors, including healthcare, where it is revolutionizing how patient data is managed and shared among hospitals, diagnostic laboratories, pharmacies, and healthcare providers. By leveraging Blockchain networks, healthcare systems can ensure the secure and transparent exchange of medical data, enhancing performance and eliminating errors that could be potentially harmful. This technology empowers medical institutions by providing deeper insights and improving the analysis of medical records, thereby bolstering overall efficiency and security. In this chapter, we explore the transformative potential of Blockchain in healthcare, illustrating its key capabilities, facilitators, and the unified workflow processes it supports through diagrams. We highlight fourteen significant applications of Blockchain in healthcare, emphasizing its pivotal role in combatting fraud in clinical trials and enhancing data efficiency. The presented work ensures secure storage along with the seamless data verification of patients through distinct clinical stages, which further assures legitimacy and accessibility. It also empowers investigators to examine treatment outcomes in real time for large patient populations, thereby improving treatment precision and innovation in the medical field. We also discuss how Blockchain transparently secures and achieves sensitive genetic evidence, addressing issues of data ownership, privacy, and control. Blockchain ensures data integrity and security through its decentralized data storage model, offering versatility, interconnectivity, accountability, and robust authentication mechanisms for data access. This ensures that health records remain confidential and protected from specific threats, addressing concerns about data manipulation in healthcare settings effectively.

Keywords: Blockchain technology, Consent management system, Clinical trials, Electronic health records (EHRs), Healthcare data security, Interoperable healthcare systems.

[*] **Corresponding author Mandeep Kaur Sandhu:** Department of Computer Science, Guru Nanak Dev University College, Pathankot, Punjab, India; E-mail: gimeti4@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

INTRODUCTION

Blockchain technology forms an immutable chain of records by recording transactions across numerous computers in a way that prevents retroactive manipulation without affecting the following blocks. Blockchain technology is a decentralized and public digital ledger. It is an anonymous and distributed electronic record. The integrity and credibility of the data obtained are maintained and ensured by this feature due to its guarantee of high levels of responsibility. To reduce the risk of exposing the patient to the wrong medications and fight against counterfeit products, Blockchain provides end-to-end tracking that will track the source of the fake products. This is very significant in the health sector and the manufacture of drugs [1]. This architecture amplifies security against cyber-attacks as compared to the traditional centralized databases in an attempt to safeguard patient records and retain their unalterable medical history in a secure domain. It can be noted that with the help of Blockchain, the problem of data handling and its protection is solved, at the same time making the data of all participants in the network to be open and available. Patient engagement is achieved in a separate process – patients learn who has access to their information and for what purpose and make choices concerning their records themselves [2]. Precision medicine applies Blockchain to analyze large-scale modality of anonymized data for enhancing healthcare services. By combining Blockchain IoT and wearable devices, healthcare practitioners are able to monitor real-time parameters such as glucose levels and blood pressure and consequently manage high-risk patients and provide early responses to emergencies [3].

It makes sense to use blockchain in the protection of personal information and to provide the capabilities of fast sharing and pooling of data in a single secure place because blockchain works on the basis of a P2P network of nodes that stores and exchanges information safely [4]. It enhances teamwork because patients' information is stored in a central database, which will enable easy identification of practitioners for the study with specific characteristics. Blockchain is a distributed P2P system characterized by blocks, nodes, and miners that ensures the reliability of records of patients' transactions in distributed systems. This design distributes data across several computers so as to be relatively more immune to manipulation and illegal access than the conventional centralized systems [5]. With the help of different models, such as public, private, hybrid, and consortium Blockchain networks, it enables customers/users to exchange value directly and with or without the help of an intermediary. These networks are made to be applied in specific industries such as logistics, medicine, and finance, where communication is strictly required to be First in, First out, open, and most importantly, secure.

A Blockchain maintains a distributed digital ledger *via* a chain of blocks. Each block contains:

- Data (the type depends on the blockchain's purpose).
- Hash (a unique digital fingerprint).
- Previous hash (linking the current block to the previous one).

This structure ensures data integrity, as tampering with one block would make all following blocks invalid (Fig. **1**).

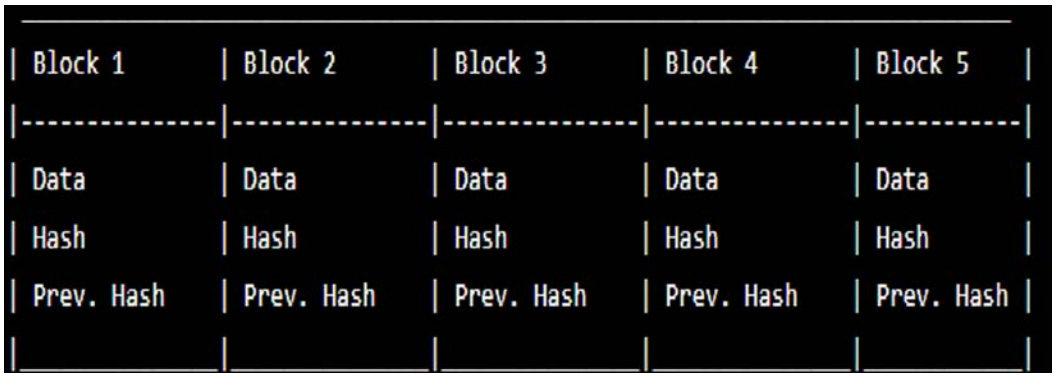

Fig. (1). The structure of the block.

BLOCKCHAIN *VS.* TRADITIONAL DATABASES

Blockchain and traditional databases provide different methods for managing data in healthcare systems [6]. Blockchain has decentralized control and uses encryption to protect data immutability and security. It offers great fault tolerance but has limited querying and familiarity. This new technology can integrate with Web 3.0 while improving the privacy and integrity of medical records. Traditional databases, on the other hand, provide well-known, dependable systems with broad SQL querying capabilities and a vast skill pool for management. However, they are centrally regulated and rely on optional encryption. Blockchain offers novel advantages for secure and immutable data management, possibly revolutionizing the handling and protection of healthcare information, while traditional databases benefit from their maturity and compatibility [7].

TYPES OF HEALTHCARE BLOCKCHAINS

In healthcare, blockchain can be implemented in both public and private settings. The choice depends on the specific use case and privacy requirements.

CHAPTER 2

Blockchain Applications in Healthcare

Vikas Kumar[1,*], **Mushtaq Ahmad Rather**[2] and **Saptadeepa Kalita**[3]

[1] *Department of AI & DS, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India*

[2] *Department of CSE-IoT, Noida Institute of Engineering and Technology, Greater Noida, India*

[3] *Department of Computer Science and Engineering, Sharda University, Greater Noida, India*

Abstract: Blockchain technology has become an influential power in different areas, one of which is healthcare. Using Blockchain technology, the paperwork is reduced, and the information is secured in the database, which further aids research and development. Focusing on the healthcare industry, the patients and the doctors do not receive the complete medical record, which is the major challenge being faced. This issue has been very well addressed in Blockchain technology. Further, Blockchain helps securely share data across digital systems with the consent of the patients, which makes technology more robust. This chapter covers the manifold usage possibilities of blockchain in healthcare, focusing on aspects such as control over electronic health records, the safety of supply chains, conducting clinical trials, the functioning of the system for medical insurance claims, and telemedicine. The chapter aims to present a comprehensive review of how security, transparency, and efficiency can be improved in healthcare systems through the use of blockchain by considering its advantages, disadvantages, and future directions. Also covered are some issues relating to blockchain-based support for patient-oriented medical care, data interchangeability in the health sector, and lightening administrative burdens. Finally, the chapter discusses several case studies and currently available research that show practical implications and real-life applications of blockchain technology in healthcare operations. Moreover, there are also insights into regulatory considerations as well as the dynamic nature associated with blockchain adoption trends within the healthcare industry at large.

Keywords: Blockchain technology, Clinical trials, Electronic health records (EHR), Healthcare, Health insurance claims, Supply chain integrity.

INTRODUCTION

Digital technologies have evolved rapidly, and this has resulted in significant changes across different sectors of the economy, with healthcare being a major

[*] **Corresponding author Vikas Kumar:** Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India; E-mail: vsangwan06@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

beneficiary. This chapter explores the possible uses of blockchain in healthcare and its potential benefits, emphasizing how it has reformed EHR management, supply chain integrity, clinical trials, health insurance claims, and telemedicine. In addition to data breaches, interoperability challenges, and ineffective management of information systems, among others, the industry is grappling with other struggles, including loss of data [1 - 3].

BACKGROUND AND FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

At its core, cryptographic hashing ensures data integrity and transparency through consensus algorithms as well as immutable ledgers that exist within blockchain technology (Fig. **1**). In the healthcare setting, it enhances secureness; therefore, tamper-proofing systems that are also interoperable become increasingly significant. The existing traditional healthcare systems often face issues such as loss of data both in terms of breaches, which affect privacy policies in relation to confidentiality, especially when addressing patients' medical records, and poor communication between hospitals, leading to a lack of proper care coordination among providers or even prescribing unnecessary medications since doctors were not aware about last tests conducted on him/her by other physicians, *etc.* The above weaknesses can be solved by employing decentralization properties that blockchain offers, thereby enhancing robust security measures against unauthorized access attempts [4 - 8].

Fig. (1). Key elements of blockchain.

EVOLUTION OF BLOCKCHAIN TECHNOLOGY

The evolution of blockchain can be categorized into three generations (Fig. **2**):

Blockchain 1.0 (Cryptocurrency)

Concentrated on electronic coins and specifically on Bitcoin.

Blockchain 2.0 (Smart Contracts)

Created programmable contracts that self-execute when a specific set of conditions exist on the blockchain. Ethereum is perhaps the quintessential example of this generation.

Blockchain 3.0 (DApps and Beyond)

Concerns itself with DApps and other Novum beyond financial uses such as healthcare.

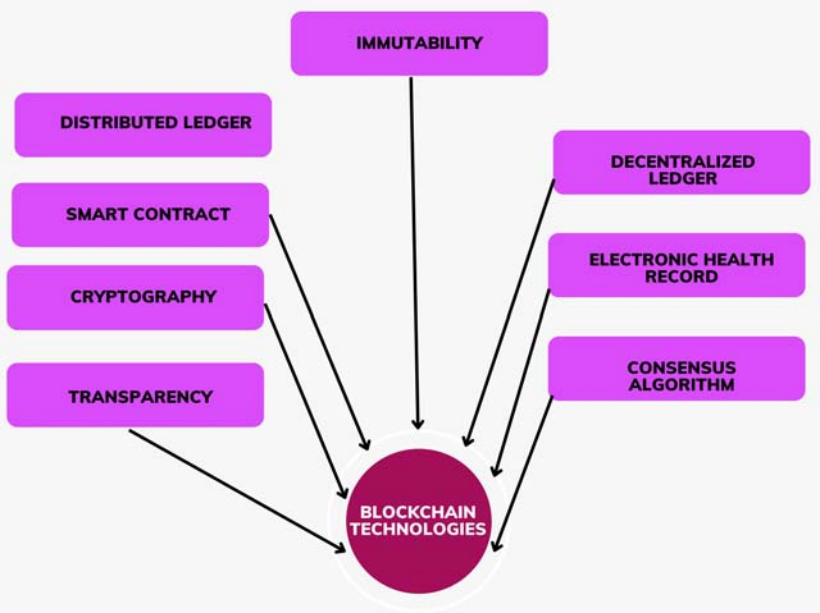

Fig. (2). Blockchain technologies.

BLOCKCHAIN TYPES AND RELEVANCE TO HEALTHCARE

In its broad sense, there are three types of blockchains [9]. Two of them are very distinct in their features that qualify them to be used in the different fields of healthcare.

CHAPTER 3

Blockchain Technology in Healthcare: Uses and Challenges

Anita Tanwar[1,*]

[1] *Chitkara Business School, Chitkara University, Rajpura, Punjab, India*

Abstract: Blockchain is the amalgamation of encryption and noble technology for communication. By giving individuals precise, customized, and safe accessibility to their healthcare information, tailored electronic medical records may help patients take charge of their own care. Tailored health records facilitate the creation of an innovative system that integrates electronic interventions, medical data collection, and access to smart contracts. Blockchain retains every patient's complete medical history, providing a secure means to store and maintain detailed medical data for every patient. This technology can be used to ensure the safe transfer of private data, including records of patients, episode summaries, disease logs, test results, medical treatments received, and emergency medical services. The healthcare industry is now front and center as a potential use case for blockchain technology. We can see a high-level picture of blockchain pertaining to healthcare. The system is composed of many blocks that are interconnected using hash functions based on cryptography. The blockchain is an important yet resourceful technique for transmitting and receiving data in an efficient and highly secure manner. Anyone involved in a transaction initiates the process by creating a block. The system is composed of many blocks that are interconnected using hash functions based on cryptography. This chapter discusses the conceptual background of blockchain technology in healthcare, user's need for blockchain, and challenges in using blockchain technology in healthcare. Blockchain technology has produced a permanent record that many financial technology systems utilize to detect cryptocurrency double-spending in order to meet efficiency and security criteria.

Keywords: Blockchain technology, Decentralized ledger, Healthcare data management, Privacy, Security, Smart contracts.

INTRODUCTION

Blockchain technology is a decentralized platform that uses a collaborative distributed ledger system. It was initially created by Satoshi Nakamoto in 2008 for financial companies, but it has now become a fundamental technology for various decentralized applications [1]. Blockchain is the amalgamation of encryption and

[*] **Corresponding author Anita Tanwar:** Chitkara Business School, Chitkara University, Rajpura, Punjab, India; E-mail: anitatanwar.ggn@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

noble technology for communication. The system is composed of many blocks that are interconnected using hash functions based on cryptography. The blockchain is an important yet resourceful technique for transmitting and receiving data in an efficient and highly secure manner. Anyone involved in a transaction initiates the process by creating a block. A multitude of machines are distributed everywhere on the net that verify the block (Fig. **1**). The verified block is appended to a blockchain, which is subsequently distributed over the internet, creating both a singular and distinctive record with a unique historical trail. Therefore, in the context of blockchain technology, transactions are deemed genuine when there is a consensus among blocks, which is achieved through contractual agreements. The decentralized characteristics of blockchain technology result in the decentralization of trust, making trust between system users crucial for issuing keys [2].

Blockchain has undergone significant evolution throughout the years. We categorize blockchain into five distinct versions, referred to as blockchain technology 1.0 to 5.0. The initial iteration of the blockchain, known as blockchain technology 1.0, was developed by Nakamoto. It serves as a fundamental decentralized ledger system that facilitates transaction tracking and data storage across several devices. Simply put, the data stored in the original blockchains was limited to the intrinsic worth of an object that saw shifts in ownership during its lifespan. The entity we are alluding to was commonly a type of virtual currency, like dogecoin, ripple, and similar variants. Blockchain 2.0, commonly referred to as the emergence of Ethereum, is an upgraded iteration of cryptocurrency [3]. Ethereum was the pioneering blockchain that incorporated an integrated virtual technology for smart contracts. Smart contracts are an array of programs that are immediately performed when certain conditions are fulfilled, in a nutshell. These agreements let people or corporations conduct more intricate transactions beyond basic cryptocurrency trades. It is well-suited for applications that involve decentralized distribution and decentralized autonomous organizations. Blockchain 3.0 encompasses a broader series of applications, particularly in the realm of enterprise blockchain. Blockchain technology 3.0 encompasses several applications, such as healthcare, supply chain, cybersecurity, and manufacturing. Blockchain 4.0 now facilitates the implementation of industry and healthcare 4.0. Its objective is to optimize the experience of users inside the industry. Rchain and Metaverse are examples of blockchain technology 4.0 platforms. Blockchain technology 5.0 refers to the latest or current iteration of blockchain technology. The objective is to mitigate the conventional limitations and security concerns associated with blockchain technology. Relictum Pro, Hedra, and Hashgraph are typical applications of Blockchain 5.0 [4].

After traditional health information exchanges (HIEs) and health record-based exchanges failed to fulfill the claim of a common coalescent, blockchain technology presented a promising alternative. Various causes, including medical records that are electronic, competing goals, and others, keep bringing attention to the problem that comes with traditional health data exchange intermediaries [4, 5]. The healthcare industry is now front and center as a potential use case for blockchain technology. We can see a high-level picture of blockchain pertaining to healthcare. Patients and doctors are the data generators in the healthcare blockchain, together with medical cloud computing and the network of blockchain connections that houses the smart contracts. The worldwide Google Trends for the term "Blockchain - Healthcare" indicate a noticeable uptick in interest from academics.

Safety, interoperability, medical data transfer, and mobility are the different requirements of the healthcare division. The collection of healthcare statistics in the framework of the Industry 4.0 revolution takes place through files, devices with sensors, and various other applications. Electronic Medical Records, Health information technology, and Individual Health Records are the three types of digital health records. For such data, restricting access with suitable authentication is important. Additionally, the search performed for obtaining medical data needs to be tested with adequate access restriction to avoid management attacks [6]. Furthermore, encrypting is a poor method of protecting medical documents.

Also, encoding is a poor method of protecting medical papers. Interoperability difficulties arise when several encoding methods are designed to encode several types of medical records [7, 8]. Inadequate security of healthcare information also results in a number of privacy issues [9 - 11]. Another crucial prerequisite for healthcare records is interoperability. Interoperability is the ability to integrate and transfer data across diverse sources [12]. The utilization of central loading for data is the foundation of interoperability. Healthcare storage of data presents a challenge since centralizing all of the data might result in sluggish access, safety issues, and issues with privacy. Since healthcare data typically grows over time, it is not practical to send all of the data to central processing *via* untrusted networks. The centralized organization of the data makes it difficult to obtain in an efficient and safe way. Various scientific projects require the sharing of health-related information; thus, it is very tough to guarantee accessibility, consistency, and scalability when doing so [13, 14]. Patients havebecome more and more independent and demand that their medical information mobility becomes more and more important in the field of healthcare. With the increasing prevalence of sensors and smart devices linked to the internet, data transfer capacity is becoming more and more important.

CHAPTER 4

The Application of Blockchain Technology in Medical Credential Verification and Fraud Prevention

Prabh Deep Singh[1], Riya Sharma[2,*], Kiran Deep Singh[3] and **Meenakshi Mandola[1]**

[1] *Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[2] *Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[3] *Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Rajpura, Punjab, India*

Abstract: Blockchain technology is an innovative concept in the financial and computer fields. In view of medical treatment, medical information, and the authenticity of medical staff, it involves the vital interests of the personal and financial security of every patient diagnosed and treated in a medical institution. By sorting out the relevant research at the institutional level, it is found that blockchain technology has not yet been established as an industry standard, and there is significant room for development in the medical industry. Based on the advantages of advanced technology, the introduction of relevant application performance of blockchain technology in the latter part of this paper expounds the method and process of medical staff credential verification and medical fraud prevention. This chapter is based on the blockchain technology of avoiding the inconvenience, long time, and high cost of medical staff qualification review in a traditional management method with the advantages of tamper resistance, traceability, sharing, privacy protection, and new auxiliary to improve the traditional cross-independent credential verification mode. It further provides a method for preventing fraud in the cross-independent medical diagnosis and treatment process. The significance of this research is to enhance the intelligent and digital level of medical management and increase the confidence of management decisions at the utmost. Finally, the conclusion and prospect are drawn, and at the same time, the application of blockchain technology in the field of transaction settlement, clearing, and other basic application fields is prospected.

Keywords: Auditing, Blockchain, Drug abuse, Efficient employment, Fraud prevention, Healthcare, Medical ID theft, Medical credential, Non-repudiation.

[*] **Corresponding author Riya Sharma:** Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India;
E-mail: riyasharma6568@gmail.com

INTRODUCTION

In the emerging digital economy, e-commerce transactions, electronic document signing, and online voting have become popular applications over the internet. Trust in the Internet has become a concern, especially in electronic business and transactions. In general, users seek secure systems in which to conduct their online transactions. The use of blockchain technology (BCT) can satisfy these needs. Currently, it has been actively applied in finance, supply chain, Internet of Things, energy, and other sectors. However, security issues of personal data have attracted much attention from the public. Medical personnel may provide fake diplomas or practice without certification. Patients can be harmed if they are treated by these unaccredited personnel. To prevent these problems, the verification of medical personnel should be established. Therefore, this research applies BCT to protect the personal data of certified medical personnel from being hacked and enables secure access to this data. In addition, when lying about diplomas to medical organizations or insurance companies to get paid, individuals with the wrong data can be verified quickly. The blurry coalition by threshold secret sharing (BCTSS) technology is applied to protect the diploma patient's decryption condition access structure key. The access control and authority flow are also utilized to manage the personnel's credentials. Finally, we propose a smart contract for rapid medical-credential verification. The proposed system enhances the security of the diploma, as shown by the experimental results. It prevents anyone from holding all decrypted data, and only the required number of appointed members can decrypt the data.

Definition and Key Concepts

Blockchain is a particular type of distributed ledger technology (DLT). Specifically, it refers to a shared, replicated, permissioned, append-only digital ledger that is secured by cryptography. Organizations use it as a tool for creating a database or ledger shared across multiple entities. Information is held in the ledger in packages known as blocks. Each block holds a set of data, and all are identified by a unique cryptographic identifier that links it to the previous block, creating the chain [1]. Information is publicly available, and no single entity controls the chain or data. Data is confirmed by consensus, meaning that all entities within the blockchain must approve data entries, preventing a single actor from introducing incorrect or fraudulent data. This makes blockchain information stored therein extremely difficult to tamper with and effortless to use. The range of potential applications for blockchain is considered significant [2]. Healthcare has been established as a plausible use platform for blockchain, offering many groundbreaking advantages such as a solution to mitigate disjointed patient data and maintaining accurate records for protection [3]. Since pharmaceuticals and

medical devices are prone to and at risk of counterfeiting, blockchain can portray a mechanism to reduce the incidence rate and the negative effects of counterfeiting. Blockchain can be interestingly used to handle exclusive medical credential verification and avoid duplicate medical imaging datasets in this realm. Blockchain will be a possible platform for the validation of medical certification, prevention of fraud, and the abolition of duplication of radiological imaging datasets. The opportunities and challenges in the coupling of blockchain in the personalized medicine system are also discussed in this paper.

Fig. (**1**) represents the architecture of a blockchain-based healthcare credential verification system. The user interface and healthcare institutions interact with the blockchain network, which includes a smart contract layer. This layer manages the credential storage, verification, and access control modules, ensuring secure and compliant verification of healthcare credentials.

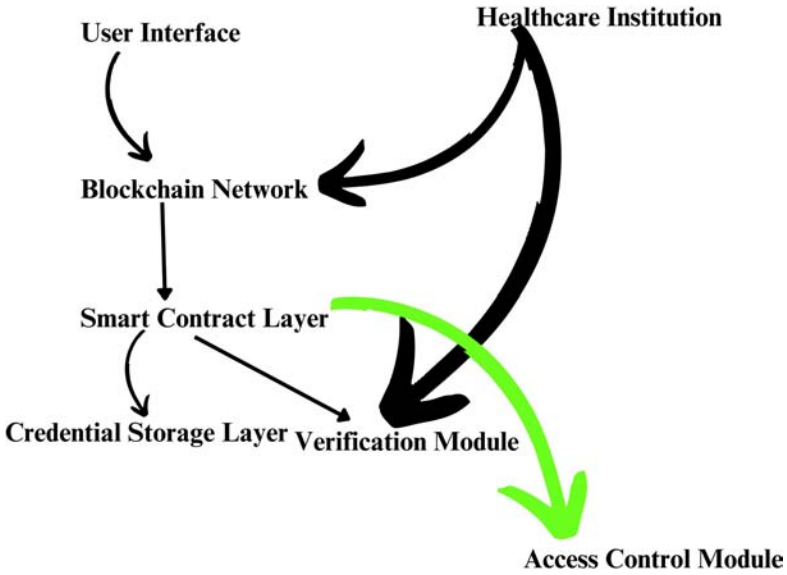

Fig. (1). Blockchain-based healthcare credential verification architecture.

BASIC PRINCIPLES AND FUNCTIONALITY

The basic concept is to create a distributed ledger through a network that operates under a certain consensus algorithm. This chain of blocks is ever-increasing, which directly solves the problem of single points of failure. Each new block contains within itself a reference to the previous block, creating a timeline through the blocks. Importantly, establishing consistency and integrity of data is the responsibility of multiple parties, rendering it difficult to alter any data once it has been included in the chain. The process of adding data to the blockchain is done

CHAPTER 5

The Impact and Implementation of Blockchain-Based Solutions for Efficient Electronic Health Record (EHR) Management

Kiran Deep Singh[1], Sharon Christa[2,*], Pardeep Kumar Jindal[3] and **Garima Sharma[4]**

[1] *Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Rajpura, Punjab, India*

[2] *Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune, Maharashtra, India*

[3] *Department of Electronics and Communication, Chandigarh Engineering College, Mohali, Chandigarh, India*

[4] *Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

Abstract: An electronic health record (EHR) system can facilitate complete and accurate patient information to authorized users and can help organizations and service providers gain improved productivity. Furthermore, the doctors can effortlessly access the records of the patients, including medicines, medical records, and laboratory results, resulting in more conversant decisions along with improved care. The EHR technology improves patient care, which allows for better patient engagement by the medical practitioners. With this technology, patients can easily get their medical records, which further aids in taking active care of their own health. The technology of EHR permits real-time availability of scientifically-proved tools, permitting providers to make better decisions on the health of the patient. EHRs improve patient safety by reducing the likelihood of duplicate tests and medication errors. However, the global implementation of EHR systems is still facing multiple challenges due to the underlying issues related to security, data integrity, and privacy preservation. Several EHR security issues are mainly associated with centralized data storage systems and their integrators/providers. The decentralized control and access capabilities of blockchain can offer a suitable solution to EHR security and data management issues. This paper examines the challenges associated with EHR systems and solutions based on blockchain, which can be used to overcome the barriers related to data security, integrity, and patient ownership. Finally, through the review of two EHR blockchain application areas, it is illustrated how research can provide various applications and propose openings for related debates and research to highlight future directions.

[*] **Corresponding author Sharon Christa:** Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune, Maharashtra, India;
E-mail: sharonchrista@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

Keywords: Blockchain, Electronic health record, Patient information, Security.

INTRODUCTION

The rise in corporate data breaches, cyber-warfare, and quickly evolving sophisticated hacking methods is alarming, enabling the fast passage of regulation and enforcement that carries significant costs in terms of compliance, risk mitigation, and the policing of the digital economy. Further complexity is generated through the increased globalization of business and society. The primary strategies that have emerged to meet these challenges are centralization in all forms, such as data centers and cloud storage solutions, and the excitation of cyber security and information assurance at the system, software, hardware, and network levels [1]. Unfortunately, these strategies result in the creation and operation of data silos through restricted centralization methods that prohibit distributed management practices and threaten the privacy and sovereignty of the data's owners, creators, and subjects, as well as every intermediary actor involved in their access, processing, and distribution. On the other hand, the secondary field of cryptography is derived primarily from mathematics and involves the application of computational systems for the transformation of data in order to achieve selective information disclosure and the mathematical modeling and automatization of 'trust' and the design of 'secure' systems [2]. However, this field remains conceptually complex as it embroils the following elements: distributed parties that communicate; long-standing promises of collision resistance, security, and identity of electronic and virtualized objects; automation, identification, and encryption tools; and the properties of 'simplicity' and 'reliability' that are based on mathematical algorithms. Notably, these privacy practices are highly valued in economic terms, which generates demand [3]. In the more general context of computer science and distributed systems, there is an inability to deploy, enact, and manage the explicit, ongoing function adhesion of these properties at the scale of complexity and diversity required to be seamlessly interoperable with the vast range of existing systems and actors.

Background and Significance of EHR Management

Electronic Health Record (EHR) management is a critical function in healthcare. One of its primary benefits is that it provides authorized users with access to their patients' health information at all times [4]. It enables real-time, secure, and accurate access to health information required for the management of care delivery services. The access may involve patients themselves, health professionals, and other healthcare providers within and outside the facility where the patient received care services. They can quickly and securely retrieve and review the patient's health information to diagnose and treat the patient

accordingly. In addition, in any case that requires immediate attention for critical diagnoses and treatment, authorized health professionals can quickly access patient health information [5]. Moreover, EHR is a critical source for clinical research and population health management. Properly formatted patient data in electronic health records can advance evidence-based research and contribute to the creation of effective healthcare solutions optimized for patients' specific treatments, medications, and protocols. These benefits mean that the management of EHR should emphasize efficient, secure, and real-time accessibility, integrity, and reliable information. To meet these requirements, the traditional central server-based EHR systems are not suitable. An EHR central server-based solution is implemented that has encountered significant challenges, both in addressing user on-demand real-time access to health information and concerns about health record data ownership, integration, security, auditability, and interoperability in the main system [6].

Overview of Blockchain Technology

Blockchain, by its most useful definition, is a collective agreement method with which the global state of networked message contents can be maintained. The participants interact by either using a network protocol with which aggregated data services can be performed, updating its network, and/or confirming the addition of a new work or message. What makes blockchains really special is that anyone can download a complete state of the network, and the reader of a complete state, hereafter a node, will locally validate the state [7]. The main drivers of this and the success of blockchains are the automatic completeness, correctness, security, and integrity of the replicated database that the nodes together maintain, the cryptographic chaining of blocks of transactions to ensure the integrity of the network combined with ensuring their public, global uniqueness, and the ability to create hierarchical blockchains using Positional Based Navigation (PBN) to bootstrap the management of the initial database that was initially applied to create the first blockchain of Bitcoin. Blockchain technology is notable because it is self-contained; the implications propagated through the blockchain to all participants generally hold – since we assume the link installers of the blocks to be trustworthy [8]. If we use a commonly accepted mechanism, we can use any blockchain effectively without having to rely on a third party in order to administer it. Since this feature is mandatory, we can isolate the design of the inserting mechanism and consider independent blockchains within the same system, allowing us to focus on their contents.

UNDERSTANDING ELECTRONIC HEALTH RECORDS (EHR)

An electronic health record (EHR), or a personal health record (PHR), refers to

CHAPTER 6

The Impact of Blockchain Technology on Streamlining Insurance Claims

Riya Sharma[1,*], **Sharon Christa**[2], **Deep Mann**[3] and **Rajbir Kaur**[4]

[1] *Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[2] *Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune, Maharashtra, India*

[3] *Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala, Punjab, India*

[4] *Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India*

Abstract: Blockchain technology has witnessed a significant level of curiosity from several industries, including the insurance sector, in relation to extensive applications in claims management processes. In the present study, a blockchain-distributed system for the insurance sector is proposed, which utilizes smart contracts to create valid insurance policies. Blockchain, being a distributed ledger, has several advantages and disadvantages, which are explained in detail. This system provides mechanisms that automate the complex processes of claim settlements, ensuring appropriate compensation to claimants and verifying the conditions and terms of insurance policies on the occurrence of a specific unforeseen event. Data retrieved from a real case has been used to consolidate the assessment of the approach proposed here. The profitability and sustainability of the insurance sector are underpinned by a smooth claims process. Traditional techniques for the adjustment of insurance claims are responsible for high administrative costs and the payment delays that occur after unforeseen events have occurred. Inefficient communication channels lead to conflict and civil fragility in the sector. However, traditional models have shown that the efficiency of the claims process can be improved by the adoption of modern digital technologies, notably the use of blockchain protocols. Blockchain is expected to streamline the end-to-end operations of insurers, thereby reducing the churn rate and enabling value-based partnerships. This chapter develops a reference framework with functional and non-functional requirements for Blockchain-based Accredited Parametric Insurance (Blake) that will ensure the on-time payment of rightful beneficiaries.

Keywords: Blockchain technology, Claims management, Insurance claims, Insurance, Smart contracts.

[*] **Corresponding author Riya Sharma:** Graphic Era Deemed to be University, Dehradun, Uttarakhand, India; E-mail: riyasharma6568@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

The insurance business has a long and storied history, having existed in some form, at least since the early days of the written word. For millennia, the fundamental mechanisms underlying insurance have remained remarkably consistent [1]. But today, we stand poised on the precipice of an inevitable, remarkable change. With time, what elements of traditional insurance models will remain intact for the duration will be revealed. Blockchain technology is a distributed ledger that is spearheading a revolution in the financial world today, providing an unparalleled level of trust among untrusted parties. We look at how it is uniquely positioned to bring radical efficiencies to insurance, particularly in the claims and billing processing area. The basis of Blockchain technology can be traced to an article written by two researchers titled "Blockchain – A Brief Introduction" and "Blockchain – A Supporting Technology in Case of Supply Chain Finance?" in 2011. Blockchain technology is a distributed ledger that is secure, transparent, and immune to fraudulent changes [2]. Entries are highly secured using a cryptographic hash. Any new entry created uses the hash of the previous entry. It is used across continents, bridging supra-national borders. There is no central location or a central trust anchor in the blockchain. A list of records – blocks- is used to track transactions across all the ledgers. A sharp token or a cryptographic hash is used to define the previous block. Blockchain is secured using cryptographic techniques. Specially designed consensus algorithms are used to elect a controller among the blockchain transactions [3]. It can be implemented through distributed or decentralized models. The blockchain system is open for participation, which enables innovations and technical developments through community participation. Small agents and the general public are provided with enormous benefits through consumer digital services. Blockchain, being a distributed ledger, has several advantages and disadvantages, which are explained in detail.

Definition and Key Concepts

Millions of work hours are spent working with manual, paper-intensive processes in the insurance industry. Fortunately, emerging technologies such as blockchain have the potential to address these challenges by streamlining and automating separate insurance processes, from claims, billing, and investing to reporting and compliance [4]. This particular report examines the use of blockchain technologies in streamlining the insurance industry's claim and billing process. It discusses the advantages provided by blockchain technology and the challenges that need to be understood and resolved. The report also includes prototype models and application patterns used to deploy blockchain to streamline the claim and billing processes. Blockchain provides new technologies for solving this

problem and uses a decentralized platform to update transactions from stakeholders. Blockchain applications in the insurance industry can help speed up and automate certain processes, eliminate the need for trust building between parties in a deal, reduce the number of compliance violations, and decrease costs and complexity [5]. It is possible to release resources from these calls so they can be used with expertise. Blockchain is an implementation of this concept. This technology enables network participants who do not know each other to establish a decentralized information exchange process, create control among participants, and avoid planned activities that would otherwise take place between participants and third parties (such as shareholder registration agencies, banks, and operations). Due to these advantages, insurers see the value of embedding it into their business processes.

CHALLENGES IN INSURANCE CLAIMS AND BILLING PROCESSES

Since the earliest times of human civilization, people have always faced unexpected possible losses or damages in their lives, leading to the creation of contractual relationships to exchange economic risk. Insurers assume a variety of risks of loss due to hazards and perils. Insurance services have become essential for individuals and organizations globally, providing coverage for possible losses in defined conditions. They can be inclusive of life, health, property, accident, and liability insurance. Various contractual relationships can be created between insurers and respective individuals or organizations to provide insurance services [6]. Claims and billing management are essential processes for the insurance industry. Quick and precise claims and billing management processes can be differentiators for an efficient and excellent insurance company. These processes become fundamental to be performed in hours or days to prevent dissatisfaction and reputational risks. Claims are intended to compensate insured parties for the accidental loss of covered hazards. After incidents happen, the insureds or their representatives inform the insured insurers about those happenings, starting the claims management process. For valid claims, the insurers provide an indemnity payment to the insured and, if applicable, to the third-party claimants [4]. Claims are not only linked with charges but can also link insurers with sophisticated law litigations. Therefore, insurers often have claim units specialized in claims management and, if necessary, in the assurance of appropriate trials. However, not all claim reports may result in a claim file; sometimes, these can just represent fake or unqualified claims. Billing management is the process by which insurance consumers receive and handle invoices from insurers, mainly regarding policy renewals or the invoicing of additional premiums. These invoices shall be received, supervised, and paid when the insurance contract is adjusted. When an insurer discovers errors in previous payments, refunds or charges are invoiced and processed. Both claims and billing management processes are administrative and

CHAPTER 7

Smart Contracts and Healthcare Transactions

Keesara Sravanthi[1], P. Prasant[2,*], Rajeev Kumar Bedi[3] and **Navneet Kumar Rajpoot[4]**

[1] *Department of Information Technology, VNRVJIET University, Hyderabad, Telangana, India*

[2] *Department of Computer Science, AIPH University, Bhubaneswar, Odisha, India*

[3] *Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Jalandhar, India*

[4] *Department of Computer Science & Engineering, Graphic Era (Deemed to be University), Dehradun, India*

Abstract: This chapter delves into the transformative role of smart contracts within healthcare transactions, emphasizing their potential to streamline processes, enhance data security, and optimize patient engagement. Built on blockchain technology, smart contracts automate agreements with embedded terms in code, offering a more secure, efficient, and transparent alternative to traditional methods. This study highlights the benefits of smart contracts in patient record management, insurance claim processing, and supply chain logistics, addressing critical challenges like high implementation costs, technical integration, and regulatory compliance. By exploring both opportunities and hurdles, this chapter provides insights into the future of smart contracts in the healthcare sector. This chapter is aimed at bringing a comprehensive view of smart contracts and their potential to transform healthcare transactions. The objectives of this chapter include exploring business opportunities of smart contracts and enhancing health products and services in the areas of electronic health records and processing of insurance claims. Further, the deployment of smart contracts will be evaluated with respect to risks, challenges, and ethical considerations for data privacy and regulatory compliance. It also evaluates the cost-benefit analysis that deals with financial implications and return on investment. Examples from the real world, along with future trends of applicability, practice, and novelty in this area, are addressed at the end of the chapter on the use of smart contracts in healthcare.

Keywords: Automation, Blockchain technology, Data privacy, Healthcare efficiency, Healthcare innovation, Healthcare transactions, Insurance claims, Patient data security, Regulatory compliance, Smart contracts.

[*] **Corresponding author P. Prasant:** Department of Computer Science, AIPH University, Bhubaneswar, Odisha, India; E-mail: pprasant@aiph.ac.in

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

INTRODUCTION

Smart contracts, developed on blockchain technology, represent a radical development associated with the management of healthcare transactions. They are self-executable contracts with directly embedded terms in code, thus making them efficient, secure, and transparent. Considering that the sector is heavily burdened by administrative complexities, high costs, and data privacy problems, smart contract implementation is likely to be very effective. Smart contracts have already established themselves in areas like patient record management, insurance claims, supply chain logistics, and other processes that have many intermediaries involved and are prone to errors. This chapter reviews smart contract capabilities to make a change in healthcare, explaining the technical grounds of their diverse applications and related benefits and addressing the challenges and future directions in this innovative field.

Structure

The chapter first discusses the opportunities and challenges in healthcare transactions, followed by enhancements to healthcare products and services, risks and challenges of implementing smart contracts, ethical and regulatory considerations, and utilization and cost analysis of smart contracts.

Potential of Blockchain in Healthcare

Blockchain holds immense potential to reshape healthcare by enhancing security, transparency, and efficiency in managing sensitive data and transactions. At its core, blockchain offers a decentralized, tamper-resistant system that can transform how patient records, insurance claims, and supply chains are managed, reducing reliance on intermediaries and lowering administrative costs. Smart contracts, a key feature of blockchain, can automate processes like insurance payouts and consent management, allowing instant, secure actions based on pre-set conditions. For patients, this means greater control over personal health data and assurance that information is securely stored and accessible only with permission.

Opportunities and Challenges in Healthcare Transactions

Opportunities

Streamlined Operations through Automation

Smart contracts in the operations of healthcare can revolutionize operations through a lot of routine procedures that make workflow easier and reduce many burdens of administration. Conventional health systems are characterized by

manual operations, especially in areas such as patient registration, billing, and record keeping. These activities are very time-consuming, besides being prone to human error, hence giving rise to inefficiencies and inaccuracies.

These processes are automated using self-executing code under smart contracts. In the case of patient registration, smart contracts can automatically verify insurance details, fix appointments, and update the records of patients without human intervention [1]. The automation guarantees that all the steps involved in the process are efficiently followed, thus avoiding delays and reducing administrative workload.

One practical example of this is in the area of billing and insurance claims. Today, underwriting processes within the insurance industry are very hands-on; every claim made requires submission, verification, and subsequent reimbursement, which generally goes through a wide number of intermediaries, and involves a great deal of paperwork and information control. With smart contracts, once the healthcare service is rendered, the contract is executed—that is, a claim is automatically generated, with all the details verified against the patient's insurance policy for its viability, and upon approval, payment is then made. It reduces the time taken for reimbursement and also minimizes fraudulent cases involved in claims since everything is recorded on the blockchain and is transparent and immutable [2].

Enhanced Data Security and Privacy

Security and privacy in healthcare, with regard to the sensitivity of the patient's information, are paramount. Any traditional health system is easily prone to data breaches and undesired access, leading to huge financial and reputation losses.

Hybrid coordination, in which the Proof of Work (PoW) and proof of Stake (PoS) layers cross-verify each other's outputs, just adds another layer of redundancy to prevent manipulation by the entire system from one single entity. Implementations in the real world of hybrid consensus mechanisms have shown a potential yet still a considerable area of improvement. Ethereum 2.0 would replace the traditional PoW consensus algorithm and function as a hybrid system, adding more layers of security, while the scalability of Komodo, a blockchain application, would rely on its notarized checkpoints alongside PoW.

Looking forward, hybrid consensus mechanisms must balance scalability and security trade-offs such that increasing the capacity of transactions does not weaken the robustness of the system. Moreover, energy efficiency continues to be a significant challenge for hybrid models because they want to reduce the energy-intensive demands of PoW while ensuring reliability and decentralization, which

CHAPTER 8

The Role of Smart Contracts in Ensuring Regulatory Compliance in Blockchain Healthcare Systems

Riya Sharma[1,*], Prabh Deep Singh[2], Rohan Verma[2] and **Deep Mann[3]**

[1] *Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[2] *Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[3] *Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala, Punjab, India*

Abstract: In the last decade, blockchain technology has evolved in various applications, especially in healthcare systems where decision-making needs to be reliable, secure, and transparent. In these applications, the main concern is the storage and transfer of the patient's medical data to offer solutions for data privacy, user control over their data access, and satisfying regulatory compliance. Moreover, due to the need for security assurance and integration with other systems, *i.e.*, traditional healthcare systems, the platform needs a system that, in addition to storing the data, can be able to simplify exchange and manage patient data records through collaboration with smart contracts. This chapter considers the constraints surrounding the role and growth of blockchain smart contracts in promoting healthcare regulatory compliance, positional questions that are yet to be resolved or explored, and boundaries in the underlying structure of international regulatory policies. The chapter introduces the methodological issues inherent in the process of resolution of regulatory compliance. The main purpose is to help system designers understand how to systematically evaluate how blockchain-based systems comply with General Data Protection Regulation (GDPR) requirements. Further the study proposes a set of smart contracts for a blockchain-based healthcare data exchange aimed at the resolution of regulatory compliance accounting issues.

Keywords: Blockchain technology, Decision making, Data privacy, Healthcare systems.

[*] **Corresponding author Riya Sharma:** Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India; E-mail: riyasharma6568@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

INTRODUCTION

Blockchain technology is intended as an advanced tool with the ability to resolve difficulties linked to safety, data sharing, and compliance with regulatory standards across healthcare organizations, jointly offering the essentials necessary for current electronic health records and management systems and trying to mitigate electronic healthcare data transfer and access constraints [1]. In essence, a public record is used by multiple nodes to collectively record a range of operations by forming a digital sequence. A blockchain is a decentralized and distributed ledger. Each portion of this sequence, known as a block, is connected to the preceding one, constructing a lengthy and untampered lineage chain [2]. The chain serves both as an anchor and archive of transactions' history, safeguarding contributed contents against internal or external cyber threats. Many healthcare utilizations have been recommended. Given the different blockchain abilities to establish and maintain longevity and protect or verify transmitted data, as well as its ability to automate and validate various procedures, these plans can result in substantial advances in healthcare data management.

The blockchain's custom-designed smart contracts might address several compliance issues and extend assured advantages to healthcare, including healthcare providers and patients. Intended regulatory measures are required for management and information structures that blockchain can automate. Furthermore, smart contracts might also create opportunities and consequences for non-compliance, resulting in potentially increased data integrity through enhanced consistency of process control and the capacity to disclose reliable results [3].

Fig. (**1**) illustrates the process of managing healthcare data using blockchain technology. The patient provides health data to the healthcare provider, who encrypts and stores the data on the blockchain. A smart contract is executed to ensure compliance, validate data access, and notify authorized entities.

Background and Significance

Several interdisciplinary studies [4, 5] on regulatory guideline level approaches permit integration with blockchain systems that influence the laboratory medicine environment. The usage of smart contracts in the defined scope of regulatory compliance in healthcare blockchain systems or mechanisms to ensure data integrity or even proof for longer than a year remains a gap that will not be addressed by existing research in the current field [6].

Looking exclusively from the standpoint of the blockchain operational integrability with a specific, national eHealth system development, they have also

identified that immediate policy change support is required from additional legislative documents, linking the activities with international priorities such as the Digital Single Market Strategy published by the European Commission" [7].

The usage of blockchain in healthcare is on the rise due to the underlying principles such as security and anti-tampering, confidentiality, distributed verification, and storage of data or event provenance. However, the need to comply with different data protection laws and regulations indicates that the adaptation must be highly intricate or intricate in a well-defined manner. More concretely, research indicates that smart contracts are decentralized, transparent, and secure tools, capable of automatically resolving the actions that are predefined by the contract parties without any intermediaries at a very low cost. This study can also support the understanding of strategic adoption, system audits, or blockchain conceptualization and design work.

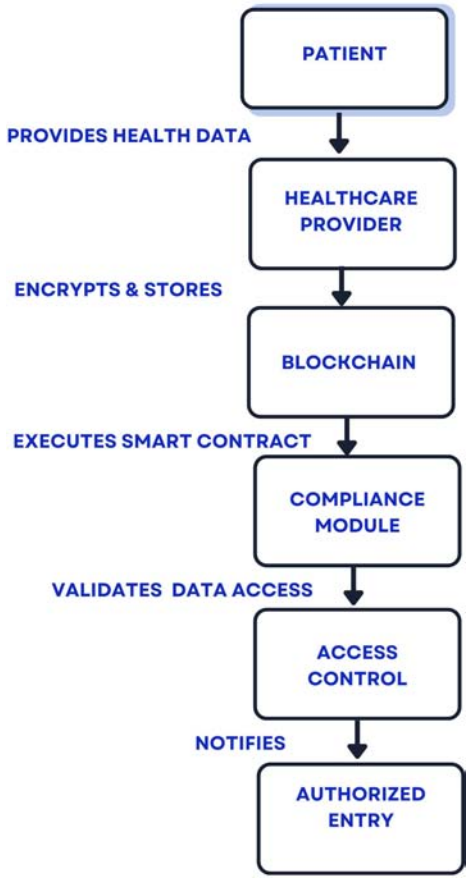

Fig. (1). Blockchain-enabled healthcare data management.

CHAPTER 9

Exploring the Intersection of HIPAA Compliance and Blockchain Technology in Health Information Systems

Prabh Deep Singh[1], Kiran Deep Singh[2], Riya Sharma[3,*] and **Sharon Christa[4]**

[1] *Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[2] *Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Rajpura, Punjab, India*

[3] *Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[4] *Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune, Maharashtra, India*

Abstract: The healthcare industry's transformation into an information-rich world has led to an unprecedented level of data availability and data sharing, thus encouraging the development of sophisticated information-sharing platforms facilitated by technologies such as blockchain systems. Standard health data models like Fast Healthcare Interoperability have been raising issues more crucially regarding data security, managing and controlling different types and levels of access privileges, and ensuring that sensitive health data is access-controlled according to HIPAA regulations. A trusted blockchain maintains its decentralized and tamper-proof characteristic and enables its participating stakeholders to share and/or store information. Consequently, it is anticipated that this technology may have a fruitful effect on healthcare applications. These distributed systems, which are comprised of ever-growing unchangeable transaction records, ensure security in data storage and exchange processes. However, the advantages gained from applying blockchain to healthcare create fundamental challenges in terms of security and privacy. To date, discussions focused on the intersection of the private healthcare sector with blockchain technology have been quite limited. This research, therefore, examines how the principles of the Health Insurance Portability and Accountability Act (HIPAA) can be aligned with blockchain technology in health information centers. Consequently, the research not only has implications for companies, especially health information centers and blockchain developers, but will also inform regulatory bodies as they deliberate on updating the rules governing privacy, healthcare technology, and use.

* **Corresponding author Riya Sharma:** Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India;
E-mail: riyasharma6568@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

Keywords: Blockchain systems, Data availability, Data security, Distributed systems, Healthcare transformation, Information sharing.

INTRODUCTION

Health information systems (HIS) are becoming more integrated and centralized with the advances in technologies and regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The access control framework of HIPAA has some security requirements that make this control in HIS more complex, difficult, and sensitive [1]. Moreover, the frauds and breaches of privacy in the healthcare system are increasing, and the importance of HIS for humans in preserving their health has been growing with new care available, preserving secret health data, like self-aware systems, that provide consultation and automated healthcare. This paper discusses the Health Information System's security problem using the concept of Hyperledger, a hybrid permissioned blockchain as private, private-permissioned or permissioned-public, which possesses high alteration and confidentiality in local access and a sustainable level of decentralization [2].

The adopted approach uses the Hyperledger Caliper from the Hyperledger project, which is a benchmark program to assist clients in calculating their capacity to use blockchain in a transactional system, supporting developers to choose the best framework through benchmark comparisons, and the FlexSCIB, a two-level Sensitive Information Model that makes it easier to understand and operate with healthcare information and its sensibilities, furthering its correct model and enabling improved access control [3]. The computational replica used was implemented through Blockchain Explorer, a live demo tool of Hyperledger. The obtained results showed that all requirements established by the benchmarking target were met and surpassed with successful compliance with access controls and sensibilities of patient history data. The response time to the transaction was 100% of committed transactions, and the ratio of private transactions remained less than 1% for both in the current configuration (high performance) for the considered blockchain. The system resiliency was reached with no partition. The observer (compared to the verifier) results were consistent and reliable (consistency test passed).

This paper follows the following structure: In Section 2, the background and research problem are discussed, followed by state-of-the-art and related work in blockchain and HIPAA and the adopted methodology and Hyperledger Framework in Section 3. In Section 4, the Sensitive Information Model is depicted, and the experimental setting is exposed. Section 5 reports the obtained results, and Section 6 ends with our outlook on the results and future work.

Background and Significance

ProgressHUD is a lightweight and easy-to-use HUD for iOS. This demonstrates how to use it on NimbleHQ's latest jobs, and it only takes a couple of minutes to install and set up. It is about the installation of technology in a hospital facility. When a change in the measured features is detected, the cardiac device's wireless transmission of the patient's vital signs becomes a sequence of alert alarms [4]. Physicians, an important target of the alerts, cannot access any of these data on any of the hospital's PCs while still on the hospital campus. The protection of electronic health records and data in health information systems is in line with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which safeguards the confidentiality, integrity, and availability of an individual's health records. Blockchain technology, on the other hand, is a relatively new concept that is garnering attention from various fields. It has the potential to provide a secure layer for electronic health record access in decentralized environments and address security, integrity, data management, and many of the existing challenges in health information systems [5]. However, the capability of blockchain with respect to the implementation and compliance of HIPAA standards has not been researched thoroughly in the current literature. Additionally, as blockchain is not fully regulated, it is particularly essential to pay attention to data privacy and confidentiality regulations when deploying it in healthcare. In this paper, we review HIPAA compliance with telecommunications, storage, and blockchain basics and then explore the intersection of HIPAA compliance with the current capabilities of blockchain technology in enabling the secure sharing of electronic health records.

Purpose of the Study

This examination using the grounded theory method was performed because of its ability to develop theoretical frameworks based on data derived and validated from intense research within a domain. The results' quality comes from the methodological fact that inquiries rely on the industriousness in the research laboratory to construct useful and interesting explanations of how non-technical people working at an organization with mission-critical information security responsibilities construct, tack up, and evaluate their internal audit staff to support their chief executive's, board's, and shareholders' intent. They are given the opportunity to face the realities of actual corporate practices by laptop tests to test models that dissatisfy the attractiveness of theoretical and postulated hypotheses through qualitative research. The use of case-oriented methodologies in the inquiry permits what has not been allowed to date in hypothesis testing in broad general classificatory studies. This rigorous inquiry asks radical questions about what a relatively little-studied population in information security is. The purpose

CHAPTER 10

Securing Healthcare Data: Privacy and Regulatory Compliance Through Blockchain

Sandeep Singh[1], Sonal Rattan[2,*], Varinder Pabbi[3] and **Navneet Kumar Rajpoot[4]**

[1] *Department of Computer Science Engineering, SGT University, Gurugram, Haryana, India*

[2] *Department of UCRD and Apex Institute of Technology, Chandigarh University, Mohali, Punjab, India*

[3] *Department of Computer Application, I. K. Gujral Punjab Technical University, Phagwara, Punjab, India*

[4] *Department of Computer Science & Engineering, Graphic Era (Deemed to be University), Dehradun, India*

Abstract: Blockchain technology has a solid base to improve privacy and compliance in healthcare. Its basic features—immutability, decentralization, and transparency—are most of the issues related to the management of sensitive health information. The health sector has been swamped with many challenges to the assurance of privacy and regulatory compliance. This chapter, with an insight into the basic concepts and types of blockchains, elaborates on the ability of healthcare organizations to make use of this technology for protecting data security by ensuring compliance with set regulations and creating trust among stakeholders. Blockchain technology will be central in the evolving healthcare sector for protecting patient data while increasing quality care. This chapter explores the vital role of privacy and regulatory compliance in the healthcare sector, focusing on the protection of sensitive patient data in an increasingly digital world. As healthcare providers adopt technologies like blockchain, safeguarding data from unauthorized access and ensuring regulatory adherence become paramount. Key regulations such as HIPAA, GDPR, and the HITECH Act are examined alongside challenges posed by cybersecurity threats, data breaches, and fragmented health records. Blockchain technology is proposed as a transformative tool for enhancing privacy, security, and compliance through mechanisms like encryption, access control, and automated compliance checks. The chapter also discusses future trends, including the convergence of blockchain with artificial intelligence (AI) and the Internet of Things (IoT), offering a forward-looking perspective on how healthcare can leverage these innovations for improved data protection and regulatory compliance.

[*] **Corresponding author Sonal Rattan:** Department of UCRD and Apex Institute of Technology, Chandigarh University, Mohali, Punjab, India; E-mail: sonal.e15123@cumail.in

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

Keywords: Artificial intelligence, Blockchain technology, Compliance automation, Cybersecurity, Data security, Encryption, GDPR, Healthcare, HIPAA, HITECH Act, Internet of Things, Patient data, Privacy, Regulatory compliance.

INTRODUCTION

The intersection of privacy and regulatory compliance in the health sector seeks to protect patient data and uphold trust in healthcare systems. Given that this industry is becoming digital, the integrity of data and its security become matters of greatest concern. Privacy ensures that patients' information is safeguarded from unauthorized access or breaches, and compliance refers to various legislations and regulations set out to ensure this protection. Data integrity is a guarantee of the accuracy, completeness, and reliability of records, all of which are essential in effectual diagnosis and treatment. This technology also offers a decentralized, immutable ledger that enhances data security and transparency at the very core level of blockchain. Thus, blockchain aids healthcare providers in ensuring the security of their patients' data and that it is maintained accurately and only accessed by those who have proper authorization, adhering to strict privacy and regulatory requirements. This chapter reviews critical aspects of privacy and regulatory compliance in healthcare and explores how blockchain technology can be a transformative tool in their accomplishment.

Structure

The following topics are covered in this chapter:

- Regulatory Landscape in Healthcare.
- Challenges in Ensuring Privacy and Compliance.
- Blockchain Technology: An Overview.
- Leveraging Blockchain for Privacy and Compliance.
- Implementing Blockchain in Healthcare Systems.
- Comparative Analysis.
- Future Trends and Opportunities.

Objectives

The chapter “Privacy and Regulatory Compliance” deals in detail with how privacy should be protected and regulatory requirements implemented in healthcare. This chapter aims to give a realistic overview of the current regulatory environment, showing essential regulations like HIPAA, GDPR, and the HITECH Act and their bearing on healthcare providers. It seeks to locate challenges in ensuring the integrity and security of data amidst rising cyber threats and data

breaches. To that end, the chapter will further explore ways in which blockchain technology may improve privacy and compliance. This is through strong mechanisms for data encryption, access control, and automated compliance checks. The chapter is aimed at providing real-world case studies and best practices to equip healthcare professionals with practical insights and strategies to achieve the effective implementation of blockchain for protecting patient data and delivering regulatory compliance.

Regulatory Landscape in Healthcare

This section gives an overview of the key regulations and standards that set a minimum threshold for data privacy and security in healthcare, including the precise compliance requirements that organizations must put in place. Regulatory compliance is important in the health sector since this protects patients' information and the general trustworthiness of health providers.

Key Regulations and Standards

HIPAA (Health Insurance Portability and Accountability Act)

The Health Insurance Portability and Accountability Act was enacted in 1996 to protect the health information of patients. HIPAA contains several key provisions:

- **Privacy Rule:** This is part of the HIPAA legislation that creates national standards to protect individuals' medical records and other personal health information. It applies to healthcare providers, health plans, and healthcare clearinghouses [1]. It demands that appropriate safeguards on protecting the privacy of PHI be in place, limits on its use, and disclosure without patient authorization. Patients retain the right to receive a copy of their medical records and request corrections.
- **Security Rule:** This rule sets certain standards to maintain the security of electronic PHI (ePHI) that must be assured of confidentiality, integrity, and security. This requires the covered entities to develop and implement administrative, physical, and technical safeguards under the Security Rule. Administrative safeguards are policies and procedures that manage the selection and development, as well as the implementation and maintenance of security measures. Whereas physical safeguards are concerned with controlling physical access to protect ePHI, technical safeguards concern the technology and policies for protecting ePHI and controlling access to such information [2].
- **Breach Notification Rule:** This requires a covered entity to notify affected individuals, the Secretary of Health and Human Services (HHS), and, at times, the media when there is a breach of unsecured PHI. A business associate must also notify the covered entity in case of a breach [3, 4].

CHAPTER 11

The Transformative Role of Blockchain in Healthcare Privacy and Compliance

Mohit Angurala[1], Sandeep Singh[2], Navneet Kumar Rajpoot[3] and **Sonal Rattan[4,*]**

[1] *Department of Computer Science, Guru Nanak Dev University College, Pathankot, Punjab, India*

[2] *Department of Computer Science Engineering, SGT University, Gurugram, Haryana, India*

[3] *Department of Computer Science & Engineering, Graphic Era (Deemed to be University), Dehradun, India*

[4] *Department of UCRD and Apex Institute of Technology, Chandigarh University, Mohali, Punjab, India*

Abstract: Blockchain technology transforms the complicated process of verifying credentials and licensing among professionals in healthcare into an easy one, further ensuring adherence to all prerequisites of the qualification protocol and regulatory standards. Because of decentralized and immutable nature, blockchain technology holds huge potential for disrupting healthcare systems globally. It is a beacon of what blockchain can realize in creating a secure and transparent environment in the management of highly sensitive health data by using its decentralized ledger and cryptographic capabilities. This chapter explores the vital role of privacy and regulatory compliance in the healthcare sector, focusing on the protection of sensitive patient data in an increasingly digital world. As healthcare providers adopt technologies like blockchain, safeguarding data from unauthorized access and ensuring regulatory adherence become paramount. Key regulations such as HIPAA, GDPR, and the HITECH Act are examined alongside challenges posed by cybersecurity threats, data breaches, and fragmented health records. Blockchain technology is proposed as a transformative tool for enhancing privacy, security, and compliance through mechanisms like encryption, access control, and automated compliance checks. The chapter also discusses future trends, including the convergence of blockchain with artificial intelligence (AI) and the Internet of Things (IoT), offering a forward-looking perspective on how healthcare can leverage these innovations for improved data protection and regulatory compliance.

[*] **Corresponding author Sonal Rattan:** Department of UCRD and Apex Institute of Technology, Chandigarh University, Mohali, Punjab, India; E-mail: sonal.e15123@cumail.in

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

Keywords: Artificial intelligence, Blockchain technology, Compliance automation, Cybersecurity, Data security, Encryption, GDPR, Healthcare, HIPAA, HITECH Act, Internet of Things, Patient data, Privacy, Regulatory compliance.

INTRODUCTION

Blockchain offers some very innovative solutions to the integrity and security of the data within a sphere like healthcare through its tamper-proof and transparent ledger system. Its ability to record and track decentralized transactions securely not only enhances data integrity but also streamlines processes related to EHR, management of drug supply chains, clinical trials, patient data security, and processing of health insurance claims. This chapter reviews case studies representing the implementation of blockchain in these critical areas and their objectives, technology stacks, outcomes realized, and challenges overcome. By considering these real-life applications, blockchain's potential to disrupt healthcare delivery and improve patient outcomes comes to the fore, benchmarking new standards about integrity and privacy in health services.

Structure

The topics covered in this chapter are:

- Electronic Health Records (EHR).
- Drug Supply Chain Integrity.
- Clinical Trials Management.
- Patient Data Security and Privacy.
- Health Insurance Claims Processing.
- Comparative Analysis of Case Studies.
- Future Trends and Innovations.

Objectives

The chapter looks at several practical applications of blockchain technology in healthcare with regard to the solution of problems associated with data integrity and security. Case studies across sectors—electronic health record management, drug supply chain management, clinical trials, patient data security, and health insurance claim processing—are examined to ascertain whether they can help shed some light on how effective blockchain really is at bringing improved levels of transparency, efficiency, and trust into health systems. Case studies will underline the exact objectives pursued, the technological frameworks employed, and the outcome of the same by sending out varied signals related to successes and challenges in their implementation. What this chapter tries to do is provide

examples of how blockchain can revolutionize healthcare services in terms of both integrity and privacy of sensitive healthcare data while smoothening processes for better patient care and operational efficiency.

ELECTRONIC HEALTH RECORDS (EHR)

EHR stands for Electronic Health Records as it has become imperative to maintain records electronically. Electronic Health Record systems are very vital in current healthcare through digitization and management of health information concerning patients. They promise to improve the coordination of patient care, enhance clinical decision-making, and streamline all administrative duties. Traditional EHR systems, however, face several challenges that bring about problems in their effectiveness and pose a risk to data security and integrity.

Challenges of EHR Management

Managing electronic health records means going through complex challenges, such as:

Data Security: Ensuring the confidentiality, integrity, and availability of patient information in the wake of growing cybersecurity threats and data breaches.

Interoperability: Facilitating hassle-free data exchange between heterogeneous systems and providers, helping providers offer better coordination of care to the patient.

Privacy Concerns: Safeguarding patients' privacy while ensuring adherence to the provisions laid down by the United States in the Health Insurance Portability and Accountability Act and the European Union's General Data Protection Regulation.

Data Fragmentation: Dealing with health information fragmented across a bunch of systems brings inefficiency and creates gaps in the availability of information to patients.

Role of Blockchain in EHR Security and Integrity

Blockchain technology provides a game-changing solution to such challenges by managing EHRs in a decentralized, transparent, and immutable way. Some of the key benefits include:

Immutability: Blockchain records are immutable, which means that once data has been recorded, it cannot be changed retroactively. This characteristic provides integrity to the EHRs in such a way that unauthorized modification is disallowed and maintains a transparent audit trail of changes [1].

CHAPTER 12

Leveraging Blockchain Smart Contracts for Enhanced Data Integrity and Compliance in Healthcare

Sharon Christa[1,*], Raminder Kaur Khattri[2], Kamlesh Gautam[3] and **Rajbir Kaur[4]**

[1] *Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune, Maharashtra, India*

[2] *Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[3] *Department of Advance Computing, Poornima College of Engineering, Jaipur, India*

[4] *Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India*

Abstract: As information technology underpins advances in life and healthcare sciences, there is a growing intersection of healthcare and information engineering that is opening new possibilities for remote health monitoring and the secure exchange of health information between patients and clinicians. To gain the trust of the citizens, healthcare technologies need to ensure that the information they store and process is confidential, has not been tampered with, and, in the case of large-scale processing, is conducted according to probabilistic compliance policies. Currently, the onus on data protection practices of healthcare technology providers is drawn from legislation. This paper outlines data integrity and compliance policies and shows how these can be encoded in a blockchain-based system. The study enhances this blockchain-based system to use the Ethereum blockchain for executing smart contracts, which can execute probabilistic compliance rewarding health-related workflows. These smart contracts increase transparency and data integrity by not only laying out a set of promises for citizens and public health physicians to monitor the state of a blockchain protocol to ensure there are no attempted violations, thus increasing the service's trustworthiness. While the security of the blockchain is used to ensure data privacy and security, all blockchain-located proxy healthcare data can only be accessed through patients appointing a blockchain address and the associated articulated smart contract at their own discretion, making the proposed solution particularly patient-centric.

Keywords: Blockchain, Data privacy, Data integrity, Healthcare technology, Remote health monitoring, Secure health information exchange.

[*] **Corresponding author Sharon Christa:** Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune, Maharashtra, India;
E-mail: sharonchrista@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

INTRODUCTION

In a healthcare setting, managing extensive patient data, including sensitive details of medical history, treatment information, and personal identification details, securely and effectively is a core need for effective services and informed decisions [1]. At the same time, ensuring that the data collection and access processes are compliant with evolving data protection and privacy regulations is equally vital for ensuring the legal and ethical operation of healthcare organizations. Distributed ledger technology such as blockchain promises several capabilities, including the ability to provide an immutable audit trail of changes made to healthcare data and enable tracking, monitoring, and control of data access and data provenance and usage in line with applicable regulations. Additionally, as blockchain capabilities increasingly include the usage of smart contracts, which can enable new forms of extended data control, and the development of user-centric techniques for implementing compliance in a more decentralized manner, blockchain can increasingly offer new insights and solutions for ensuring effective and scalable healthcare data compliance [2]. This work examines the existing and potential role that blockchain and smart contracts may play in enabling and retaining healthcare data quality and compliance. We also argue that blockchain-based solutions require a degree of caution and user-centric design to ensure this role can provide the promised advantages. Themes taking the perspectives of healthcare compliance design, trust models, and regulatory requirements are discussed. Specifically, in the rest of the sections of this chapter, we start by providing an overview of the key challenges in ensuring the quality and compliance of healthcare data. We then describe the key blockchain and smart contract technologies and examine the role that they may currently have and the possible future roles to play a part in addressing the challenges of healthcare data quality and compliance enforcement.

Background and Significance of Data Integrity and Compliance in Healthcare

As healthcare becomes increasingly dependent on information technology, data is stored in various formats, including transcribed text files, relational databases, and machine-generated encrypted codes [3]. To achieve an interconnected healthcare ecosystem that spans care providers, medical devices, pharma companies, and insurance providers, integrated technology platforms provide the required infrastructure for multinational, multi-institutional patient data-sharing scenarios. Meeting the data integrity and compliance requirements such as data protection and security, privacy, and auditability in various national and international healthcare-related regulatory frameworks such as the Health Insurance Portability

and Accountability Act (HIPAA) in the US and the General Data Protection Regulation (GDPR) in the EU has become a significant challenge [4]. Blockchain smart contracts are essentially computer programs that govern the operation of a blockchain by facilitating, verifying, enforcing, and executing credible transactions without intermediaries [5]. With these automated contracts, it is possible to address relevant health data sharing and compliance concepts, such as the ability to strictly adhere to the patient data use agreements and care continuum. This section of the paper provides the conceptual background and significance of ensuring data integrity and compliance in healthcare, especially in a national and international healthcare-related compliance framework. With the advent of and trek toward data-driven, data-powered, value-based healthcare, value-added features and services are embedded in operational healthcare processes [6]. Along with the benefits that these value-added features and services offer come challenges in how to ensure that the data generated or used is integral and compliant from individuals' perspectives (*i.e.*, patients) and from that of regulators, data consumers, industry stakeholders, and payers (referred to as data consumers collectively). In a marketplace value chain that includes medical device companies, pharmaceutical companies, care providers, and insurance providers, such healthcare data should be considered integral and inherently trusted throughout their lifecycle [7]. The technological expansion of this marketplace value chain into a country, multinational legal jurisdiction, and international trade environment requires improved or new digital data transfer models for seamless data sharing in a trusted data usage ecosystem.

Fig. (**1**) is the flowchart that details the process of data access and retrieval using blockchain technology. It begins with data collection, followed by data encryption and storage on the blockchain. Data access requests are validated through smart contracts and an access control check. Once access is approved, data retrieval takes place, ensuring a secure and compliant process from start to finish.

FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

Hyped as one of the most disruptive technologies, the blockchain is, in fact, three separate components. The first component is the “chain of blocks,” linked together through the hash value (or a function), beginning with a unique block (defined as the Genesis block), with each block referencing its predecessor [8]. The second component is the actual data structure, designed to store specific information – for traditional ledgers, this data is a record of financial transactions, but in practice, it can store any data. Blocks are needed for data chaining and consistency (each new block saves the changes and any new data), and the final hash value is used to connect the new block to the previous ones. The third component, preventing “double-win” issues and, most importantly, making the

CHAPTER 13

Facilitating Patient Consent and Data Sharing with Blockchain Smart Contracts

Kiran Deep Singh[1], Prabh Deep Singh[2,*], Ankita Gupta[3] and **Rohan Verma[2]**

[1] *Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Rajpura, Punjab, India*

[2] *Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[3] *Department of Computer Science and Engineering, C.T. Institute of Engineering, Management and Technology, Lambri, Punjab, India*

Abstract: The healthcare sector has vast untapped potential in data management in biotech, pharmaceutical companies, research centers, and other clinical institutions. Health research that involves access and analysis of individuals' health information can lead to a much-improved understanding, prevention, and treatment of health conditions. Blockchain's potential has been identified in various applications, including managing personal health data. There are extensive data sets that can advance patient care protocols and deepen the understanding of patient pathology, fostering the development of new treatments. However, there has always been a privacy concern, and the financial value of these datasets deters stakeholders from sharing their data. The regulatory body has provided protection in promoting patent rights and data sharing through initiatives like common health research data spaces and fair data principles. Trust in the healthcare industry is paramount, where the protection of patient information is critical. While patients can withdraw consent for data use in research, blockchain technology offers a solution for managing patient consent and facilitating the securing of the data. This research implements a smart contract system for patient consent management and data sharing amongst state holders, which includes patients, researchers, data controllers, and supercomputer owners. Unlike traditional healthcare data management models, this mechanism shifts power from data controllers to a consortium of stakeholders. This chapter proposes a permission blockchain and smart contract mechanism that can enhance data sharing and consent management in healthcare, offering a more flexible and secure approach to handling sensitive health data.

Keywords: Consent management, Data governance, Electronic health records (EHR), Healthcare industry, Permissioned blockchain.

[*] **Corresponding author Prabh Deep Singh:** Graphic Era Deemed to be University, Dehradun, Uttarakhand, India; E-mail: ssingh.prabhdeep@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

INTRODUCTION

Distributed Ledger Technologies (DLTs) in the healthcare domain concerns the use of smart contracts to manage consent and associated settings that regulate the sharing of electronic health records across industry and geographical boundaries. Several DLT implementations attempt to take control of Personal Health Records (PHRs) and consent a step further by leveraging permissioned and semi-permissioned ledgers in conjunction with identity mechanisms. Moreover, advanced signature schemes can rely on DLT protocols and tools to enable differential privacy in record sharing. Today, however, breaking silos and embracing interoperable solutions are paramount to reaching the meaningful and widespread success of DLT use in the healthcare domain, and little to nothing has been briefly discussed or addressed about the smart contract logic that would be needed to rely on a public, un-permissioned ledger infrastructure for such goals [1].

This chapter will argue that thanks to such logic, it is indeed possible to embrace public, un-permissioned ledgers in the healthcare domain to cater to data sharing (and hence consent management) needs without relinquishing the trust assumptions that firms have agreed upon and embraced when deciding to use distributed ledgers in the first place. Blockchain technologies permit the creation of smart contracts and computer protocols used to facilitate, verify, or enforce a contract's performance or negotiation. This allows automatic consent by the contracting parties, immutability of the agreement, and semi-automated contract execution [2]. This chapter explores the feasibility of using blockchain smart contracts for patient consent and data sharing across systems. It describes the design of several smart contracts covering a wide variety of patient consent types. Support for consent delegation, bilateral agreements, informational self-determination, and safeguards to prevent erosion of patient consent are described.

Background and Rationale

Prior research related to blockchain has attempted a decentralized blockchain solution to eliminate an intermediary who brokers patient consent and mitigates the possible risk of data breach [3]. Implementing a blockchain zero-knowledge proof to validate the authenticity of the patient consent and preserve patient privacy, more security and privacy compliance on the blockchain can be enhanced. However, no existing research further assesses the integrity of the patient consent in the blockchain once it is formed and verified.

Research Objectives

Blockchain-related research offers strengths and includes a stream customized to healthcare, identifying emerging principal drivers of patient (age, gender, education) and health data trust (financial status, requiring interoperability, perception concerning use cases and industries). Further, a particular blockchain tool (smart contracts) in the form of database triggers and stored procedures the innovations offer is critically evaluated. Fifty one experts' insights are operationalized and used to understand why currently smart contracts see limited practice and to suggest a possible way to overcome these barriers. Moreover, it is argued that tools can deliver direct advantages for patients by enabling a more transparent and comprehensive assessment of the informed consent and data-sharing process. In doing so, a five-level maturity model is used to point out the likely factors that will affect the progression from non-disclosure to total transparency levels of Smart Contract Governance over health data [4].

The objective of the chapter is to demonstrate how the smart contract minimizes human error in facilitating patient consent records while increasing trust and transparency among all stakeholders using a private blockchain. The numerical example depicts the intensity of the interaction among each stakeholder and finally presents the exchange done by all stakeholders. The research questions about how electronic patient consent can be promoted and validated in blockchain have been partially answered in a recent study. With a focus not only on breaking the information silos and enabling patients to share more data with different stakeholders for various purposes but also supporting the full operation of a collaboration agreement, as well as informing or enforcing healthcare policies, this chapter goes beyond e-patient consent and is an extension to the work by implementing blockchain smart contract.

This research aims to examine the practical use of blockchain technology, in particular the developer tools where self-enforced procedures are stated, outlined, and translated in a language easily understood by both healthcare professionals and patients, *i.e.*, smart contracts. No insight is linked to encrypted data on the blockchain or requires regulatory support as a patient is still struggling with personal data protection.

BLOCKCHAIN TECHNOLOGY IN HEALTHCARE

Blockchain technology supports the NHIN Detailed Participant Directory (which is a part of the NwHIN Directory), for it supports the secure and private exchange of electronic health information. It is used for the authentication of the providers for the purpose of public health reporting using the NwHIN Direct, as there is a report that states that data integrity and signature are needed, apart from the secure

CHAPTER 14

Startup Innovations: Blockchain Solutions for Integrity and Transparency in Pharmaceutical Supply Chains

Riya Sharma[1,*], Kiran Deep Singh[2], Prabh Deep Singh[3] and **Ambika Prakash Mani[1]**

[1] *Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[2] *Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Rajpura, Punjab, India*

[3] *Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

Abstract: The pharmaceutical supply chain plays a critical role in infrastructure that ensures the delivery of safe and effective drugs to consumers. However, the prevalence of counterfeit drugs poses a significant risk to public health, intellectual property, and industry development. Blockchain technology, with its decentralized and immutable ledger, offers a robust solution to these challenges. This chapter is an attempt to explore the role of blockchain technology in ensuring the integrity and transparency of the pharmaceutical supply chain. The study presents a comprehensive overview of research studies and patents on the use of blockchain technology in diverse industries. Essentially, a blockchain is a string of transactional blocks linked by a hashing algorithm to the previous block. This chapter proposes blockchain-based processes designed to ensure the integrity and transparency of the supply chain in the pharmaceutical industry. With a detailed case study and examples, this chapter illustrates how startups and pioneering blockchain-based solutions create a secure, transparent supply chain. Additionally, this chapter also examines the integration of smart contracts in transactions, emphasizing their role in automating compliance and streamlining processes. The study discusses regulatory compliance in deploying blockchain solutions. Analyzing the potential of blockchain to enhance the supply chain's integrity and transparency, this chapter offers valuable insights for entrepreneurs, industry professionals, and policymakers. The study demonstrates how blockchain technology can be leveraged to combat counterfeit drugs and ensure a more sustainable and resilient pharmaceutical industry.

Keywords: Automation, Blockchain solutions, Drug safety, Intellectual property protection, Industry development, Public health.

[*] **Corresponding author Riya Sharma:**Department of Commerce, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India; E-mail: riyasharma6568@gmail.com

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

INTRODUCTION TO THE PHARMACEUTICAL SUPPLY CHAIN

The role of the pharmaceutical industry has evolved in developing chemical and biological compounds capable of curing diseases and health problems. While the development stage of a drug is particularly complex and involves numerous elements, the elements usually highlighted are of a scientific nature [1]. However, the development of new drugs and medications is not only based on chemical and pharmaceutical elements but also involves economic and business considerations that are key during the production, distribution, and sales stages. It is in these stages that the collaboration and cooperation of all actors involved are key to ensuring the correct functioning of the pharmaceutical supply chain. The pharmaceutical industry involves the production and selling of pharmaceutical products and services. Thus, the industry is complex and needs a comprehensive approach to incorporate all players in the supply chain [2]. There are different key stakeholders associated with the production and selling of pharmaceutical products that interact with each other to ensure that patients receive medicines at the right time. One of these is the manufacturers who undertake research and development, manufacture pharmaceuticals, and finally extract the pharmaceutical products. They ensure that pharmaceutical products are made available to the retailers or the wholesalers. The transportation companies are responsible for moving the products from one player to the other [3]. The task needs to be completed in a timely manner so that the drug order arrives in good condition. Although each of these players is significant, this study focuses on wholesalers in the pharmaceutical supply chain, and more specifically counterfeit drugs, to find out how blockchain technology can be used to ensure integrity and transparency in the pharmaceutical supply chain. In the evolutionary landscape of the pharmaceutical industry, where product integrity and patient safety are paramount, startups are pioneering innovative solutions that are powered by blockchain technology. Blockchain's immutable leisure system helps startups to reshape the traditional supply chain paradigm, which ensures transparency and traceability of the pharmaceutical journey at every stage [4]. From research and development to distribution and consuming engagement, blockchain offers a robust structure for verifying product origins, validating the manufacturing process, and safeguarding against counterfeit products. With groundbreaking initiatives, startups are not only revolutionizing the supply chain but also building trust and confidence among consumers, ultimately leading to the advancement of the industry toward a more secure and sustainable future. An illustration of how different stakeholders in the pharmaceutical supply chain interact with the blockchain network is presented in Fig. (**1**). The system includes a user interface and involves manufacturers, distributors, retailers, pharmacies, and patients. The blockchain network integrates a smart contract layer and a data storage layer, which further utilizes an encryption module and an access control module to

ensure secure and transparent transactions. Firstly, this chapter defines the pharmaceutical supply chain in order to refer to the main problems and risks in this area. The study also addresses the legislative and regulatory measures that have been implemented to control and regulate the activities of companies in this sector. Finally, we will also explore the solutions, especially blockchain technology, that can be implemented in the supply chain, allowing greater visibility and integrity, eliminating intermediaries, and increasing cooperation between the different actors involved. The chapter ends with a brief reflection on public policies that can be established in this area and identifies future opportunities for analysis and research in this area.

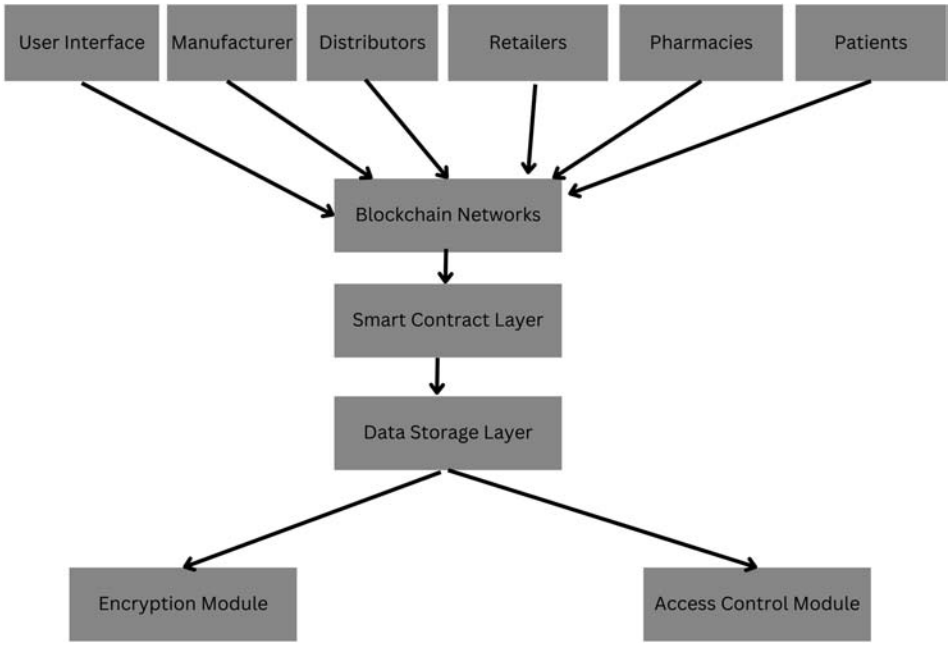

Fig. (1). Blockchain-based pharmaceutical supply chain architecture.

Challenges in the Current Pharmaceutical Supply Chain

In the case of detection of counterfeit drugs available for consumers, the company appears in the press and headlines negatively. This is because the population fears that the product that they have bought is fake and does not meet the necessary standards and sanitary standards, which increases the possibility of harming health, making complaints, and demanding compensation [5]. For this reason, the use of blockchain technology appears as a technology that provides several solutions to minimize these threats and risks, thus creating a transparent, efficient, and reliable link, making it possible to distribute high-quality medicines to patients with more agility and efficiency in their care [6]. The supply chain used

CHAPTER 15

The Future of Blockchain in Healthcare: Trends, Opportunities, and Challenges

Mohit Angurala[1], Rajeev Kumar Bedi[2,*], Gurpreet Singh Panesar[3] and **Navneet Kumar Rajpoot[4]**

[1] *Department of Computer Science, Guru Nanak Dev University College, Pathankot, Punjab, India*

[2] *Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Jalandhar, Punjab, India*

[3] *Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, India*

[4] *Department of Computer Science & Engineering, Graphic Era (Deemed to be University), Dehradun, India*

Abstract: Blockchain technology is revolutionizing the healthcare industry by enhancing data integrity, security, and interoperability. Healthcare data are principally fragmented by different systems and formats, making smooth data sharing difficult. Blockchain has the ability to standardize data exchange in health by putting up any similar protocol of data storage and sharing. These standardizations guarantee the consistency of data and its accurate, easy accessiblity and availablity across different healthcare providers and systems. For any implementation of blockchain solutions, the regulatory, technical, ethical, and social considerations must be taken into account. From safe management of patient data and transparent supply chains of pharmaceuticals to frictionless claim processing, the current applications of blockchain can only demonstrate the potential for solving some of the perennial problems of the healthcare sector. This chapter delves into the future trends and opportunities of blockchain in healthcare, focusing on areas like decentralized clinical trials, patient data control, and supply chain transparency. The adoption of blockchain can transform patient care, streamline clinical trials, and improve pharmaceutical supply chains by reducing fraud and ensuring data authenticity. In addition to providing insights into emerging technologies like quantum-resistant cryptography and blockchain-AI integration, the chapter explores regulatory challenges, technical considerations, and the ethical implications of deploying blockchain in healthcare. By examining case studies and identifying key success factors, this chapter offers a roadmap for healthcare professionals, researchers, and policymakers to leverage blockchain for a more secure, efficient, and patient-centered healthcare ecosystem.

[*] **Corresponding author Rajeev Kumar Bedi:** Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Jalandhar, India; E-mail: drrajeevbedi@ptu.ac.in

Mohit Angurala, Preet Kamal, Aryan Chaudhary, Rasmeet Singh Bali & Vijay Bhardwaj (Eds.)

Keywords: Blockchain, Data integrity, Decentralized clinical trials, Healthcare, Patient data security, Smart contracts.

INTRODUCTION

Blockchain technology is already creating a revolution in the healthcare space by enhancing the level of data integrity, security, and interoperability. The real power of blockchain is in the future applications. It becomes even more important to explore the emerging trends and opportunities that blockchain opens as we stand on the threshold of its mass adoption. The better prepared and adept stakeholders are carving out the future with this technology, the more they can understand potential improvements from these emerging trends. This chapter will investigate the upcoming promising trends of blockchain in healthcare and the opportunities lying in the patient, provider, researcher, and insurer domains.

Structure

The topics covered in this chapter are:

- Emerging Trends in Blockchain for Healthcare.
- Opportunities for Healthcare Stakeholders.
- Challenges and Considerations.
- Case Studies and Pilot Projects.
- The Future Outlook.

Objectives

This chapter, “Future Trends and Opportunities,” presents a discussion on the future potential developments and disruptive effects of blockchain technology in healthcare. The chapter attempts to go in depth into the analysis of blockchain's emerging trends, such as decentralized clinical trials, advanced interoperability, and security features, together with its integration using AI and patient-centered care solutions. The chapter will identify trends to underline the opportunities that exist for the different stakeholders—patients, healthcare providers, researchers, and payers—while drawing attention to the challenges and considerations from a regulatory, technical, and ethical point of view. It will attempt to provide readers with insights into how blockchain can change healthcare by proposing case studies or future outlooks on how this technology can revolutionize healthcare by improving data integrity and, hence, spur innovation in this industry.

Emerging Trends in Blockchain for Healthcare

Blockchain technology is most likely to make a significant difference in healthcare regarding data integrity, security, and interoperability. We shall now discuss some of the emerging trends that have the potential to transform this sector and also provide insight into each domain in detail.

Decentralized Clinical Trials

Decentralized clinical trials leverage the power of blockchain to redesign a traditional model of clinical trials by making the process more efficient, ensuring better data integrity, and guaranteeing more engagement amongst patients.

Improved Data Integrity

In typical clinical trials, the available data is subject to loss of integrity, particularly due to errors, manipulation, and reporting when conducted manually at the conversational-data-entry level, among other issues; the blockchain provides an immutable ledger with which entries are timestamped and cryptographically sealed. Each exchange is also authenticated by the participants of the network, thus ensuring the integrity and irrefutability of data. This transparency not only serves to improve the validity of clinical trial data but also eases regulatory compliance with a view to the full and tamper-proof history of all entered data [1]. Decentralization guarantees that data cannot be manipulated by a single entity, making the clinical trial process more trusted and accountable.

Patients can dole out and lease their health data if there is a need for it, with privacy ensured by data protection legislation [2]. Smart contracts further automate the process of taking and maintaining permission from the patients. Trust and participation can be encouraged by the increased transparency and control of data, leading to more robust and representative patient populations within clinical trials. Researchers will be able to capitalize on patient engagement potential even more by utilizing token-based incentives to drive and sustain long-term patient interest during the clinical trial process.

Interoperability and Data Sharing

Data sharing and interoperability have been the backbones of improved healthcare and collaborative research. Blockchain technology can equally play a very important role by providing a standardized exchange of data in a secure platform.

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

P

Q

R

S

T

V

Mohit Angurala

Dr. Mohit Angurala serves as an Assistant Professor at GNDU College, Pathankot. He previously held academic roles at Chandigarh University, VIT Chennai, Khalsa College of Engineering and Technology, and Chitkara University. He earned his Ph.D. in Computer Science from I.K. Gujral PTU in 2021 and holds M.Tech, MBA, and B.Tech degrees. His research focuses on energy management in wireless sensor networks, IoT, network security, and optics. He has 44 international publications, several book chapters, and 9 patents (4 granted). Dr. Angurala is also on editorial boards and reviews for reputed international journals indexed by Scopus and Web of Science.

Preet Kamal

Dr. Preet Kamal is an Assistant Professor at Chandigarh University. She earned her Ph.D. in CSE from Chitkara University, M.Sc. IT from Panjab University, and BCA from Punjabi University. With 17 years of academic experience, her expertise includes data mining, machine learning, cybersecurity, and AI. She has authored numerous papers in reputed journals and conferences and is known for her dedication and innovative teaching approach.

Aryan Chaudhary

Aryan Chaudhary is the Chief Scientific Advisor at BioTech Sphere Research and former Research Head at Nijji HealthCare Pvt Ltd. His work focuses on integrating AI, IoT, and blockchain in healthcare. He has authored numerous papers and is a keynote speaker, editor of CRC book series, and guest editor for prestigious journals. Aryan has received several honors, including "Most Inspiring Young Leader in Healthtech 2022." He is a senior member of international science associations and serves on editorial boards of reputed biomedical journals.

Rasmeet Singh Bali

Dr. Rasmeet Singh Bali is Additional Director at the Apex Institute of Technology, Chandigarh University. He received his Ph.D. from Thapar Institute of Engineering and Technology and M.E. from NITTTR, Chandigarh. His research spans vehicular communication, data dissemination, blockchain, hybrid computing, IoT, and intelligent transportation systems. He is passionate about developing algorithms that simplify complex processes across diverse domains.

Vijay Bhardwaj

Dr. Vijay Bhardwaj is an Associate Professor at Chandigarh University with a Ph.D. and M.Tech in CSE. He has over 19 years of academic, research, training, and industry experience. Previously, he served as Dean at Guru Kashi University and HOD at Manav Institute. He has published extensively and supervised M.Tech and Ph.D. students. His research interests include machine learning, data science, pattern recognition, and AI. He has also worked in the IT industry with companies like Siebel and IFW Infotech.