Chapter 12
Application of Blockchain in E-Healthcare Systems

Aman Ahmad Ansari
The LNM Institute of Information Technology, India

Bharavi Mishra
The LNM Institute of Information Technology, India

Poonam Gera
The LNM Institute of Information Technology, India

ABSTRACT

The e-healthcare system maintains sensitive and private information about patients. In any e-healthcare system, exchanging health information is often required, making privacy and security a primary concern for e-healthcare systems. Another major issue is that existing e-healthcare systems use centralized servers. These centralized servers require high infrastructure and maintenance costs for day-to-day services. Along with that, server failure may affect the working of e-healthcare systems drastically and may create life-threatening situations for patients. Blockchain technology is a very useful way to provide decentralized, secure storage for healthcare information. A blockchain is a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. These blocks create a chain of immutable, tamper-proof blocks in a ledger. This chapter will discuss the different aspects of blockchain and its application in different fields of the e-healthcare system.

DOI: 10.4018/978-1-7998-8382-1.ch012

INTRODUCTION

Healthcare generates a large amount of health data regularly. Due to the sensitive nature of health data, storing and communicating such a vast amount of health data is critical and difficult (Griebel et al., 2015). In healthcare, safe, and secure health data sharing is vital for diagnosing and treating patients. Medical professionals should be able to communicate their patients' health data in a privacy-sensitive and timely fashion.

On the other hand, in e-healthcare, the patient data is transferred either by real-time monitoring or via store and forward technology (Bhatti et al., 2018; Houston et al., 1999). Patients can be diagnosed and treated remotely by experts using shared health data. Because of the sensitivity of health data, security and privacy are major challenges while sharing it. The capability to safely, securely, and scalably share health data helps in improving diagnostic accuracy and effective treatment (Berman & Fenaughty, 2005; Castaneda et al., 2015; Zhang et al., 2018).

Furthermore, various interoperability challenges are faced while sharing health data. The safe and secure communication of health data between healthcare providers or research institutes needs substantial, reliable, and healthy collaboration between them. Before sharing health data, involved entities need to be agreed upon a data-sharing agreement, nature of health data, sensitivity, procedures, ethical policies, and governing rules (Downing et al., 2017).

Recently, there has been unprecedented interest in using blockchains for store and share health data (Dubovitskaya et al., 2020; Hashim et al., 2021), real-time remote patient monitoring (Chelladurai et al., 2021; Ray et al., 2021), pharmaceutical supply chain (Bryatov & Borodinov, 2019; Jamil et al., 2019), health insurance claim (Loukil et al., 2021; Thenmozhi et al., 2021) and clinical research (Kim et al., 2021; Mamo et al., 2019).

BLOCKCHAIN

Blockchain is a growing list of records, known as blocks, and each block is linked to the previous block by including the hash of the previous block, with a timestamp and Markle tree. As each block contains information of the previous block, they form a chain (Figure 1). A server that installed a mining application and has sufficient computing resources to mine, called a full node, can generate a block. Developing a new block known as mining (Swanson, 2015). Complete blockchain will be loaded on the user's machine, which connects the blockchain with the full node to trace all transactions to the first block (Nakamoto, 2008). Presently, there exist four types of blockchain systems: public, private, hybrid, and consortium (Ray et al., 2021).