

# Chapter 11

## Blockchain for Healthcare and Medical Systems

**Sanaa Kaddoura**

*Zayed University, UAE*

**Rima Grati**

*Zayed University, UAE*

### **ABSTRACT**

*Blockchain is one of the trendy technologies in the current era. All industries are merging blockchain with their production line to benefit from its features such as security and decentralized data. One of the main problems in the healthcare system is the lack of interoperability (i.e., data should be patient-centered and not institution-centered). Healthcare information systems, in the current state, cannot communicate. Each organization works within its boundaries and owns its data. To make this shift, many challenges should be solved such as data privacy, standards, scalability, and others. Blockchain can solve these problems by giving the patients control over their data; therefore, they can share it with any institution for a time period. It is expected that blockchain will improve healthcare data management. In this chapter, the authors study the opportunity of blockchain to leverage biomedical and healthcare applications and research. Blockchain also contributes to the medication manufacturing area.*

### **INTRODUCTION**

Various countries are experiencing a rapid increase in the number of patients at hospitals and medical centers, making it hard to handle and manage through the existing infrastructure by available doctors and staff according to Tanwar et al. (2020). In fact, the recent technological breakthroughs bring up major updates and enhancements for healthcare centers to better capture the different challenges imposed with this increase. Healthcare systems are currently being directed with such vision in many aspects. It is expected that in 2030, healthcare systems will integrate different technologies to allow monitoring the health situation of each patient and allow accurate measurement of information that may help save the lives of patients and increase their well-being. Internet of Things (IoT) and wearable devices are key

DOI: 10.4018/978-1-7998-5839-3.ch011

enablers for this vision, leading to a higher quality of care for patients. Being tailored for individual's use, doctors are able to monitor each patient through his/her own IoT and wearable device, and thus treating more patients efficiently and accurately without the need to regularly visit clinics and hospitals, except in case of emergency. Patients are thus able to constantly update their doctors with their continuous changes to increase welfare and life-expectancy. This also reduces medical costs and helps in better utilization of resources in available healthcare.

This transformation towards a technological based healthcare system is expected to generate a massive amount of data that is created, stored, and accessed daily. However, this data is subject to multiple challenges imposed due to the nature of communication over the Internet. In fact, data security and privacy in healthcare systems are considered a top concern to be addressed when discussing healthcare data corresponding to patients. In 2018, over 13 million healthcare records were breached (Moro Visconti, 2020). Due to the sensitivity of healthcare data, healthcare data centers may be an attractive place to attackers who aim at financially benefiting from this information through selling it to a third-party provider. This raises the demand for a system that reserves healthcare data of the patients from any fraud. Saha et al. (2020) developed a new scheme that increases security and patients' data privacy against attackers. This approach showed efficiency in terms of computation cost with respect to other relevant approaches. Further, limitations on the patient's ownership of his/her medical data is a main concern as the patient is in need of a system that allows him/her to control access to this data.

Blockchain technology is one of the novel efforts that are being explored to solve this problem, which can offer an important solution that solves multiple challenges imposed by healthcare systems and hence provide better experience for users (De Aguiar et al., 2020). Blockchain can be defined as a decentralized and distributed digital ledger that allows recording transactions in a chain of immutable blocks linked together by cryptographic hashes. In a blockchain system, transactions are stored over multiple network participants whereby there is no need for a central authority to manage the transactions being done. The procedure starts by the user requesting a certain transaction which can be of any type of data including financial, health, or even a message. The user then provides a signature with his private key for this transaction, enabling other entities to verify the authenticity of this transaction using the public key of this user. The transaction is then sent to the entire network of peer-to-peer participants. Blockchain miners, a community of people responsible for ensuring the security of moving data over blocks in blockchain, select a batch of the available transactions to form a block. Each miner tries to find the correct hash output for the given batch of encoded transactions within this block. Whenever a blockchain miner is able to add a block of transaction to the blockchain, this block is considered complete, locking the ability to alter it. This necessitates recomputing the whole block and the blocks added after it. The complexity of this process protects the transactions from fraud and attacks as it involves high computational power to try different combinations of strings until the output string matches the stipulated requirements, hence, providing a highly secure aspect. Further, being a decentralized technology is also a key advantage, it hinders the action of malicious users through replicating data over multiple nodes and eventually malicious users should alter data across all nodes which are a hard task. For this reason, blockchain has been considered as a key solution to transform the current healthcare systems into a patient-centered systems through which the patient has his/her healthcare data records properly secured and shared everywhere at any time (Chen et al, 2019). A patient would then use mobile applications to record his/her data and send it to healthcare providers within seconds through the private blockchain network. This will enable patients to control and restrict the access over their data to only the concerned medical practitioners.

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/blockchain-for-healthcare-and-medical-systems/280854](http://www.igi-global.com/chapter/blockchain-for-healthcare-and-medical-systems/280854)

## Related Content

---

### The Value of Personal Information

K.Y Williams, Dana-Marie Thomas and LaToya N. Johnson (2017). *Identity Theft: Breakthroughs in Research and Practice* (pp. 308-326).

[www.irma-international.org/chapter/the-value-of-personal-information/167233](http://www.irma-international.org/chapter/the-value-of-personal-information/167233)

### Hasta La Vista Privacy, or How Technology Terminated Privacy

Konstantinos K. Stylianou (2011). *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices* (pp. 44-57).

[www.irma-international.org/chapter/hasta-vista-privacy-technology-terminated/50407](http://www.irma-international.org/chapter/hasta-vista-privacy-technology-terminated/50407)

### On the Design of an Authentication System Based on Keystroke Dynamics Using a Predefined Input Text

Dieter Bartmann, Idir Bakdi and Michael Achatz (2007). *International Journal of Information Security and Privacy* (pp. 1-12).

[www.irma-international.org/article/design-authentication-system-based-keystroke/2458](http://www.irma-international.org/article/design-authentication-system-based-keystroke/2458)

### Information Sharing for CIP: Between Policy, Theory, and Practice

Neil Robinson (2013). *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection* (pp. 324-351).

[www.irma-international.org/chapter/information-sharing-cip/73131](http://www.irma-international.org/chapter/information-sharing-cip/73131)

### Patching our Critical Infrastructure: Towards an Efficient Patch and Update Management for Industrial Control Systems

Konstantin Knorr (2013). *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection* (pp. 190-216).

[www.irma-international.org/chapter/patching-our-critical-infrastructure/73125](http://www.irma-international.org/chapter/patching-our-critical-infrastructure/73125)