Blockchain Technology for Healthcare

Rushil Balasubramanian, Edmond Prakash, Imtiaz Khan, and Jon Platts

Cardiff Metropolitan University

Computers have significantly improved healthcare over the past decades. Healthcare organizations have benefited from advanced computers that can upgrade and automate healthcare activities. These computers have transformed - from physical to virtual - the management, usage and monitoring of health data. Models of AI/Big Data have been successfully used to analyse health data for medical diagnoses, prognoses and treatments, clinical researches and pharmaceutical drug discoveries [1]. Public health policy-making is easier than ever before. Next generation computing systems are expected to be large-scale, distributed and heterogeneous – cloud computing and IOT. Modular, adaptive, scalable, automated and decentralized technologies would be required to enforce data ethics and transparency in these systems.

It is crucial to protect data and regulate data operations, especially with compliance requirements of data laws such as the Health Insurance Portability and Accountability Act (HIPAA, USA, 1996), California Consumer Privacy Act (CCPA, USA, 2018), Data Protection Act (DPA, UK, 2018), General Data Protection Regulation (GDPR, EU, 2018), etc. For example, the HIPAA establishes standards for the collection and rules for the sharing of health data among healthcare organizations.

It is paramount for healthcare organizations to respect their patients' privacies in order to avoid bad reputations and legal battles. Leading healthcare organizations possess large volumes of health data. Data laws and security challenges prevent these organizations from using their health data silos. Blockchain technology (BT) is receiving great attention from academia, industries and policy makers. It has been hailed as a disruptive and revolutionary technology which can provide robust infrastructures whose salient features are data privacy and security [2]. It can offer innovative, integrated, trustworthy and reliable solutions without third-party intermediaries - especially for healthcare [3].

However, a comprehensive framework is needed to develop world-wide BT standards. This framework should be assembled by researchers and policy makers and should define design principles and core features of BT solutions. Solutions based on the framework should satisfy generic and specific requirements of their application areas. The framework's ethical principles can vary from one BT solution to another. Its metrics should be able to evaluate whether a BT solution is data ethical or not. These metrics would depend on the solution's data transparency.

Data ethics and transparency are important debate topics in AI; data usage should be ethical and transparency should respect privacy [4]. Reconciliation of data transparency and privacy is an important general research problem in computing systems. Data laws determine the responsibilities and rights that organizations have over their clients' data [5]. With BT solutions for

healthcare [6]: (1) data objects can be monitored throughout a blockchain network which follows a dynamic consensus protocol, (2) the framework's ethical principles can be encoded and enforced by smart contracts in the network, (3) research groups can use patients' health data in exchanges for cryptotokens - defined by smart contracts - to develop personalized healthcare and (4) patients can exchange these cryptotokens within or outside the network for values. Therefore, BT can incentivize data management and enable its users to be custodians of their data.

Lesser resources are needed to implement permissioned blockchain networks that follow lighter consensus protocols than others. Although BT is emerging, it is an optimistic topic for R&D in many industries. BT-IoT solutions with cloud computing, smart contracts, cryptotokens and DApps would be successful for healthcare [7].

Prospects and challenges of BT solutions as services for healthcare were briefly discussed in this article. BT can provide robust infrastructures to efficiently manage the 3Vs of Big Data - volume, velocity and variety - and to maintain data lineage and provenance. We aspire to develop novel and optimized models for data processing using BT with a focus on healthcare. These models would enhance the control of data flow and quality. We would be collaborating with academic and industrial research groups for relevant case studies. Our work would contribute to the establishment of world-wide BT standards that can be used across industries for feasible, reliable and scalable IT solutions.

References

[1] Karim Abouelmehdi, Abderrahim Beni-Hssane, Hayat Khaloufi, and Mostafa Saadi. Big data security and privacy in healthcare: A review. *Procedia Computer Science*, 113:73–80, 2017.

[2] Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Comput. Surv.*, 52(3), July 2019.

[3] Erikson Júlio De Aguiar, Bruno S. Faiçal, Bhaskar Krishnamachari, and Jó Ueyama. A survey of blockchain-based strategies for healthcare. *ACM Comput. Surv.*, 53(2), March 2020.

[4] Elisa Bertino, Ahish Kundu, and Zehra Sura. Data transparency with blockchain and AI ethics. *J. Data and Information Quality*, 11(4), August 2019.

[5] Jan Philipp Albrecht. How the GDPR will change the world. *European Data Protection Law Review*, 2(3), 2016.

[6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, 2016.

[7] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung. Decentralized applications: The blockchain-empowered software system. *IEEE Access*, 6:53019–53033, 2018.

[8] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib. Introducing blockchains for healthcare. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pages 1–4, 2017.