Chapter 6
Quantum-Enhanced Blockchain Architecture in Healthcare

Mohammad Nasar
http://orcid.org/0000-0001-8196-380X
Mazoon College, Muscat, Oman

Mohammad Abu Kausar
http://orcid.org/0000-0002-7997-8292
University of Nizwa, Nizwa, Oman

Mohamed Abbas Abdul Alleem
http://orcid.org/0000-0002-8556-5953
University of Technology and Applied Sciences, Sur, Oman

ABSTRACT

Healthcare systems are increasingly data-driven through EHRs, telemedicine, and IoT-based medical devices. However, cyber threats, poor interoperability, and data tampering expose the vulnerabilities of centralized systems. Blockchain offers immutability and transparency, yet its traditional cryptography faces risks from quantum computing, which can compromise existing encryption. To address this, the chapter proposes a quantum-enhanced blockchain framework integrating post-quantum cryptography (PQC), quantum key distribution (QKD), and hybrid quantum-classical consensus. The model strengthens confidentiality, integrity, and availability (CIA) of healthcare data while ensuring interoperability and regulatory compliance. Key applications include secure EHR and genomic data management, automated patient consent handling, transparent drug supply chain monitoring,

DOI: 10.4018/979-8-3373-7189-4.ch006

and protection of clinical research. The chapter also discusses ethical, technical, and regulatory challenges, offering insights into building resilient, quantum-secure healthcare ecosystems.

INTRODUCTION

Across the world, healthcare systems are impacted by a deep digital transformation. "Digital Transformation" is revolutionizing every walk of life, and the health care has not been an outlier; EHRs, Internet-of-Medical-Things (IoMT) sensors including those in hand-held or wearable devices for remote monitoring, Telemedicine platforms incl., IVR systems AI-based diagnostics, are re-sculpting clinical workflow routines and patient management value chain (Kasyapa & Vanmathi 2024). And with this evolution also comes a strategic double-edged sword: because health information is created and shared more easily, healthcare networks are also becoming increasingly susceptible to cyber-attacks, data corruption and privacy breaches. Healthcare breaches represented nearly one-third of all reported global incidents of data-leak events as of 2023, confirming the failure of conventional centralized security architectures (Nguyen et al., 2021).

In silos of information, traditional databases store all records on different servers managed independently by each hospital or national agency. They rely on perimeter defenses (firewalls, access control systems and encoded keys) but these can be easily breached using methods like phishing, insider threats and online hostage taking. A major limitation is the absence of transparent audit trails. There is no way to check who has accessed or altered a patient's data once it leaves the hands of one organization. But as we move health care beyond single organizations and geographical locations trying to make sure that our data is always right there when we need it becomes a major challenge (Weintrop et al., 2020)

Blockchain technology was developed as a disruptive blue ocean approach that can provide solutions to many of the problems above. By spreading transaction records out across several nodes, blockchain eradicates single points of failure and creates a permanent record of activity. In healthcare, this means that each patient's information, prescription, insurance claim can be verifiable, and time stamped to increase the confidence of hospitals and laboratories and pharmaceutical companies or regulatory agencies (Kaushik & Kumar.,2023). The decentralized approach also allows for interoperability, which is something that hasn't been possible with traditional EHR systems, many of which were developed on differing standards like (Health Level Seven International) HL7 and (Fast Healthcare Interoperability Resources) FHIR.