Chapter 7
Quantum Proof Cryptography as the Security Backbone of the Metaverse

Semila Fernandes
http://orcid.org/0000-0002-6835-5356
Symbiosis Institute of Business Management, Symbiosis International (Deemed to be) University, Pune, India

Anshul Dhunna
http://orcid.org/0009-0005-3139-1109
Symbiosis Institute of Business Management, Symbiosis International (Deemed to be) University, Pune, India

ABSTRACT

The metaverse is emerging as a persistent, immersive digital environment that enables continuous social interaction, economic activity, collaboration, and identity development through constant data exchange. Unlike traditional digital platforms, it relies on sustained synchronisation and presence, generating extensive sensitive data such as identity attributes, behavioural patterns, biometric signals, spatial information, and transaction records across decentralised networks. This chapter examines the expanded cybersecurity risks arising from continuous data flows, highlighting how breaches can have long-term consequences due to persistent digital identities and ownership histories. As metaverse applications expand into healthcare, education, workplaces, and finance, security failures may lead to privacy loss, identity harm, and erosion of trust. The chapter outlines how cryptography supports secure com-

DOI: 10.4018/979-8-2600-2313-6.ch007

munication, authentication, and data integrity through encryption, hashing, digital signatures, and key management, while addressing long-term risks from future computational advances.

INTRODUCTION

A new dimension for our lives, the metaverse starts to take form as a permanent, immersive digital environment that supports continuous digital socialisation, economic activity, professional collaboration, and identity development in virtual spaces (Accenture, 2022). Unlike traditional digital platforms, which are limited to short periods of time with limited data exchange, metaverse environments depend on a constant exchange of data, allowing for sustained immersion, synchronisation, and presence (Uddin et al., 2023). The continuous exchange and generation of vast amounts of individual user interaction creates multiple streams of sensitive data, including user identity attributes, user behaviour patterns, biometric signals, spatial information, and transaction data; all of which must ultimately be processed through many different types of devices and between many different decentralised networks. This dependence on the exchange of continuous data transforms the cybersecurity requirements of immersive virtual environments (Dionisio et al., 2013).

Cybersecurity issues resulting from the pervasive and intensive usage of data in the metaverse are explored in this chapter, which analyses the scope of the attack surface created by continual movements of extremely sensitive information and the impact of security breaches in these environments (Sun et al., 2022). Data is generated and collected in a variety of different ways throughout an immersive environment, but when such information is lost or breached, it typically has a long lifetime and is difficult or impossible to erase or replace. The presence of extremely large amounts of persistent digital identity information (e.g., persistent digital identities), extensive behavioural history, and ownership records creates risks that go beyond those associated with traditional forms of online platforms. The implications of these risks can potentially be exacerbated as the metaverse continues to advance into areas such as healthcare simulations, remote workplaces, educational institutions, and financial institutions. Consequently, failures in the security mechanisms of the metaverse can result in the loss of privacy for users; significant damage to individuals' personal identities; and the erosion of trusted relationships with others (Lee et al., 2021).

In addition to being effective against the current threat landscape, the effectiveness of these methods of securing data in the metaverse will be tied to classical computational limitations and risk models from today through to the near and intermediate future (Statista, 2025; World Economic Forum, 2023). A critical issue covered in this chapter is how to safeguard long-term and highly sensitive data