Chapter 7
Enhancing Cybersecurity in Blockchain:
Legal Challenges and Solutions

Sudipta Dhar
https://orcid.org/0009-0004-4998-3041
Brainware University, India

Shivangi Kashyap
https://orcid.org/0009-0002-1685-330X
Brainware University, India

Pravin Kumar
https://orcid.org/0009-0008-9393-7324
Brainware University, India

ABSTRACT

Blockchain enables decentralization, transparency, and security and faces threats from cybersecurity and legal. The cryptographic algorithms and consensus protocols add a layer of security, while the associated risks of possible 51% attack, inappropriate private key management, and smart contract vulnerabilities still persist. Legal issues arise with the clashes with data protection laws like the GDPR and with the challenge of finding who is liable due to this decentralization. The uncertain legal context around smart contracts is preventing their enforcement. Also emerging threats like quantum computing will require quantum-resistant cryptographic standards. A proposed solution includes better security, adaptive regulations, and collaboration of governments, industry, and academia. An equilibrium will allow for a secure, legally complaint, and sustainable blockchain fit for applications into the future.

DOI: 10.4018/979-8-3373-2282-7.ch007

INTRODUCTION

In the past few years, blockchain technology showed itself in the scope of an innovative breakthrough that changed not only the finance and healthcare businesses but also industries from supply chain management to everyday routine. Blockchains are famous for their utility of decentralized and tamper-resistant architecture, which leads to security, transparency, and efficiency of the system. Nevertheless, as more organizations globally embrace blockchain, the number of attacks targeting them increases, and the global legal and security complexities grow.

The security of blockchain is often cited, but blockchain is no different from any other information technology when it comes to being vulnerable to cyberattacks. The vulnerabilities in smart contracts, 51% attacks, phishing, and malware have shown us that hackers are crafting new tricks to exploit weaknesses in blockchain networks. These threats are not only damaging to the integrity and reliability of blockchain systems but also ruin the public confidence in this new technology.

The technical, legal, and regulatory boundaries of blockchain cybersecurity are also compounding. Blockchain, however, introduces a new set of challenges for the legal framework, which is not designed to deal with cross-border cybercrimes and jurisdictional ambiguity as the enforcement of accountability. Beyond, the working pace of blockchain innovation usually surpasses that of the ability of legal frameworks to streamline, filling regulatory gaps that heighten cybersecurity perils.

This paper investigates cybersecurity challenges interceded by blockchain technology. It looks into the vulnerabilities in blockchain systems, lists some known cyber incidents, and examines the legal complexity of such threats. The guidelines of this document show how blockchain cybersecurity improves by promoting industrial cooperative ventures and technological advancements. The discourse examines blockchain cybersecurity to establish both the technological and legal aspects of blockchain security, which strengthen ecosystem resilience and protectability.

LITERATURE REVIEW

Literature Review on Blockchain Technology

Blockchain technology holds much interest for research because it is believed to change the ways digital security and trust can be achieved and support decentralized systems. Blockchain was introduced initially by Satoshi Nakamoto in 2008 as the underlying technology powering Bitcoin. Then, the space became so wide and complex that the applications kept expanding beyond cryptocurrency. Its architecture, security frameworks, consensus mechanisms, and regulatory challenges have been