


# Chapter 6


## Improving Cybersecurity and Risk Management Techniques in AI Blockchain Governance Systems

**Puneet Chauhan**

 <https://orcid.org/0009-0000-1652-8764>

*Swami Vivekanand Subharti University,  
India*

**Vikas Sharma**

 <https://orcid.org/0000-0001-8173-4548>


*SRM Institute of Science and  
Technology, Delhi, India*

**Krishan Pal**

 <https://orcid.org/0009-0008-3040-9954>


*Swami Vivekanand Subharti University,  
India*

**Tarun Kumar Vashishth**

 <https://orcid.org/0000-0001-9916-9575>


*IIMT University, Meerut, India*

**Almash Saifi**

 <https://orcid.org/0009-0003-6303-8663>

*Swami Vivekanand Subharti University,  
India*

**Kajal Choudhary**

 <https://orcid.org/0009-0000-6713-6509>

*IIMT University, Meerut, India*

### ABSTRACT

*The combination of AI with Blockchain or AI-Blockchain integration disrupts existing governance structures. Cybersecurity however becomes an important area of concern in system fortitude, data trust, and public confidence. The focus of this chapter is the AI-Blockchain governance system's cybersecurity vulnerabilities such as smart contracts' flaws, AI model attacks, and other blockchain specific weaknesses like 51% and Sybil attacks. Addressing these concerns, some of the focus areas include*

DOI: 10.4018/979-8-3373-3760-9.ch006

*Protecting AI model training, issuing decentralized identities, end-to-end encryption, and blockchain auditors to enhance security. More importantly, fostering proactive threat intelligence, robust governance policies and frameworks, and resilient design architectures for active defences against sophisticated cyber threats is paramount.*

## **INTRODUCTION**

The intersection of Artificial Intelligence (AI) and Blockchain has transformed digital governance systems into decentralized, intelligent, automated frameworks capable of sophisticated AI-Blockchain governance. These frameworks aim for the maximum possible level of information transparency, decision automation, and reliability of the information. The implementation of these technologies, however, introduces new risks related to cybersecurity, trust, and scalability. In traditional systems, a central authority with a predetermined set of security controls effectively reduces risk. In contrast, decentralized, AI driven systems, while inherently more versatile, expose vulnerable trust borders to new attack vectors. For instance, AI algorithms are vulnerable to data poisoning or adversarial examples. Moreover, blockchain systems are not immune to 51% attacks, Sybil attacks, and abuse of smart contract vulnerabilities. This chapter designs specific cybersecurity and risk management frameworks tailored to the governance of AI-Blockchain systems. It highlights the need to safeguard the data's trust, ensuring automated activities are safeguarded from an override, and maintaining ethics and compliance. A proactive approach to defending against sophisticated disruptive policies is pre-emptive threat identification, strong policy formation, and systems built to withstand attacks (Ahmed, 2025).

### **Summary of AI- Blockchain Governance Systems**

AI-Blockchain governance systems represent a paradigm shift in managing infrastructure because of the unique combination of technique and intellect used to run administrative work on digital frameworks. They do not concentrate all authority in one place but instead employ a network of nodes which operate on algorithms that independently decide, apply, and manage rules as well as operations. With the aid of Artificial Intelligence, such systems are able to recognize unique patterns within data, classify them, and make real-time predictions or decisions. This helps in ensuring that governance mechanisms are adaptable, responsive, and anticipatory to emerging situations. Blockchain, on the other hand, guarantees complete assurance of transparency as all actions and outcomes of the decisions are stored in the unchangeable ledger which fosters trust and accountability. Moreover, gover-

30 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/improving-cybersecurity-and-risk-management-techniques-in-ai-blockchain-governance-systems/390944](http://www.igi-global.com/chapter/improving-cybersecurity-and-risk-management-techniques-in-ai-blockchain-governance-systems/390944)

## Related Content

---

### Beacon-Based Cluster Framework for Internet of People, Things, and Services (IoPTS)

Gitanjali Rahul Shinde and Henning Olesen (2018). *International Journal of Ambient Computing and Intelligence* (pp. 15-33).

[www.irma-international.org/article/beacon-based-cluster-framework-for-internet-of-people-things-and-services-iopts/211170](http://www.irma-international.org/article/beacon-based-cluster-framework-for-internet-of-people-things-and-services-iopts/211170)

### An Internet Trading Platform for Testing Auction and Exchange Mechanisms

Haiying Qiao, Hui Jie and Dong-Qing Yao (2005). *International Journal of Intelligent Information Technologies* (pp. 20-35).

[www.irma-international.org/article/internet-trading-platform-testing-auction/2391](http://www.irma-international.org/article/internet-trading-platform-testing-auction/2391)

### Arabic Query Expansion Using WordNet and Association Rules

Ahmed Abbache, Farid Meziane, Ghalem Belalemand Fatma Zohra Belkredim (2016). *International Journal of Intelligent Information Technologies* (pp. 51-64).

[www.irma-international.org/article/arabic-query-expansion-using-wordnet-and-association-rules/164512](http://www.irma-international.org/article/arabic-query-expansion-using-wordnet-and-association-rules/164512)

### Studies of Computational Intelligence Based on the Behaviour of Cockroaches

Amartya Neogi (2015). *Handbook of Research on Swarm Intelligence in Engineering* (pp. 99-146).

[www.irma-international.org/chapter/studies-of-computational-intelligence-based-on-the-behaviour-of-cockroaches/131248](http://www.irma-international.org/chapter/studies-of-computational-intelligence-based-on-the-behaviour-of-cockroaches/131248)

### Solution to Big Data Security Issues

Prashant Srivastava, Niraj Kumar Tiwari and Ali Abbas (2021). *Computational Methodologies for Electrical and Electronics Engineers* (pp. 67-74).

[www.irma-international.org/chapter/solution-to-big-data-security-issues/273835](http://www.irma-international.org/chapter/solution-to-big-data-security-issues/273835)