

# Chapter 9

## Integration of Blockchain and Mobile Edge Computing

**Aarti Sharma**

*University Institute of Engineering and Technology, Thanesar, India*

**Mamtesh Nadiyan**

*National Institute of Technology, Kurukshetra, India*

**Seema Sabharwal**

*Government P.G. College for Women, India*

### **ABSTRACT**

*This chapter begins with the fundamentals of blockchain and MEC. Integrating new technologies like blockchain and MEC is seen as a potential paradigm for managing the voluminous amounts of data produced by today's pervasive mobile devices and subsequently powering intelligent services. With blockchain technology, they can boost the safety of existing MEC systems by using decentralized, immutable, secure, private, and service-efficient smart contracts. These smart contracts fall into three broad categories: public blockchains, consortium blockchains, and private blockchains. Moreover, this chapter discusses the classification and current defence mechanisms of security threats. Potential solutions to MEC's main security challenges are then discussed. Following that, the authors present a classification to assist developers of various architectures in selecting an appropriate platform for specific applications, as well as insights into potential research directions. Finally, the authors present key blockchain and MEC convergence features, followed by some conclusions.*

DOI: 10.4018/978-1-6684-6864-7.ch009

## **INTRODUCTION**

As the internet of things advances, billions of devices are becoming connected to the network. There are more devices connected to the system than ever before, but it's the data volume, not the number of devices, that is growing exponentially. Due to the coordination between devices throughout the network, data traffic is increasing dramatically. According to estimates, by 2022, every person will produce about 2 GB of data per day (Bhat et al., 2020). This is a significant amount of data, but the data collected by devices will blow it away. According to estimates, a connected aeroplane generates five terabytes of data per day. In contrast, a connected hospital produces three terabytes, a smart factory produces three petabytes, and an autonomous vehicle can produce four terabytes. As data is generated, it cannot simply be sent to the cloud for analysis. Even though we have a fast uplink, we cannot carry such a large volume of data with the available bandwidth. Those factors encourage academics and businesses to develop next-generation cloud computing technologies such as Mobile Edge Computing (MEC).

In addition, this chapter first discussed the fundamental principles of blockchain and the MEC system. After that, a discussion of the integration of blockchain and MEC systems, including their requirements and the importance of integration, was presented. Furthermore, several key components based on blockchain technology are discussed. This chapter also discusses some challenges for future research directions with its real-life application and outlines key convergence features of integration based on blockchain and MEC.

### **A. FUNDAMENTAL PRINCIPLE OF BLOCKCHAIN AND MEC SYSTEM**

- ❖ Over the years, cloud computing has evolved into an essential component of data processing. In contrast, cloud servers deployed globally must process enormous amounts of data. In addition, response times and QoS deterioration grow with the user's separation from the cloud. Moreover, computing time is significantly affected by the performance of the user's device. In the future, edge devices will be able to store, compute, and analyse data as we move towards next-generation computing technologies. It is possible to create a wide range of applications using 5G networks and blockchain technology. These include trade and finance, smart cities, smart hospitals, supply chain management, the internet of vehicles, the energy internet, digital asset management, and the industrial internet. A 5G network integrated with blockchain technology offers the following technical benefits (Mafakheri et al., 2018):

21 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/integration-of-blockchain-and-mobile-edge-computing/324153](http://www.igi-global.com/chapter/integration-of-blockchain-and-mobile-edge-computing/324153)

## Related Content

---

### Communiqué Issues in MANET and VANET Protocols With Network Security Disquiet

Mamata Rath, Bibudhendu Patiand Jhum Swain (2020). *Forensic Investigations and Risk Management in Mobile and Wireless Communications* (pp. 195-220).

[www.irma-international.org/chapter/communiqu-issues-in-manet-and-vanet-protocols-with-network-security-disquiet/234078](http://www.irma-international.org/chapter/communiqu-issues-in-manet-and-vanet-protocols-with-network-security-disquiet/234078)

### Electronic Discovery (E-Discovery)

(2021). *Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM* (pp. 69-83).

[www.irma-international.org/chapter/electronic-discovery-e-discovery/259154](http://www.irma-international.org/chapter/electronic-discovery-e-discovery/259154)

### Digital Forensics of Cybercrimes and the Use of Cyber Forensics Tools to Obtain Digital Evidence

(2021). *Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM* (pp. 45-68).

[www.irma-international.org/chapter/digital-forensics-of-cybercrimes-and-the-use-of-cyber-forensics-tools-to-obtain-digital-evidence/259153](http://www.irma-international.org/chapter/digital-forensics-of-cybercrimes-and-the-use-of-cyber-forensics-tools-to-obtain-digital-evidence/259153)

### A Methodological Study of Fake Image Creation and Detection Techniques in Multimedia Forensics

Renu Popli, Isha Kansal, Rajeev Kumarand Ruby Chauhan (2023). *Examining Multimedia Forensics and Content Integrity* (pp. 173-196).

[www.irma-international.org/chapter/a-methodological-study-of-fake-image-creation-and-detection-techniques-in-multimedia-forensics/324151](http://www.irma-international.org/chapter/a-methodological-study-of-fake-image-creation-and-detection-techniques-in-multimedia-forensics/324151)

### 3D Data Security: Robust 3D Mesh Watermarking Approach for Copyright Protection

Imen Fourati Kallel, Ahmed Gratiand Amina Taktak (2023). *Examining Multimedia Forensics and Content Integrity* (pp. 1-37).

[www.irma-international.org/chapter/3d-data-security/324145](http://www.irma-international.org/chapter/3d-data-security/324145)