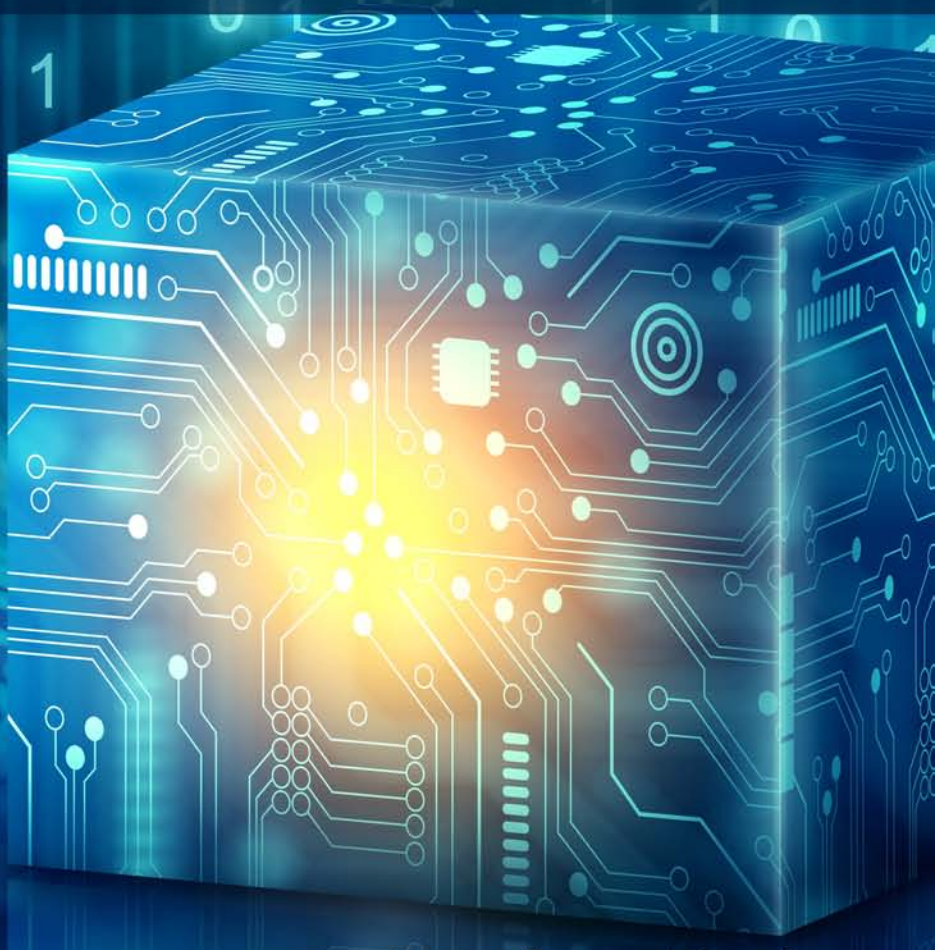
BEYOND BLOCKCHAIN:
REVIEWING THE IMPACT AND EVOLUTION OF DECENTRALIZED NETWORKS - PART 2



Editors:
Sharmila Arunkumar
Neha Goel
R.K. Yadav
Manoj Kumar
Shashi Bhushan

Bentham Books

Beyond Blockchain: Reviewing the Impact and Evolution of Decentralized Networks *(Part 2)*

Edited by

Sharmila Arunkumar, Neha Goel, R.K. Yadav
Department of ECE
Raj Kumar Goel Institute of Technology
Ghaziabad, India

Manoj Kumar
Faculty of Engineering and Information Sciences
University of Wollongong in Dubai
Dubai, United Arab Emirates

&

Shashi Bhushan
Department of Computer and Information Sciences
University Teknologi PETRONAS, Perak, Malaysia

Beyond Blockchain: Reviewing the Impact and Evolution of Decentralized Networks *(Part 2)*

Editors: Sharmila Arunkumar, Neha Goel, R.K. Yadav, Manoj Kumar & Shashi Bhushan

ISBN (Online): 979-8-89881-009-2

ISBN (Print): 979-8-89881-010-8

ISBN (Paperback): 979-8-89881-011-5

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA.

First published in 2025.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

FOREWORD

In an era of rapid technological change, decentralized networks and blockchain technology are revolutionizing various industries. “Beyond Blockchain: Reviewing the Impact and Evolution of Decentralized Networks” provides deep insights into these transformative technologies and their potential to reshape our world.

As an observer of blockchain’s evolution, I am honored to introduce this comprehensive work. This book highlights the significant impact of decentralized technologies and their promising future. It explores these systems in detail, covering applications and emerging trends that will redefine sectors from finance and healthcare to education and environmental monitoring. The authors present 13 well-curated chapters that explain foundational concepts and innovative applications. From Ethereum smart contracts transforming supply chain management to blockchain models promoting sustainable agriculture, each chapter examines real-world solutions offered by these technologies. Notably, the book explores the synergy between blockchain and other technologies like artificial intelligence (AI) and the Internet of Things (IoT). These chapters reveal how combining blockchain with AI can enhance connectivity, security, and efficiency. The discussions on quantum resilience and protective measures against advanced threats are both timely and critical. The authors’ balanced view of the opportunities and challenges of decentralized networks is commendable. They provide a realistic roadmap for future developments, acknowledging hurdles while inspiring readers with future possibilities.

Beyond Blockchain is a vital resource for anyone interested in the transformative power of decentralized networks. Whether you are a student, researcher, industry professional, or tech enthusiast, this book offers the knowledge and insights needed to navigate and contribute to this rapidly evolving field.

I highly recommend this essential read to anyone looking to explore the frontiers of decentralized networks and blockchain technology.

Welcome to the future of blockchain!!

Vinay Rishiwal
Department of CSIT
M. J. P. Rohilkhand University Campus
University in Bareilly
Uttar Pradesh, India

PREFACE

Beyond Blockchain: Reviewing the Impact and Evolution of Decentralized Networks (Part 2) delves deeper into the progressive developments and emerging intersections of decentralized technologies with advanced computing paradigms. Building on the foundational insights from Part 1, this section focuses on futuristic integrations, security concerns, and transformative use cases across various sectors.

Comprising six comprehensive chapters, the book presents a nuanced exploration of cutting-edge innovations that are shaping the next era of decentralized systems. It caters to researchers, academicians, and professionals who seek to understand the evolving synergy between blockchain and other frontier technologies. Chapter 1 begins with an exploration of the convergence between Artificial Intelligence (AI) and blockchain within the Internet of Things (IoT), emphasizing enhanced connectivity, security, and autonomous interactions. Chapter 2 introduces a paradigm shift in machine learning through blockchain-driven federated learning, enabling secure, decentralized, and privacy-preserving data collaboration. Chapter 3 addresses critical security challenges by examining quantum resilience. It outlines potential quantum threats and explores strategies to fortify decentralized systems against quantum attacks. In Chapter 4, the discussion expands to broader technological advancements and the development of blockchain beyond conventional applications, showcasing its relevance in diverse industrial landscapes.

Chapter 5 offers an analytical perspective on the transformative impact of decentralized networks, exploring their evolutionary pathways and socio-technical implications. Finally, Chapter 6 presents a comprehensive review of state-of-the-art research, emerging trends, and real-world use cases of blockchain technologies across sectors.

This book aims to deepen the understanding of advanced decentralized technologies and inspire innovations that drive secure, intelligent, and inclusive digital ecosystems.

Sharmila Arunkumar
Department of ECE
Raj Kumar Goel Institute of Technology
Ghaziabad, India

Neha Goel
Department of ECE
Raj Kumar Goel Institute of Technology
Ghaziabad, India

R.K. Yadav
Department of ECE
Raj Kumar Goel Institute of Technology
Ghaziabad, India

Manoj Kumar
Faculty of Engineering and Information Sciences
University of Wollongong in Dubai
Dubai, United Arab Emirates

&

Shashi Bhushan
Department of Computer and Information Sciences
University Teknologi PETRONAS, Perak, Malaysia

List of Contributors

A. A. Abd El-Aziz	College of Computer and Information Sciences, Jouf University, Sakaka, Kingdom of Saudi Arabia Faculty of Graduate Studies for Statistical Research, Cairo University, Al Giza, Egypt
Anuj Kumar	Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India
A. Sowmya	Department of Computer Science and Engineering, Vardhaman College of Engineering Narkhuda, Telangana-501218, India
C. Kavita	Department of Computer Science and Engineering, Vardhaman College of Engineering Narkhuda, Telangana-501218, India
Divya Dutt	Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India
Daksh Kalia	Amity School of Engineering and Technology, Amity University Punjab, Mohali, Punjab, India
Farah Naz	Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India
Hashmat Usmani	Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India
K. Nallarasu	BSA Crescent Institute of Science and Technology, Chennai, India
L. Remegius Praveen Sahayaraj	Loyola-ICAM College of Engineering and Technology, Chennai, India
Manoj Kumar	Faculty of Engineering and Information Sciences, University of Wollongong in Dubai, Dubai, United Arab Emirates
Maged Nasser	Department of Computer & Information Sciences, Universiti Teknologi Petronas, Perak, Malaysia
Nikhil Gupta	IIMT Engineering College, Meerut (U.P.), India
Pramod Kumar	Himalayan School of Science and Technology, SRHU, Dehradun, India
R. Uma Mageswari	Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
R.K. Yadav	Department of ECE, Raj Kumar Goel Institute of Technology, Ghaziabad, India
Renu Rani	Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India
Sharmila Arunkumar	Department of ECE, Raj Kumar Goel Institute of Technology, Ghaziabad, India
Shashi Bhushan	Department of Computer & Information Sciences, Universiti Teknologi Petronas, Perak, Malaysia
Shanthi Makka	Department of Computer Science and Engineering, Vardhaman College of Engineering Narkhuda, Telangana-501218, India
Shailesh Kumar Gupta	IIMT Engineering College, Meerut (U.P.), India
Soniya Gupta	FET, Swami Vivekanand Subharti University, Meerut, India
Shobhita Singh	Amity School of Engineering and Technology, Amity University Punjab, Mohali, Punjab, India

CHAPTER 1

A Paradigm Shift: Blockchain-Driven Federated Learning

R. Uma Mageswari[1,*], K. Nallarasu[2], L. Remegius Praveen Sahayaraj[3] and **A. A. Abd El-Aziz[4,5]**

[1] *Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India*

[2] *BSA Crescent Institute of Science and Technology, Chennai, India*

[3] *Loyola-ICAM College of Engineering and Technology, Chennai, India*

[4] *College of Computer and Information Sciences, Jouf University, Sakaka, Kingdom of Saudi Arabia*

[5] *Faculty of Graduate Studies for Statistical Research, Cairo University, Al Giza, Egypt*

Abstract: Blockchain-driven Federated Learning (BFL) represents an intriguing intersection of two cutting-edge technologies: blockchain and federated learning. A form of distributed machine learning technique known as Federated Learning (FL) aims to preserve the privacy of user data. FL supports privacy preservation, decentralization, and collaborative learning by the means of retaining user data on local devices, training the models without sharing raw data, minimizing the danger of leakage of user data, and avoiding the need for centralized data storage. Beyond these attractive features held by FL, arduous challenges like ensuring secure model aggregation and communication, failure of single points, vulnerability faced by centralized parameter servers, minimal client participation due to lack of motivation, and incentives lacking are encountered. To provide a solution for these obstructions, an innovative idea is to integrate FL with blockchain, which is another decentralized cutting-edge technology. This collaboration leads to a much more robust BFL. FL can be enhanced through blockchain *via* data provenance where blockchain records data origins as well as model updates by using consensus mechanisms. The consensus mechanisms here ensure the decentralized model integrity, and then the Smart Contracts ensure the automated reward distribution to incentivize participation. FL and blockchain technology use cases are mostly involved in sectors like healthcare, finance, transportation, smart cities, *etc*. independently. These two core technologies, FL and blockchain, are constructively combined to achieve inviolable higher-end applications, which promise minimized data leakage risk in collaborative data sharing.

[*] **Corresponding author R. Uma Mageswari:** Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India; E-mail: uma18.research@gmail.com

Sharmila Arunkumar, Neha Goel, R.K. Yadav, Manoj Kumar & Shashi Bhushan (Eds.)

Keywords: Blockchain, Byzantine fault tolerance (BFT), Data provenance, Data privacy, Decentralized AI, Data ownership, Data governance, Decentralization, Federated learning, Machine learning, Smart contracts, Scalable machine learning.

INTRODUCTION

Traditional methods of data collection and analysis often involve centralizing data, raising issues regarding privacy breaches and data security. Federated Learning (FL) emerges as a promising solution, offering a paradigm shift in how we approach machine learning models. As a subset of the machine learning field, FL works on training a local model to ensure that the data remains decentralized in the local node or server from where the data originates. Alternatively, federated learning is called collaborative learning. Moreover, it differs from traditional machine learning in terms of decentralization [1]. A local model is trained by each client in the respective local node by using one's own generated data samples. In order to cope up with the global model, these local nodes exchange the weight and bias parameters of Deep Neural Networks periodically. From the perspectives of data privacy, data minimization, and data access rights, FL faces tremendous challenges such as single point of failure, malicious data injections, and vulnerable nodes due to unreliable communications in the network. Nevertheless, FL is made to provide data privacy by incorporating blockchain and federated learning, thus resulting in Blockchain-driven Federated Learning (BFL). Blockchain smart contracts automate the processes based on predefined rules that prevent the contract-violating malicious nodes from taking participation [1]. Meanwhile, blockchain records each transaction and Proof of Work (PoW) consensus for ensuring data integrity and preventing malicious behaviour [2].

Integrating blockchain technology with FL introduces several benefits and addresses certain challenges inherent in decentralized learning environments.

Data Integrity and Immutability

Blockchain's decentralized and tamper-resistant ledger ensures the integrity and immutability of transactions. In FL, where model updates are transmitted and aggregated across multiple nodes, blockchain can confirm the integrity and authenticity of these updates, thus avoiding unauthorized modifications or tampering.

Transparent and Auditable Transactions

Blockchain provides transparency and auditability by recording all transactions in a distributed ledger. This transparency can enhance trust among participants in FL

ecosystems, as they can verify the history of model updates and consensus mechanisms used for aggregation.

Decentralized Governance

Blockchain facilitates decentralized governance mechanisms, enabling stakeholders in FL ecosystems to participate in decision-making processes. Smart contracts, deployed on blockchain networks, can automate governance rules, such as determining eligibility criteria for participating nodes or allocating rewards based on contributions to model training.

Secure Data Sharing and Monetization

Blockchain enables data sharing in a secure and transparent manner among participants in FL networks. For providing privacy, smart contracts enforce data access control mechanisms by allowing the data owners to maintain control over their data while still monetizing its value through FL collaborations.

Incentive Mechanisms

Blockchain-based incentive mechanisms, such as tokenization and Decentralized Finance (DeFi) protocols, can incentivize participation and contribution to FL networks. Participants can earn rewards or tokens for sharing data, training models, or providing computational resources, thereby fostering a more collaborative and incentive-aligned ecosystem.

Scalability and Interoperability

Blockchain offers scalability and interoperability features that can facilitate FL being integrated with other decentralized networks and technologies. By leveraging blockchain's interoperability protocols, FL systems can interact with diverse blockchain platforms and ecosystems, expanding their reach and potential applications.

Privacy-Preserving Infrastructure

Some blockchain platforms, like privacy-focused blockchains or Zero-Knowledge Proof (ZKP) protocols, offer advanced privacy-preserving features. These features can improve the user privacy and confidentiality of FL transactions and data exchanges by ensuring the protection of crucial data throughout the training duration.

CHAPTER 2

Quantum Resilience: Protecting Blockchain from Advanced Threats - Unveiling Quantum Attacks and Enhancing Security Measures

Sharmila Arunkumar[1,*], Shashi Bhushan[2], Manoj Kumar[3], R.K. Yadav[1] and **Pramod Kumar[4]**

[1] *Department of ECE, Raj Kumar Goel Institute of Technology, Ghaziabad, India*

[2] *Department of Computer & Information Sciences, Universiti Teknologi Petronas, Perak, Malaysia*

[3] *Faculty of Engineering and Information Sciences, University of Wollongong in Dubai, Dubai, United Arab Emirates*

[4] *Himalayan School of Science and Technology, SRHU, Dehradun, India*

Abstract: The emergence of quantum computing poses a significant threat to the security of blockchain protocols, primarily due to the vulnerability of current cryptographic algorithms to quantum attacks. This vulnerability jeopardizes the integrity of data and assets stored on blockchain networks, which currently hold hundreds of billions of dollars in cryptocurrencies and other digital assets. To mitigate this risk, various proposals and solutions have been presented in the literature. However, most existing proposals are either theoretical, rely on large quantum key distribution (QKD) networks, or advocate for the development of new quantum-resistant blockchain networks from scratch. Despite the understanding of the quantum threat and potential solutions, practical implementations are scarce. A recent survey paper addresses this gap by proposing an end-to-end framework for achieving post-quantum resistance in existing blockchain networks. The framework, outlined in the survey, is compatible with Ethereum-based networks and offers practical solutions for key generation, secure communication between nodes, and transaction verification. Notably, the framework utilizes quantum entropy for key generation, and post-quantum TLS connections, and introduces post-quantum signatures in transactions. Additionally, it incorporates on-chain verification mechanisms using Solidity smart contracts and modified EVM Opcode. This chapter represents a significant contribution to the field by providing a comprehensive overview of existing solutions and proposing a practical framework for enhancing blockchain security against quantum threats.

* **Corresponding author Sharmila Arunkumar:** Department of ECE, Raj Kumar Goel Institute of Technology, Ghaziabad, India; E-mail: Sharmila1ece@gmail.com

Sharmila Arunkumar, Neha Goel, R.K. Yadav, Manoj Kumar & Shashi Bhushan (Eds.)

Keywords: Blockchain security, Cryptographic resilience, Public-Key cryptography, Quantum computing, Quantum entanglement, Quantum attacks, Quantum algorithms, Quantum superposition, Quantum-resistant algorithm.

INTRODUCTION

Quantum computing, based on the principles of quantum mechanics such as superposition and entanglement, offers processing power that far surpasses that of classical computing. This immense capability allows quantum computers to solve complex problems at previously unimaginable speeds, posing a direct threat to established cryptographic systems. Notably, Shor's and Grover's algorithms have demonstrated the potential to breach widely-used cryptographic protocols, putting blockchain security at risk and making systems vulnerable to sophisticated quantum attacks.

The first part of this chapter delves into the foundational concepts of quantum computing and its impact on information processing. It explores the vulnerabilities of current blockchain systems to quantum attacks and underscores the critical importance of developing cryptographic algorithms resistant to quantum threats. By examining Quantum Key Distribution (QKD) and other quantum cryptography methods, the research highlights how quantum mechanics can provide unprecedented levels of security [1].

This chapter's initial section thoroughly examines the fundamental theories of quantum computing and their relevance to information processing. It details how existing blockchain systems are susceptible to quantum attacks and emphasizes the necessity of creating quantum-resistant cryptographic algorithms. The research illustrates the potential for quantum mechanics to offer previously unseen degrees of security by analyzing Quantum Key Distribution (QKD) and other quantum encryption techniques [2].

The discussion extends to practical implementations and theoretical advancements in quantum cryptography and Quantum Key Distribution (QKD). These systems utilize the unique properties of quantum physics to establish secure communication channels, offering fundamentally different security assurances compared to classical cryptography assumptions [3 - 5].

As the chapter navigates the complexities of quantum resilience, it also highlights ongoing research and experimental advancements in the field. The aim is to provide a comprehensive overview of the current landscape, emerging trends, and future directions in quantum computing and blockchain security. This includes examining the role of quantum entropy in generating perfect randomness for

cryptographic keys and addressing advanced threats in the quantum computing era.

Understanding and preparing for the impact of quantum computing on blockchain security is imperative for the future. This research aims to equip researchers, practitioners, and stakeholders with the knowledge necessary to enhance blockchain security strategies and ensure resilient cryptographic solutions in the face of quantum advancements. By investigating the interplay between blockchain security and quantum computing, the study contributes to the growing body of knowledge, promoting the development of resilient security protocols that can withstand the quantum future. The chapter starts with an exploration of the foundational concepts of quantum computing and blockchain, elucidating how quantum computing's immense processing power threatens traditional cryptographic systems. It then delves into the vulnerabilities of current blockchain systems to quantum attacks, highlighting the necessity for developing post-quantum cryptographic algorithms [6 - 8].

A detailed analysis is presented on the impact of quantum attacks on blockchain, examining specific vulnerabilities in cryptographic schemes. The discussion extends to practical applications and use cases affected by these quantum vulnerabilities, illustrating the real-world implications of this emerging threat [9].

Furthermore, the chapter explores various fields of application for quantum-resistant cryptographic methods and outlines future research directions in quantum computing and blockchain security. By addressing these critical areas, the chapter aims to equip researchers, practitioners, and stakeholders with the knowledge needed to enhance blockchain security strategies and develop resilient cryptographic solutions in the face of quantum advancements.

QUANTUM COMPUTING

Computers today operate based on the principles of classical physics, and their performance improvements have historically followed Moore's Law, which predicts a doubling of computational power approximately every 18 months due to the increasing number of transistors on integrated circuits. However, as transistors shrink to atomic sizes, we approach a fundamental physical barrier, necessitating the exploration of new technologies to sustain and surpass this growth [10].

The field of quantum computing is a cutting-edge combination of computer science and physics that focuses on developing data processing devices and techniques based on the ideas of quantum mechanics. Unlike classical computers, which employ bits that can only be either 0 or 1, quantum computers use qubits,

CHAPTER 3

Unveiling Tomorrow: Emerging Technologies and Development in Blockchain

Renu Rani[1], Hashmat Usmani[1,*], Farah Naz[1], Divya Dutt[1] and **Anuj Kumar[1]**

[1] *Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India*

Abstract: Blockchain can facilitate peer-to-peer digital data exchange with few or no middlemen or third parties between parties who do not particularly trust one another. Data could relate to any transaction or asset that can be converted into a digital format, such as money, contracts, insurance policies, land titles, medical and educational records, birth and marriage certificates, and the purchasing and selling of goods and services. As technology develops, we might expect to see even more innovative and cutting-edge applications for blockchain in the years to come. Blockchain has the potential to completely transform many industries while also improving safety and transparency. This possibility is currently being investigated by numerous organizations and in a number of sectors.The Joint Research Centre (JRC), the science and knowledge service of the European Commission, draws together research from various units and disciplinary fields to produce the report Blockchain Now and Tomorrow. The resilience of blockchain technology against hacking and data manipulation is comforting in an era where cybercrime is on the rise. We anticipate seeing more businesses use this technology, leading to more efficient and transparent transactions that are protected from fraud. It makes sense that business executives all over the world are interested in blockchain due to its potential to upend established business models.

Once only serving as the backbone of cryptocurrency technology, the blockchain is now serving as the basis for a wide range of exciting new applications. Looking ahead, it is clear that this technology has the ability to fundamentally alter the ways in which we engage with the digital and real worlds. This study explores the possible uses of blockchain technology in the fields of financial inclusion, urban development, supply chain management, and data security. The new era we are about to enter will be dominated by blockchain technology.

Keywords: Cutting-edge applications cryptocurrency, Hacking and data manipulation, JRC, Resilience.

[*] **Corresponding author Hashmat Usmani:** Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India; E-mail: huecefec@rkgit.edu.in

Sharmila Arunkumar, Neha Goel, R.K. Yadav, Manoj Kumar & Shashi Bhushan (Eds.)

INTRODUCTION

The software development community occasionally becomes fixated on a particular buzzword. Let me introduce you to blockchain technology, which is similar to cryptocurrencies but has more features and complexity. Its ability to pique curiosity has led to changes and increased potency in its uses. The possibilities of blockchain technology go far beyond virtual currencies.

It offers an immutable, decentralized ledger system that improves integrity, security, and transparency in a variety of industries. Atop this disruption is software development [1]. In terms of tech stacks, data management, and security are the areas where new technologies like blockchain have the biggest impact. Because of its decentralized architecture, which guarantees data integrity, it is perfect for sectors including government, healthcare, supply chain, and finance.

Developers may enable safe transactions, improve data privacy and cyber security, and produce tamper-proof data trails by incorporating blockchain into tech stacks.

For example, a web application that uses blockchain technology to verify user identities is possible [2]. This makes it possible for users to maintain control over their data. The trust between humans and machines will grow stronger with this additional security layer. Higher user adoption and improved customer experiences would result from this [3].

One of the cutting-edge technologies that is revolutionizing global business across numerous industries is blockchain [4]. Increased security reduces duplication of effort, which increases efficiency. Blockchain is transforming a number of industries including education, healthcare, financial services, business, and supply chains [5]. The future scope of blockchain technology in various fields is discussed in the chapter.

DECENTRALIZED SYSTEMS

Decentralized systems represent a paradigm shift in how data, resources, and computational tasks are managed across networks. Unlike traditional centralized systems that rely on a single controlling entity, decentralized systems distribute control, data storage, and decision-making across multiple nodes. This structure enhances scalability, fault tolerance, and resilience, making these systems ideal for modern applications where reliability and autonomy are critical. The rise of decentralized systems has been fueled by the need for greater privacy, security, and independence from central authorities. These systems empower users, promote transparency, and enable innovative solutions across various domains.

From file sharing and identity management to advanced machine learning and internet infrastructure, decentralized systems have revolutionized the way we think about technology and collaboration.

In the sections that follow, we explore diverse examples of decentralized technologies, including Distributed Hash Tables (DHTs), Federated Learning, Decentralized Identity Solutions, and the InterPlanetary File System (IPFS). Each system illustrates a unique facet of decentralization, showcasing its potential to address specific challenges in today's interconnected world.

Distributed Hash Tables (DHTs)

DHTs are a foundational technology in many peer-to-peer networks, such as BitTorrent. They enable decentralized storage and retrieval of data without relying on a central server. Each node in the network is responsible for a portion of the data, and queries are routed efficiently through a distributed structure. This system ensures resilience and scalability, which are essential for decentralized file sharing and data distribution.

Federated Learning

Federated learning represents a significant advancement in artificial intelligence, where model training occurs directly on devices rather than central servers. This approach not only enhances privacy by keeping sensitive data local but also reduces latency and bandwidth usage. Federated learning is particularly valuable in sectors like healthcare and finance, where data privacy is critical.

Decentralized Identity Solutions

Beyond blockchain, decentralized identity solutions are gaining traction as a way to give individuals control over their personal data. These systems allow users to manage their digital identities without relying on centralized authorities, reducing the risk of data breaches and enhancing privacy. Technologies like self-sovereign identity (SSI) frameworks empower users to selectively share information with service providers.

InterPlanetary File System (IPFS)

IPFS is a peer-to-peer protocol designed to make the web more decentralized by enabling users to store and share files without relying on a centralized server. Instead of retrieving files from a single location, IPFS locates and retrieves content based on its unique hash, ensuring data integrity and availability. This technology has potential applications in content distribution, data archiving, and building a more resilient internet infrastructure.

CHAPTER 4

Decentralized Networks: Transformative Impacts and Evolutionary Trajectories

Shanthi Makka[1,*], **A. Sowmya**[1] and **C. Kavita**[1]

[1] *Department of Computer Science and Engineering, Vardhaman College of Engineering Narkhuda, Telangana-501218, India*

Abstract: Decentralized networks have transcended the confines of Blockchain technology, permeating various spheres of our digital landscape. This chapter explores the profound impact and evolutionary trajectory of decentralized networks beyond Blockchain, elucidating their transformative potential and emerging trends. In addition to monetary exchanges, distributed systems are disrupting workflows of collecting and sharing data, while promoting openness, safeguards, and ownership in the age of data credibility and sovereignty crises. These networks allow Distributed File Systems that store data encrypted and in pieces in numerous nodes. Starting from ride-sharing services to peer-to-peer accommodation, such networks build reliability, effectiveness, and fair distribution of values among the nodes. In the sphere of management and cooperation, distributed systems provide a clear process of decision-making and allow to work together. Through the use of Blockchain and smart contracts, Decentralized autonomous organizations (DAOs) facilitate organisations that are self-governed through collective participation and control of assets and other organisational resources and activities. Also, decentralised networks are creating intrinsic dynamics in identity management where people own their digital identities. By means of self-sovereign identity solutions, the management and exchange of personal data are protected from third-party service providers, thus eliminating such unfavorable consequences as identity theft and surveillance. Some of the general problems being faced by decentralized networks include scale, how different parts of a network work together, and legal concerns. Though the progression of the centralization point can allow monopolization, creation of trust, and stimulation of the demand across various market sectors in terms of networks, the promise of decentralized networks in terms of democratization of access, creation of trust, and stimulation of various domains is unparalleled. Thus, it will be crucial to foster cooperation, prototyping, and better definition of regulatory requirements, which will be the defining decentralised future of the Blockchain technology era.

* **Corresponding author Shanthi Makka:** Department of Computer Science and Engineering, Vardhaman College of Engineering Narkhuda, Telangana-501218, India; E-mail: dr.shanthimakka@gmail.com

Sharmila Arunkumar, Neha Goel, R.K. Yadav, Manoj Kumar & Shashi Bhushan (Eds.)

Keywords: Blockchain, Bitcoin, Consensus mechanisms, Cryptocurrencies, Decentralized autonomous organizations, Decentralized network, Digital identities, Ethereum, Governance models, Hyper ledger fabric, Healthcare, Identity management, Proof of Work (PoW), Proof of Stake (PoS), Regulatory clarity, Smart contract, ZKPs.

INTRODUCTION

The availability of decentralized networks [1] can be cited as one of the breakthroughs in the further evolutionary perspective of technology as an open progressive potential capable of further changing society at various levels. This chapter opens up the path through the complex world of decentralised networks, their significance, and developmental paradigms. Decentralized networks differ from the omnipresent centralized networks since the latter transfer power, authority, and control to their members. These networks, made possible by current advanced technologies like Blockchain, P2P, and DLT bring new, advanced paradigms in terms of collaboration, governance, and innovation. Decentralized networks are such networks while decentralization is an ideology of a network, promoting values of openness, transparency, and justice [2]. Replacing centralized traditional middlemen with decentralized networks makes social actors more self-reliant, agile, and trustworthy in the digital environment. In this chapter, we explore the various roles of decentralized networks [3] in a wide range of applications. These networks drive significant changes across the domains of finance and commerce, governance, the healthcare industry, and many others, creating new possibilities for organizational improvements, fairness, and democratic practices.

In addition, we elaborate on the evolutional processes of decentralized networks as being developed on an experimental basis to become powerful players that are remodeling the sphere of connections between individuals. In the following work, we discuss fundamental milestones, crucial difficulties, and emerging achievements in understanding this evolutionary change aiming to reveal the relationships between the progression of technologies, policies, and social context. During this journey, we encounter essential questions and concerns related to adaptability and the future of decentralized networks, as shown in the decentralized network in Fig. (**1**).

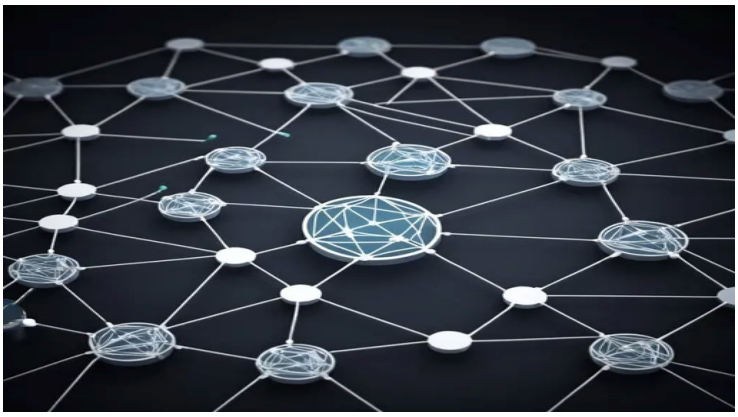


Fig. (1). Decentralized Network.

In conclusion, this chapter became a map, that shows the readers the loops of decentralized networks, defines their revolutions, and outlines further developments. In indulging in these themes, we derive the most valuable lessons in appreciating the seismic socio-technological changes that are driving our postmodern digital cultures and the uncharted territories that are on the horizon.

Decentralized network is a revolution in terms of how data and operations are handled in diverse systems. Unlike traditional hierarchical models, a single point may manage an entire network; the distributed controllers are spread out over the nodes inherent to the structure. In each network, there is no centralized control, and every node has the same level of prerogative to check or validate a particular transaction or entries, thus making it more secure, transparent, and reliable. Decentralized networks [4] have been designed to work under the concept that no particular entity should manage the network overwhelming. This basic change enables greater democracy in the functioning, reduces the occurrence of one single known failure, and also increases the levels of confidence in the members. Decentralization in its essence can be seen as a concrete outcome of the need for improving security, increasing inclusiveness, and clashing against failures or malicious intent.

Distributed Hash Table (DHT) is the distributed system for supporting the storage and lookup of data, which are partitioned and located according to hash values of keys; DHT is important to the large-scale P2P system. They afford flexibility because other peers can sign up and can take off flexibly and they ensure that the search time complexity is logarithmic. P2P networks are heavily used in the Blockchain for maintaining, and validating the decentralized ledger, and most often, DHTs are incorporated for the efficient storage and retrieval of data. For example, activities such as the preservation of big or less significant Blockchain

CHAPTER 5

Significance, Development and Applications of Decentralized Networks beyond Blockchain

Nikhil Gupta[1], **Shailesh Kumar Gupta**[1,*] and **Soniya Gupta**[2]

[1] *IIMT Engineering College, Meerut (U.P.), India*

[2] *FET, Swami Vivekanand Subharti University, Meerut, India*

Abstract: A sophisticated database system called blockchain technology makes it possible for information to be shared transparently inside a company network. In a blockchain database, information is stored in blocks that are linked together in a chain. The data is persistent over time since the chain cannot be withdrawn or changed without network permission. Thus, you may track orders, payments, accounts, and other transactions by creating an unchangeable or immutable ledger using blockchain technology. Unauthorized transaction entries are prevented by built-in system features, which also ensure consistency in the common view of these transactions. Although this new technology is in the primary stage of its development as the internet was in 1990 and has the potential of becoming a disruptive technology like the internet as a technology, Blockchain technology is the one that has changed our way of life the most in the past ten years. It can be developed as a technology over which numerous applications can be implemented . Blockchain is a decentralized, trustworthy, and challenging to use fraudulently database storage technology. The cutting-edge technology known as blockchain has the power to completely change how the industries run, how the businesses operate, how the government functions, and how people use technology in their lives. This chapter covers the features, benefits, generations, and numerous blockchain systems of blockchain technology across a variety of industries. The applications of Blockchain Technology that are being developed in the various fields are described and their future scope is investigated. This chapter highlights the transition from blockchain-centric systems to innovative decentralized architectures, focusing on their significance, development, applications, and potential to shape the future of decentralized technologies.

Keywords: Blockchain technology, Energy industry, Financial accounting, Healthcare, IoT, Insurance sector, Logistics management.

[*] **Corresponding author Shailesh Kumar Gupta:** IIMT Engineering College, Meerut (U.P.), India; E-mail:drskggbu@gmail.com

Sharmila Arunkumar, Neha Goel, R.K. Yadav, Manoj Kumar & Shashi Bhushan (Eds.)

INTRODUCTION

In November 2008, Satoshi Nakamoto (a pseudo name of a person or a group of persons) published a white paper in which he proposed the development of a virtual currency, named Bitcoin. This virtual currency is based on a chain of data blocks that is cryptographically secure, publicly available, and decentralized. According to this paper, the proposed system allows peer-to-peer digital currency transfer and eventually eliminates the need for a regulatory financial institution, like banks, for currency circulating or for settling transactions.

In this paper, two innovative technological ideas are presented. The idea of a digital currency that can be transferred without the control of a centralized authority and the concept of blockchain infrastructure. Blockchain is a chain of data blocks interconnected to each other by cryptographic algorithms that are based on complex computations. This technology ensures that any kind of digital assets having value can be stored in the blocks of the blockchain.

Blockchain can be considered a distributed ledger technology that establishes transparency and trust. Blockchain networks can be utilized as a person-to-person network and a public database that is not operated on a centralized server [1].

One of the strongest features of blockchain is the use of "hashes." Every block in the Blockchain network contains some data to be stored, and when a new block is added to the network it is encoded with a hash code that is generated by the arithmetic calculation. In this calculation, the date of the block creation is used. Hashes are normally used to secure passwords [2].

When a new block is added, the hash of the previous block is inserted into the new block. In this way, it becomes very difficult to falsify both the blocks simultaneously. Hashes of previous blocks in the current block calculate the hashes of subsequent blocks. Hence, making alterations in one block will require making changes in other blocks also, thus recreating the entire network of blocks. This process of creating links of blocks into a chain-like structure makes it extremely difficult to tamper with the blocks of the blockchain.

In 2018 [3], an author provided a summary of the issues faced by Web 2.0, explained the decentralized web, and listed the technologies currently under development. In order to improve the web, people should focus on finding solutions to their problems as well as the challenges these platforms have brought out. The decentralized web is concentrated on creating underlying technologies and protocols that are invisible to end users.

HISTORICAL OVERVIEW OF DECENTRALIZED NETWORKS

The concept of decentralized systems is relatively new in the mainstream, but it has roots that stretch back decades. Some of the innovations of the 70's and 80's laid the foundations of decentralized networks like ARPANET introduced the concept of packet switching in which data was broken into smaller packets and routed independently. USENET was a decentralized network of newsgroups and showed how peer-to-peer communication can be used for sharing information without the need for a central authority. A peer-to-peer file-sharing application Napster (1999) allowed its users to exchange music files directly. BitTorrent (2001) was an advanced peer-to-peer protocol allowing the distribution of large files. These applications demonstrated the potential of decentralized networks. Bitcoin (2009) introduced the concept of blockchain, a decentralized and immutable ledger that records transactions across several computers. Ethereum (2015) further extended the concept of blockchain by introducing smart contracts in which self-executing contracts with the terms of the agreement are directly coded into the application. These innovations further opened up the possibilities for decentralized applications (dApps) and decentralized finance (DeFi). Decentralized applications built on blockchain technology offer various promising functionalities like decentralized exchanges, decentralized web (web3), decentralized gaming, and decentralized social media. Table **1** summarizes the centralised *vs.* decentralized blockchain in tabular form.

Table 1. Centralised *vs.* Decentralized Blockchain.

S. No.	Parameter	Centralized Systems	Decentralized Systems
1	Efficiency	**Advantages:** Centralized systems can process transactions quickly. Data can be accessed and processed swiftly with reduced response times, thus having lower latency. **Disadvantages:** A single point of failure can disrupt the entire system. High traffic or overload can lead to performance degradation.	**Advantages:** The distributed nature of decentralized systems makes them resilient to failures. It can handle increasing workloads by utilizing additional nodes in the network. **Disadvantages:** Slower Processing: Consensus mechanisms can slow down the processing of transactions. Higher Computational Costs: Maintaining and securing the network requires significant computational resources.

CHAPTER 6

Unveiling the Potential: Blockchain Technology and its Applications Across Industries

Daksh Kalia[1,*], **Shobhita Singh**[1] and **Maged Nasser**[2]

[1] *Amity School of Engineering and Technology, Amity University Punjab, Mohali, Punjab, India*

[2] *Department of Computer & Information Sciences, Universiti Teknologi Petronas, Perak, Malaysia*

Abstract: In recent years, blockchain technology has emerged as a disruptive force, bringing significant improvements in security, transparency, and operational efficiency across various industries. This abstract synthesizes findings from research publications spanning 2019 to 2024, showcasing widespread applications and transformative potential of blockchain. Its decentralized and immutable characteristics address crucial issues like data trust and integrity, making it invaluable across multiple domains. In the financial sector, blockchain facilitates secure cryptocurrency transactions and drives the adoption of smart contracts, streamlining asset management and automating legal agreements. In healthcare, it strengthens the protection of sensitive patient data, ensuring both privacy and data accuracy, while also enhancing administrative workflows by centralizing records and minimizing manual paperwork. Furthermore, blockchain has begun reshaping global supply chains by improving the traceability of goods, reducing fraud, and fostering greater trust among partners. Beyond these applications, the fusion of blockchain with other emerging technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI), holds even greater promise for innovation. The integration of IoT with blockchain can facilitate more secure and efficient data exchange between smart devices, while AI can boost blockchain's role in predictive analytics and automation. This review delves into the profound influence blockchain has across industries, highlighting its pivotal role in shaping the future of digital systems and its potential to unlock new avenues for security, efficiency, and innovation.

Keywords: AI synergy, Blockchain, Cryptocurrencies, Decentralized systems, Digital transformation, Healthcare applications, IOT integration, Smart contracts, Supply chain management, Technology.

[*] **Corresponding author Daksh Kalia:** Amity School of Engineering and Technology, Amity University Punjab, Mohali, Punjab, India; E-mail: dakshalia016@gmail.com

INTRODUCTION

Blockchain technology, initially conceptualized as the underlying infrastructure for Bitcoin by an anonymous entity known as Satoshi Nakamoto in 2008, has evolved significantly since its inception. At its core, blockchain is a decentralized digital ledger that logs transactions on a distributed network of computers, ensuring that once transactions are recorded, they cannot be altered retroactively. This immutable ledger is maintained through a consensus mechanism, ensuring that all participants in the network agree on the validity of the transactions. A blockchain is made up of blocks, with each block consisting of a list of transactions [1]. Each block includes a cryptographic hash of the previous block, a timestamp, and transaction data. The cryptographic hash ensures the integrity of the data, as any change in a block's information will alter the hash, making tampering easily detectable. Unlike traditional centralized systems, blockchain functions on a decentralized network where no single entity has control over the entire system. Instead, all participants (nodes) share control. To validate, blockchain uses consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), and other algorithms that ensure network-wide agreement on the state without needing a central authority [2]. The following Fig. (**1**) is about the use cases, components, and types of blockchain below:

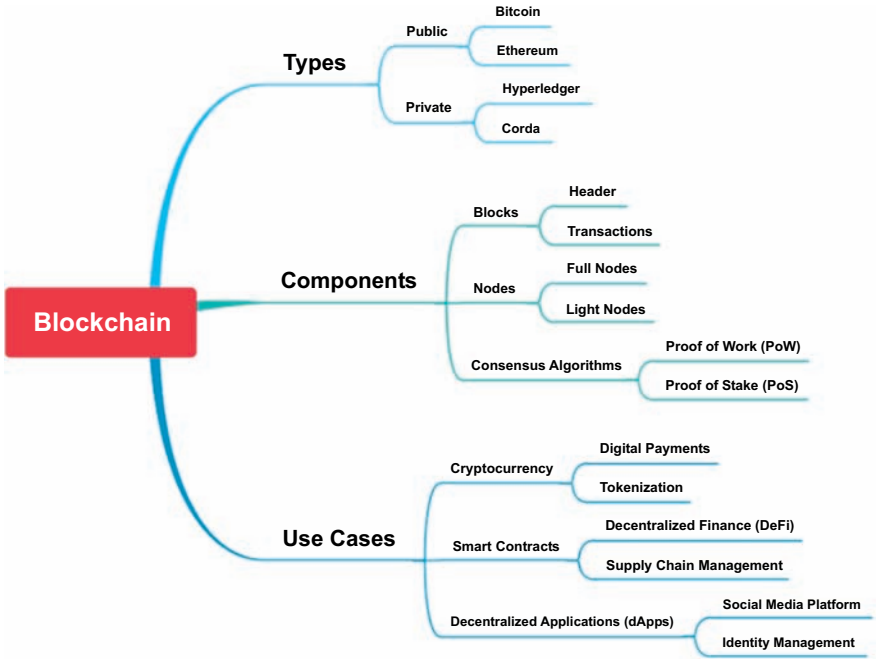


Fig. (1). Introduction to blockchain.

Blockchain's design inherently enhances security and transparency [3]. The decentralized nature makes it resistant to attacks, as altering any information would require consensus across the majority of the network. Furthermore, transparency enables all participants to see transactions, promoting trust and accountability.

APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Blockchain technology transcends its origins in cryptocurrency to offer transformative solutions across diverse sectors, including finance, medical care, supply chain management, IoT, and AI. The following Fig. (**2**) explains the growth of blockchain over the years.

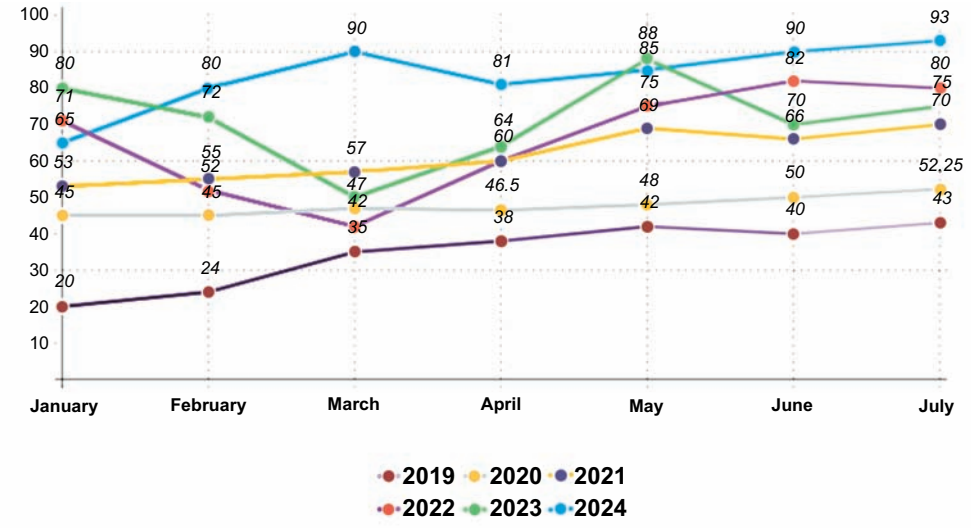


Fig. (2). Growth of blockchain.

Each application harnesses the blockchain's transparent, decentralized, and secure ledger to enhance operational efficiency, data integrity, and trust among stakeholders.

Application of Blockchain in Finance

Blockchain technology has significantly impacted the financial sector, offering solutions that enhance security, transparency, and efficiency in various financial processes. Blockchain's primary application in finance lies in cryptocurrencies, for instance, Ethereum and Bitcoin, which operate on decentralized networks secured by blockchain technology. Cryptocurrencies enable secure peer-to-peer

SUBJECT INDEX

I

K

L

M

N

O

P

Q

R

S

T

U

V

Y

Z

Sharmila Arunkumar

Dr. Sharmila Arunkumar holds a B.E. in Electronics and Communication Engineering from Annamalai University, an M.E. in Computer and Communication Engineering from Anna University, and a Ph.D. from Pondicherry University. With over 14 years of teaching experience, she is currently an Assistant Professor at Raj Kumar Goel Institute of Technology, Ghaziabad. Her research interests include Wireless Sensor Networks, Digital Image Processing, Cryptography, and Blockchain. She has authored/co-authored more than 40 research papers and five book chapters published by IET, Springer, and Elsevier. She also serves as an editor for books published by CRC Press, IGI Global, and Bentham Science.

Neha Goel

Dr. Neha Goel is working as a Professor in the Department of Electronics & Communication Engineering, RKGIT, Ghaziabad, India. She received her Ph.D. degree from SRM University, Chennai, in 2019. She has 19 years of rich experience in teaching, research, and development activities. Her areas of interest include VLSI design, CMOS design, the Internet of Things, and machine learning. She has guided several B.Tech and M.Tech projects, published 60 papers in various national and international journals and conferences, and has served as an editor for 4 books and contributed 10 book chapters in Scopus-indexed publications. She has also published four patents and attended numerous workshops and seminars in various fields.

R.K. Yadav

Dr. R. K. Yadav is a Professor and Head of the Electronics and Communication Engineering Department at RKGIT, Ghaziabad. He has more than 29 years of experience in teaching and research. His main areas of expertise include Microwave Engineering, Electromagnetic (EM) Waves, and Image Processing. He has published over 120 research papers in reputed national and international journals and conferences. He is also the author of a book on Microwave Engineering. Dr. Yadav is an active member of IEEE (a global professional body for engineers). He has successfully organized several international conferences in collaboration with IEEE and Elsevier. He also serves as an editor for a Springer journal and has worked as an editor for several books published by IGI Global, Nova Science Publishers, CRC Press, and others. He has guided eight Ph.D. candidates in various research areas such as Microwave Engineering, Image Processing, and Integrated Circuits.

Manoj Kumar

Dr. Manoj Kumar, Associate Professor at the University of Wollongong in Dubai, holds a Ph.D. from The Northcap University and an M.Sc. in Information Security from Technological University Dublin. With 12 years of experience in research, teaching, and industry, his expertise includes Cybersecurity, IoT, Digital Forensics, and Machine Learning. He has published over 115 research papers, two textbooks, and seven edited books. He has edited special issues for top publishers like Springer, Elsevier, and Taylor & Francis. He is a reviewer/editor for reputed journals and serves on technical committees. He has received several research awards and mentors Ph.D. candidates.

Shashi Bhushan

Dr. Shashi Bhushan, Ph.D. in Computer Science & Engineering, has over 15 years of experience in academia and research. He currently serves in the Department of Computer & Information Sciences at Universiti Teknologi PETRONAS, Malaysia. He has previously worked at institutions such as Amity University and UPES. His areas of interest include Wireless Sensor Networks, IoT, AI/ML, and Deep Learning. He has published over 50 research articles and books in reputed journals and conferences. He has chaired sessions and delivered talks at several international events and also serves as reviewer/editor for journals from publishers like Springer and Elsevier.