BLOCKCHAIN TECHNOLOGY FOR SECURE SOCIAL MEDIA COMPUTING

Edited by Robin Singh Bhadoria, Neetetsh Saxena, Bharti Nagpal, The Institute of Engineering and Technology, London, UK, published 2023, IET Security series 19, ISBN-13: 978-1-83953-543-7 (hardback), ISBN-13: 978-1-83953-544-4 (PDF), 265 pages.

Reviewers: Zoran S. Bojkovic and Bojan M. Bakmaz, University of Belgrade, Serbia

Blockchain can serve as a good foundation for applications based on transactions as well as interactions and can help to solve most of the security vulnerabilities together with traceability. It means that blockchain can act as a common platform for communication and interoperability among devices, enabling seamless data exchange. Blockchain technology has been applied in a variety of fields due to its capability of establishing trust in a decentralized platform. It has already established itself in developing various new complex decentralized software systems. Integrating blockchain (BC), artificial intelligence (AI), and Internet of Things (IoT) provides a promising new research and development direction together with capital investments. Each of these technologies is coming forward with new engineering challenges, e.g. understanding the requirements related to trust and ethics, system resilience towards unpredictable market behavior, or development of ultra-long-term software systems.

The primary reason for selecting this book to review is its unique way of explaining the concept of BC technology for secure social media computing which is sometimes difficult to understand. Thus, this book can help readers to bridge the gap between theory and practice, which are vital to the development of present-day BC technology in the area and can serve as a good foundation for applications based on transactions and interaction.

The book is structured in 13 chapters together with preface, forward, short bio of editors, further reading, and index. Each chapter is accompanied by the corresponding references. The chapters are categorized into 5 issues:

1. Social media computing security in mobile and wireless communication,
2. Authentication of the legitimacy of content in online social media (OSM),
3. BC-based decentralized online social networking,
4. BC as secure mediation for central knowledge graph through AI algorithms in IoT,
5. Next-generation computing of the era for better communication in social networks.

The first chapter discusses the ways of communicating with OSM which have received popularity by users. One of the reasons is the decentralization possibility, which is pointed out. BC technology as one of the most prominent for social programs with extended application in intelligent systems based on IoT, cloud, and social media insights is emphasized, too.

Chapter 2 presents BC-based security for social media computing which helps in the case of improvement payment with business-to-business marketplace. In that way, it is possible to have an investing role model in terms of guidelines and recommendations. Different fake news detection techniques have been discussed concerning authentication legitimacy of social network content such as style-based, knowledge-based, and propagation-based approaches.

Chapter 3 addresses emerging trends with social network design, models and handling. A list of different security threats with promising solutions due to the increasing cyber-crimes is provided. The various security perspectives are presented, together with the advanced and emerging trends. Future scope of this chapter can be extended toward healthcare, social engineering in terrorism, and other related activities.

Social networking including challenges, security issues, and emerging trends is offered in Chapter 4. Social networking platforms are a well-liked method of communication Internet users. They allow users to share news, pictures, ideas, and videos regardless of their location. Promising solutions for security issues are also discussed along with the challenges faced in numerous fields.

Going ahead, social media computing including tools and deployment platform for smart control are provided in Chapter 5. The solutions for BC social network are discussed, experimentally verified, and proved to have reasonable complexity. To protect privacy in the decentralized environment, the role of Ethernet Virtual machine can be utilized.

Next, Chapter 6 reviews the state-of-the-art for privacy provisioning on BC transactions of decentralized social media. Privacy provisioning solutions along with the challenges in this technology are presented. The solutions allow users to anonymize themselves in all types of digital transfer and regain control of their personal information.

BC-based knowledge graph for high-impact scientific collaboration networks is proposed in Chapter 7. The presented scenarios demonstrate a provisioning perspective when using the platform to assist interdisciplinary academic collaboration in different areas. The critical platforms based on the experts' experience, with various backgrounds, are identified. In that way, different aspects of BC technology and its role in handling issues and challenges using semantic technology and knowledge graph are identified. The application is in the domain of manufacturing and unmanned aerial vehicles in industry.

One step further, energy potential and challenges in 5G multimedia communication and BC technology are examined in Chapter 8. 5G applications have evolved significantly, including voice, video, wireless information access, and social interaction networks. As for BC, it helps establish secure multimedia communication among users and reduces transaction costs, providing at the same time, global accessibility for all users. Besides, the BC technology modifies the existing infrastructure, it transforms network domain. Many aspects of BC integration in 5G such as interoperability and standardization requirements, application and services, security and privacy, robustness and data integrity, resource allocation, energy efficiency, and management are analyzed.

The main goal of Chapter 9 is to point out IoT-based systems for intellectual property protection in social media using BC technology. To achieve this quality, advancements in an IoT environment are presented, together with the adoption of these two technologies. In the years to come, there will be an expectation that needs to be addressed, such as ensuring scalability, optimizing processing capabilities, and overcoming storage limitations associated with IoT devices in the BC system. Thus, the different trends with advancements in an IoT platform are demonstrated.

The BC architecture for social opinion vote system is analyzed in Chapter 10, together with fundamental concepts and its characteristics. Furthermore, it is discussed how an e-voting system can be designed using BC technology and at the same time being secure.

Chapter 11 opens the door for one of the fast-evolving technologies – BC, and its role in future applications, especially in smart areas. The structure of BC as well as creation of new blocks will be successfully represented for Industry 5.0 digital society.

Next, Chapter 12 covers the need for BC in social sectors, healthcare, industry as well as social media computing architecture. Also, it takes into consideration that BC is known for transparency, ensuring significant confidentiality, security and has scope to alleviate the capacities of social media computing. That's why patients, social groups, computing, healthcare providers and BC could be moved to the advanced level in the coming new era. It should be added that this chapter can help to extend the particular disease detection model and related medical contents.

Finally, Chapter 13 concludes all chapters with emerging trends in research directions and perspectives in the wide areas of different trends in security and framework for social media computing applying BC.

In conclusion, the book "Blockchain Technology for Secure Social Media Computing" edited by experts in the field addresses a number of topics through chapters written by researchers and academics who share their knowledge with readers considering the reason why customers demand the services from the point of strategic, business perspective as well as how market players are in a position to leverage competitive advantages to provide these services. At the end of the book, there is the recommendation for further reading which includes a review of implemented solutions that are the subject of scientific research which combine theory with practical use cases focused on the emerging BC technology for secure social media computing area. In that way, this book offers a good insight also for postgraduate and advanced undergraduate students giving a solid perspective for the analysis of current and future models as well as approaches to the final goal.