Blockchain and Industry 4.0 in Resilient Wireless Communications


Pradip Kumar Sharma


Abdelhakim Senhaji Hafid


Omer Rana


Rajarathnam Chandramouli


Shuping Peng

In the era of Industry 4.0, Internet of Things (IoT) technologies play an important and enabling role. IoT technologies support the capture (and increasingly processing) of data close to the point of data capture, and can be used as a basis to establish a sustainable model for cities and to preserve the quality of life of citizens. However, the implementation of Industry 4.0 still requires experimentation to evaluate potential economic impact and benefit. This stands particularly true in the face of data explosion, with faster data transfer rates across wireless communications (e.g., increasing availability of broadband, and 5G and beyond, 5G&B, networks) and the ability to support real-time decision making based on the collection and analysis of this data. Moreover, there is a need to transform the workforce, for example, integrating system operators with new skills to manage work digitally.

The transparency and auditability provided through the use of blockchain technologies enables us to address emerging challenges in Industry 4.0. Some of these challenges include the ability to provide:

- Greater "trust" in the data generated by an IoT device
- Greater understanding of operations and "behavior" of consumer devices

Blockchain technologies also enable new possibilities for trustworthy Industry 4.0 services in emerging wireless communications. For instance, using "smart contracts," workflow execution can be used to automate regulatory workflows. Monitoring, tracking, and reporting a large amount of heterogeneous data from smart cities, as well as verification and compliance checking could be facilitated through the efficient use of blockchain technologies.

Over the longer term, blockchain technologies also provide a solid foundation for next-generation computing ecosystems. Using these technologies, manufacturing industries could redefine and reshape their business models, providing greater trust in the use of remote management and monitoring capabilities. Cybersecurity challenges are other aspects that manufacturing industries require to create a robust and secure workflow in Industry 4.0. Meanwhile, emerging wireless communication networks are increasingly characterized by the integration of distributed and centralized computing and storage resources. The dramatic expansion of the bandwidth that makes wireless communication networks leads to new potential attack surfaces. Recent advances in wireless communications also raises serious concerns in terms of security and privacy with legacy solutions.

This Special Issue presents research that reflects recent advances in the use of blockchain technologies for Industry 4.0 in resilient wireless communications. We received a large number of submissions, four of which were accepted after a thorough review. The recent adaptation of artificial intelligence (AI) in Industry 4.0 is a key element in building resilient wireless communications. Collaborative learning is one of the key technologies, but it raises privacy concerns for sensitive industrial IoT data and "dishonest" computation. An article on a secure and trusted collaborative learning framework for AI IoT is included in this SI to address this challenge. The authors identify a number of security parameters to be recorded on a blockchain with each iterative round of model optimization. Along with the growing popularity of unmanned aerial vehicle (UAV) network applications, the accompanying communications security issue is also gradually gaining attention, due to its vital role in enabling resilient and reliable network performance.

An article on blockchain-based lightweight authentication scheme for resilient UAV communications in Industry 4.0 is the second in this SI. The authors discuss the potential of blockchain to facilitate resilient communications and propose a blockchain-based authentication architecture in UAV communications. For large-scale wireless networks, blockchain implementations often lead to scalability challenges, requring reliable real-time data interactivity and a fine-grained transaction support framework with high scalability. This SI accepted one article on a combinatorial blockchain architecture to enable scalable sharing economy systems. The authors conducted a proof-of-concept case study on electric vehicles sharing data to demonstrate feasibility. Blockchain implementations have brought maturity to consensus algorithms that seek to address failures within a blockchain network's validating nodes. However, failures in the creation, submission, and processing of transactions related to the operation of decentralized applications (DApps) running on an Industrial IoT device outside the core of the blockchain validating nodes have not yet been fully explored. Our fourth article overcomes the flaws in this context and describes measures to circumvent the impact that the failures can have on the functioning of smart contracts.

Acknowledgment

The Guest Editors would like to thank Professor Yi Qian, Editor-in-Chief of *IEEE Wireless Communications*, for allowing us to organize this Special Issue and the staff for their invaluable support throughout this issue. Special thanks to all the authors who submitted their valuable research works. In addition, we extend our thanks to the expert reviewers for their excellent assistance in reviewing the articles.

Biographies

Pradip Kumar Sharma [M'18, SM'21] (pradip.sharma@abdn.ac.uk) is an assistant professor of cybersecurity in the Department of Computing Science at the University of Aberdeen, United Kingdom. He received his Ph.D. in CSE (August 2019) from Seoul National University of Science and Technology, South Korea. He worked as a postdoctoral research fellow in the Department of Multimedia Engineering at Dongguk University, South Korea. His research interests are in the areas of cybersecurity, blockchain, edge computing, SDN, security and privacy in AI, and IoT security.

Abdelhakim Senhaji Hafid is a full professor at the University of Montreal. He is the founding director of the Network Research Lab and Montreal Blockchain Lab. He has extensive academic and industrial research experience in the area of communication networks and distributed systems. His current research interests include blockchain scalability and security, IoT, fog/edge computing, and intelligent transport systems.

Omer Rana is a professor of performance engineering in the School of Computer Science & Informatics, Cardiff University, United Kingdom. He holds a Ph.D. in neural computing and parallel architectures (Imperial College London), an M.Sc. in microelectronics (University of Southampton) and a B.Eng. in information systems engineering (Imperial College London).

Rajarathnam Chandramouli [M'00, SM'06] was with the faculty of the Department of Electrical and Computer Engineering, Iowa State University, Ames. He is currently a professor with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, New Jersey. His research interests include steganography, steganalysis, encryption, wireless networking, and applied probability theory. His research in these areas was sponsored by the National Science Foundation, the Air Force Research Laboratory, and industry. He was a recipient of the National Science Foundation CAREER Award. He was a Co-Founder and a Co-Program Chair of the IEEE International Workshop on Adaptive Wireless Networks in 2004 and 2005. He is also involved in several conference organizing committees. He has been an Associate Editor of *IEEE Transactions on Circuits and Systems for Video Technology* since 2000.

Shuping Peng [B.S.'05, Ph.D'10] (pengshuping@huawei.com) is a principal engineer and Datacom Standards representative at Huawei. She has extensive academic and industrial research experience in the area of communication networks. She is currently serving as IETF ART Area DISPATCH WG Co-Chair, RTG Area SPRING WG Secretary, RTG Area Directorate Member, and CCSA TC3WG2 (Network Devices and Protocols) Deputy Director. Her current interests include IPv6, SRv6, and APN6 (Application-aware IPv6 Networking).