IEEE IoT Journal Special Issue on

When Blockchain Meets 5/6G – Enabling Endogenously Secure IoT

The standardization of the fifth-generation (5G) communications has been completed, and the visioning and planning of the sixth generation (6G) communications have begun, with an objective of casting the high technical standard of new spectrum, high time and phase synchronization accuracy, and 100% geographical coverage to flexibly and efficiently connect upper trillion-level devices in future. The transition from 5G to 6G is expected to integrate all operational networks, especially the Internet of Things (IoT), which involves massive resource-constraint heterogeneous devices to interact with our physical world. As hundreds of attack vectors have been reported for IoT, security and privacy problems become obstacles to the further deployments and applications of 5/6G. Blockchain has been envisioned as a promising technology to improve efficiency, reduce cost, and mitigate security and privacy threats because of its ability to establish a trusted data sharing and computing environment. For example, FCC (Federal Communications Commission, U.S.) believes that blockchain will be a key technology for efficient and low-cost dynamic spectrum sharing in 6G. Therefore, it is worthy of exploring scalable and flexible space-air-ground integrated network architectures and integrated multi-level security considering the physical layer as well as higher layers in the 5/6G wireless networks, leveraging blockchain. Besides, incorporating smart contracts, artificial intelligence (AI), and other technologies would lead to security-enhanced, privacy-preserving, and smart data-driven 5/6G wireless networks and IoT applications, enabling a reassured and immersive user experience.

This special issue aims to seek high-quality papers regarding the integration of blockchain with 5/6G wireless networks, enabling Endogenously Secure IoT, to appeal and motivate researchers who are willing to incorporate blockchain and 5/6G and to pave the way of constructing secure IoT networks in the future. It solicits new theories and algorithms, architectures, methods, and applications that integrate blockchain, 5/6G, and IoT security. Topics include, but are not limited to:

- Blockchain architectures and protocols for 5/6G wireless network
- Blockchain-based trusted big data management, sharing and computing in IoT scenarios
- Endogenous security and blockchain-enabled defense mechanisms towards massive IoT devices.
- Dynamic spectrum sharing with blockchain and AI in 5/6G wireless networks
- Distributed consensus algorithms for 5/6G wireless networks
- Privacy preservation in blockchain-enabled IoT networks
- Blockchain-enabled crowdsourcing and other distributed services
- Blockchain empowered identity management, authentication and access control in super-dense 5/6G networks
- New opportunities, challenges, case studies, and applications for blockchain in 5/6G wireless networks
- Blockchain and quantum cryptography in space-air-ground integrated 6G networks
- Feasibility study of blockchain and 5/6G enabled IoT networks

Important Dates:

Submission Deadline:	July 1, 2021	Sec. Reviews Due/Notification:	Dec. 1, 2021
First Review Due:	Sep. 15, 2021	Final Manuscript Due:	Dec.15,2021
Revision Due:	Oct. 31, 2021	Publication Date:	2022

Submission Format and Guideline:

All original manuscripts or revisions to the IEEE IoT Journal must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Author guidelines and submission information can be found at http://ieee-iotj.org/guidelines-for-authors/.

Guest Editors:

Dongxiao Yu, Shandong University
Qingdao, P. R. China
Email: dxyu@sdu.edu.cn
Qing Yang
University of North Texas, USA
Email: qing.yang@unt.edu
Madhuri Siddula
North Carolina A&T State University
Greensboro, USA
Email: msiddula@ncat.edu
Jian Ren
Michigan State University, USA
Email: renjian@msu.edu
Sasu Tarkoma
University of Helsinki, Finland
Email: sasu.tarkoma@helsinki.fi
Falko Dressler
TU Berlin
Berlin, Germany
Email: dressler@ccs-labs.org