

Smart Blockchain for IoT Trust, Security and Privacy

The fast development of the Internet of Things (IoT) involves enormous evolutions of IoT empowered smart systems and applications, using diverse networks, remote sensors and endpoint appliances. However, these IoT smart devices may easily receive massive cyber-attacks, facing threats related to trust, security and privacy (TSP) of the IoT data. The blockchain technology, representing a decentralized, distributed, shared, and immutable database ledger that stores registry of assets, provides a potential solution for the IoT TSP, especially when dealing with large-scale of heterogeneous data that are collected via smart sensors/devices, distributed via communication networks and usually processed in real-time. Over the past few years, smart blockchain technology has emerged as an area of incredible impact, potential, and growth, with both the powers from AI and blockchain, ensuring a secure environment for IoT data communication, computation and storage, for addressing the IoT TSP issues in both academic and industrial fields.

Smart blockchain extends traditional blockchain technologies with cutting-edge artificial intelligence (AI), offering high-level economy, adaptivity and autonomy to a blockchain system. Compared with traditional blockchain techniques, smart blockchain brings extra features to blockchain systems through data mining, pattern recognition, machine learning and deep learning on the top of existing blockchain technologies, which show a great potential to benefit the modern IoT systems. Recently, tremendous efforts have been made to explore smart blockchain technologies for solving IoT TSP issues, related to different application fields including cyber security, smart city, smart grid, wireless sensor networks, mobile communications, crowdsourcing/crowdsensing, cyber-physical-social systems, and so on. However, there are still open research problems and challenges for smart blockchain empowered TSP of IoT: 1) What are the key requirements of TSP in smart blockchain solutions toward modern IoT systems? 2) What are the key algorithms in smart blockchain platforms for IoT TSP? And 3) How to realize key applications of smart blockchain with TSP concerns in diversified IoT environments?

This special issue on Smart Blockchain for IoT Trust, Security and Privacy solicits topics as follows, but not limited to:

- Smart blockchain theories and algorithms for IoT trust, security and privacy
- Trustworthy IoT data management with smart blockchain
- AI-based data analytics for blockchain intelligence
- Machine/deep learning for blockchain intelligence
- Secure IoT system design based on smart blockchain
- Trust, security and privacy of smart blockchain
- Decentralized and collaborative learning for IoT
- Decentralized computing for IoT trust, security and privacy
- End-edge-cloud computing enabled by smart blockchain in IoT
- Big data analytics based on blockchain in IoT systems
- Performance optimization of blockchains in IoT
- Blockchain related applications for intelligent IoT trust, security and privacy

Important Dates:

Submission Deadline:	November 15, 2022
First Review Due:	December 30, 2022
Revision Due:	January 31, 2023
Sec. Reviews Due/Notification:	March 15, 2023
Final Manuscript Due:	April 15, 2023
Publication Date:	2023

Guest Editors:

Xiaokang Zhou (zhou@biwako.shiga-u.ac.jp), Shiga University, Japan
Zheng Yan (zyan@xidian.edu.cn), Xidian University, China and Aalto University, Finland
Yan Zhang (yanzhang@ieee.org), University of Oslo, Norway
Stephen Yau (yau@asu.edu), Arizona State University, USA