

Guest Editorial: Blockchain Solutions for Industrial Internet of Things

THERE is a growing trend of adopting blockchain technologies to the industrial Internet of Things (IIoT) due to the traceability, nonrepudiation, and immutability of blockchain systems. The proliferation of IIoT to industrial systems is fostering the fourth industrial revolution (aka Industry 4.0) while IIoT also confronts several challenges exhibiting in the following two perspectives: 1) security and privacy protection of IIoT data; 2) interoperability absence across IIoT systems. Blockchain and blockchain-enabled smart contracts can essentially offer solutions to address the emerging challenges in IIoT.

The objective of this special section in IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS is to explore the state-of-the-art advances in adopting blockchain technologies for IIoT. We have received nearly 50 submissions for this SS, among which seven submissions have been ultimately accepted. Each accepted manuscript has gone through a rigorous peer-review process and finally been accepted after another round of review after revision (some of them have experienced two rounds of reviews). We then briefly summarize these accepted articles as follows.

The first paper proposes a blockchain-based key management scheme for a heterogeneous flying ad-hoc network (FANET). FANET consists of multiple unmanned aerial vehicles (UAVs), which communicate with each other to conduct diverse industrial tasks. However, the traditional key management of FANET heavily relies on infrastructure nodes, thereby increasing the communication overheads. Therefore, the proposed blockchain-based key management scheme can effectively address this issue. As an important issue, IIoT data management has received extensive attention recently. However, it is challenging to achieve a fair data-packing scheme in permissioned blockchain for IIoT. Thus, the second paper presents a fairness-based transaction packing approach for permissioned blockchain. Both theoretical analysis and extensive experiments have validated the effectiveness of the proposed scheme. The third paper presents a many-objective optimization algorithm based on the sharding scheme to enhance the security of blockchain-enabled IIoT. Extensive experiments verify the effectiveness of the proposed scheme.

It is a critical issue to protect data privacy while fulfilling the growth of data-sharing demands in IIoT systems. To address this issue, the fourth paper proposes two blockchain-based data publishing protocols for both histogram publishing and

anonymized data publishing. The proposed schemes can achieve the fairness and auditability of shared data. The fifth paper presents a blockchain-based access control scheme for effective data sharing across factories. In particular, this scheme can achieve the traceability of industrial data and revocability of users. Extensive experiments also validate the effectiveness of the proposed scheme. Despite the strengths of blockchain, the scalability of blockchain systems has been a major obstacle before the real adoption of blockchain for IIoT. The sixth paper presents a dynamic proof of work integrated with the block-checkpoint mechanism to address the scalability issue. Both theoretical analysis and experiments demonstrate the effectiveness of the proposed protocol. Massive smart grid data brings huge values while also posing security and privacy concerns when sharing customers' private data. To address this issue, the seventh paper presents a blockchain-based framework for auditable data-sharing services in smart grid. Experiments also demonstrate the effectiveness of the proposed scheme.

In summary, the articles included in this special section exhibit the latest advances in blockchain for the industrial Internet of things. We would like to thank all the authors who submitted their work to this special section. We also would like to express our appreciation to the reviewers who voluntarily participated in the review process. Last but not least, we want to give our deep thanks to the Editor-in-Chief, Professor Ren Luo, for providing us with this opportunity and tremendous guidance during the entire process.

YAN ZHANG, *Guest Editor*
University of Oslo, 0315 Oslo, Norway
yanzhang@ieee.org

ZIBIN ZHENG, *Guest Editor*
Sun Yat-Sen University, Guangdong 510120,
China
zhzibin@mail.sysu.edu.cn

HONG-NING DAI, *Guest Editor*
Macau University of Science and
Technology, Taipa 999078, Macau
hndai@ieee.org