Guest Editorial Special Issue on Blockchain-Enabled Internet of Things

BLOCKCHAIN, as a constantly evolving Peer-to-Peer (P2P) distributed ledger technology with characteristics, such as decentralization, security, interoperation, and trust establishment, can potentially lower the costs of the underpinning infrastructure and maintenance compared with conventional centralized systems. Consequently, the distributed structure of blockchain is naturally suitable for the Internet of Things (IoT), which can be used to build secure and trusted IoT. Despite the advances made in applying blockchain to IoT in the past few years, some research challenges remain to be addressed, including the poor scalability, heterogeneous IoT devices, and the impact of integration on network performance.

The response to our call for this special issue was overwhelming, as we received in total 99 submissions from around the world. During the review process, each article was assigned to and reviewed by at least three experts in the field, with a rigorous multiround review process. Thanks to the great support from the current Editor-in-Chief, Prof. Honggang Wang, and the dedicated work of numerous reviewers, we were able to accept 25 excellent articles covering various topics in blockchain-enabled IoT. In the following, we will introduce these articles and highlight their main contributions.

Article [A1] proposes to introduce blockchain into the FL framework to resist the malicious attacks that occurred in D2D caching networks. Furthermore, a double-layer blockchain-based deep reinforcement FL (BDRFL) scheme is designed to ensure privacy-preserved and caching-efficient D2D networks.

Chatzopoulos *et al.* [A2] introduced and analyzed Mneme, a DAG-based distributed ledger that can be maintained solely by mobile devices. Then, the authors analyze Mneme's security and justify the ability of Proof-of-Context (PoC) and Proof-of-Equivalence (PoE) to guarantee the characteristics of distributed ledgers: persistence and liveness. Furthermore, the authors prove that the probability of a successful attack is inversely proportional to the square of the number of mobile users who maintain Mneme.

Cheng *et al.* [A3] provided a trusted resource allocation mechanism based on smart contracts to effectively address the problems existing in resources pricing and service quality evaluation of edge servers. Furthermore, the proposed mechanism allows end users to choose a purchase mode in terms of actual demands on delay and price, while smart contracts can match end users with high-reputation edge servers automatically.

Lee *et al.* [A4] carefully addressed the co-design problem of communication and consensus, aiming to obtain a fast and scalable distributed wireless consensus mechanism with high resiliency against faulty nodes in the network. In addition, the authors propose two wireless consensus mechanisms that suit in large-scale wireless networks.

Article [A5] proposes a round-based two-stage blockchain consensus protocol called Proof of Transactions (PoT). The theoretical analysis and experimental verification of the proposed PoT protocol are conducted to illustrate the feasibility and superiority of PoT.

Du *et al.* [A6] analyzed IoT private chain systems and found that the leader maintains too many connections due to high latency and client request frequency, which results in lower consensus performance and efficiency. To this end, this article proposes a novel solution for maintaining low request latency and high transactions per second (TPS): replicate nontransactional data by followers and confirm by the leader to achieve nonconfliction state-machine replication (SMR).

Article [A7] proposes a new smart contract architecture and optimization mechanism for blockchain-based IoT. In addition, the authors propose a template-based light-weighted bytecode construction mechanism that only involves application requirement parsing and template assembling rather than a compilation.

Article [A8] designs a decentralized identity management framework capable of storing, protecting, and processing the constructed identity shares generated from the verifiable credentials. In addition, authentication and integrity-check mechanism are designed for externally stored identity shares.

He *et al.* [A9] proposed a multichain charging model that stores different types of information on different blockchains. To calculate reputation across chains, this article designs a cross-chain trusted smart contract to ensure the authenticity, real time, and interchain write mutual exclusion of cross-chain information.

Article [A10] studies the impact of mobility on block propagation under the single-chain structure in vehicular ad-hoc networks (VANET). In this article, the authors derive the closed-form expression of the single-block propagation time and characterize the blockchain forking as the multiblock competitive propagation. In this way, an approximate result on multiblock propagation time is discussed.

Zhang *et al.* [A11] proposed a directed acyclic graph (DAG) blockchain-enhanced user-autonomy spectrum sharing model. In the model, a dynamic tip selection method is designed to

Digital Object Identifier 10.1109/JIOT.2022.3162972

2327-4662 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

enhance the global utility, which is related to the spectrum of supply–demand.

Li *et al.* [A12] introduced a novel verifiable computing protocol, called EntrapNet, which borrows the idea from the practice of criminal entrapment. To solve the verifiable computing problem, the formulated objective is to optimize the tradeoff between security and efficiency.

Article [A13] proposes a distributed mobile edge network to sufficiently exploit advantages of blockchain and differential privacy to collect trustworthy data and protect privacy for data collectors. Furthermore, a new consensus mechanism is designed for a blockchain-based data collection structure.

Ling *et al.* [A14] proposed a Hash Access for blockchain radio access network (B-RAN) to address the trust issue between clients, aims to enforce client devices to obey the grant-free access rule. Based on the Hash Access, the authors formulate the Rogue's Dilemma from a game-theoretic model to emphasize the necessity of Hash Access.

Article [A15] proposes a deep deterministic policy gradient (DDPG)-based scheme to tackle the joint resource allocation and replica selection challenge of VR streaming in blockchain-enabled fog radio access networks (F-RANs). The proposed scheme balances the load on virtual reality streaming and blockchain maintenance.

Yang *et al.* [A16] established a multidomain vehicular authentication architecture by introducing a blockchain technique. To guarantee anonymity and traceability, a pseudonym-based privacy-preserving authentication method is proposed.

Article [A17] presents a triple subject purpose-based access control (TS-PBAC) model. Furthermore, a blockchain-enabled security and privacy-preserving data publishing and sharing prototype is proposed.

Luo *et al.* [A18] proposed a Vehicle-to-Vehicle (V2V) and Vehicle-to-Grid (V2G) electricity trading architecture based on blockchain. Then, the authors introduce a two-way auction mechanism based on the Bayesian game and design a new price adjustment strategy.

Article [A19] deploys a blockchain in communication-based train control systems. With an aim to minimize the impact of the key updating process on communication based train control (CBTC) system performance and keep the system secure, the authors formulate the block producer selection and onboard blockchain client handoff decision problem using the deep reinforcement learning approach.

Wang *et al.* [A20] developed a blockchain-enabled fish provenance and quality tracking (BeFAQT) system. A multilayer blockchain architecture based on attribute-based encryption (ABE) is proposed to tackle the privacy issue caused by applying blockchain to secure supply chain data.

Article [A21] adopts blockchain to build a multicenter data management framework. In addition, an ABE algorithm is designed for the multicenter scenarios, and the obfuscating policy is proposed to shift encryption computations to the cloud.

Yu *et al.* [A22] proposed a Shamir threshold cryptography scheme for Industrial Internet of Things (IIoT) data protection using blockchain. In this context, the edge gateway uses a symmetric key to encrypt the data uploaded by the IoT device and store it in the cloud.

Article [A23] proposes an optimal blockchain deployment mechanism for wireless IoT systems to improve the storage efficiency of massive blockchain data. Through dynamically adjusting optimal block assignment, the tradeoff between the length of the blockchain to be stored and the security level can be well made.

Zhang *et al.* [A24] proposed a blockchain-based performance-security balanced safety inspection framework (PSB-SIF). In this framework, a safety inspection box is designed to ensure the authenticity of the inspector's identity while inspection logic is executed automatically via smart contracts.

Article [A25] proposes to analyze the user association problem, computation offloading problem, and block storage problem in the blockchain-enabled HetNet. The analysis shows that the proposed blockchain-enabled HetNet can greatly avoid data congestion of BSs.

We would like to express our sincere thanks to all the authors for submitting their papers and to the reviewers for their valuable comments and suggestions that significantly enhanced the quality of these articles. We are also grateful to Prof. H. Wang, the current Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL, for his great support throughout the whole review and publication process of this special issue, and, of course, all the editorial staff. We hope that this special issue will serve as a useful reference for researchers, scientists, engineers, and academics in the field of blockchain-enabled Internet of Things.

BIN CAO, *Guest Editor*
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing 100876, China

LEI ZHANG, *Guest Editor*
School of Engineering
University of Glasgow
Glasgow G12 8QQ, U.K.

TONY Q. S. QUEK, *Guest Editor*
Singapore University of Technology and Design
Singapore 487372

SICHAO YANG, *Guest Editor*
Nakamoto & Turing Labs
New York, NY 10036 USA

APPENDIX: RELATED ARTICLES

[A1] R. Cheng, Y. Sun, Y. Liu, L. Xia, D. Feng, and M. Imran, "Blockchain-empowered federated learning approach for an intelligent and reliable D2D caching scheme," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7879–7890, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3103107.

[A2] D. Chatzopoulos, A. Jain, S. Gujar, B. Faltings, and P. Hui, "Towards mobile distributed ledgers," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7891–7903, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3113730.

[A3] H. Cheng, Q. Hu, X. Zhang, Z. Yu, Y. Yang, and N. Xiong, "Trusted resource allocation based on smart contracts for blockchain-enabled Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7904–7915, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3114438.

[A4] H. Lee, H. Seo, and W. Choi, "Fast and scalable distributed consensus over wireless large-scale Internet-of-Things network," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7916–7930, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3118928.

[A5] Z. Ai and W. Cui, "A proof-of-transactions blockchain consensus protocol for large-scale IoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7931–7943, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3108627.

[A6] H. Du, D. Zhu, Y. Sun, and Z. Tian, "Leader confirmation replication for millisecond consensus in private chains," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7944–7958, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3113835.

[A7] T. Li, Y. Fang, Z. Jian, X. Xie, Y. Lu, and G. Wang, "ATOM: Architectural support and optimization mechanism for smart contract fast update and execution in blockchain-based IoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7959–7971, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3106942.

[A8] E. Samir, H. Wu, M. Azab, C. S. Xin, and Q. Zhang, "DT-SSIM: A decentralized trustworthy self-sovereign identity management framework," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7972–7988, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3112537.

[A9] Y. He, C. Zhang, B. Wu, Y. Yang, K. Xiao, and H. Li, "A cross-chain trusted reputation scheme for a shared charging platform based on blockchain," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7989–8000, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3099898.

[A10] X. Zhang *et al.*, "The block propagation in blockchainbased vehicular networks," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8001–8011, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3074924.

[A11] H. Zhang, S. Leng, F. Wu, and H. Chai, "A DAG blockchain enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8012–8023, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3109959.

[A12] C. Li, L. Zhang, and S. Fang, "EntrapNet: A blockchain-based verification protocol for trustless computing," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8024–8035, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3124007.

[A13] T. Li *et al.*, "BPT: A blockchain-based privacy information preserving system for trust data collection over distributed mobile edge network," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8036–8052, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3117971.

[A14] X. Ling, B. Zhang, H. Xie, J. Wang, and Z. Ding, "Hash access in blockchain radio access networks: Characterization and optimization," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8053–8066, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3111915.

[A15] Y. Liu, Q. Chang, M. Peng, T. Dang, and W. Xiong "Virtual reality streaming in blockchain enabled fog radio access networks," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8067–8077, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3111115.

[A16] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A blockchain-based multi-domain authentication scheme for conditional privacy preserving in vehicular ad-hoc network," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8078–8090, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3107443.

[A17] S. Wang, G. Wu, Z. Ning, and J. Li, "Blockchain enabled privacy preserving access control for data publishing and sharing in the Internet of Medical Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8091–8104, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3138104.

[A18] L. Luo, J. Feng, H. Yu, and G. Sun, "Blockchain-enabled two-way auction mechanism for electricity trading in Internet of electric vehicles," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8105–8118, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3082769.

[A19] L. Zhu, H. Liang, H. Wang, B. Ning, and T. Tang, "Joint security and train control design in blockchain empowered CBTC system," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8119–8129, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3097156.

[A20] X. Wang *et al.*, "Blockchain-enabled fish provenance and quality tracking system," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8130–8142, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3109313.

[A21] X. Wei, Y. Yan, S. Guo, X. Qiu, and F. Qi, "Secure data sharing: Blockchain enabled data access control framework for IoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8143–8153, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3111012.

[A22] K. Yu *et al.*, "A Blockchain-based Shamir's threshold cryptography scheme for data protection in Industrial Internet of Things settings," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8154–8167, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3125190.

[A23] J. Zhou, G. Feng, and Y. Wang, "Optimal deployment mechanism of blockchain in resource-constrained IoT systems," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8168–8177, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3106355.

[A24] W. Zhang *et al.*, "A trustable safety inspection framework using performance-security balanced blockchain," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8178–8190, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3121512.

[A25] Y. Zuo, S. Jin, and S. Zhang, "Blockchain storage, computation offloading, and user association for heterogeneous cellular networks," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8191–8204, Jun. 1, 2022, doi: 10.1109/JIOT.2021.3113366.