Guest Editorial Special Issue on When Blockchain Meets 5G/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 the future. The transition from 5G to 6G is expected to integrate all operational networks, especially the Internet of Things (IoT), which involves massive 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 5G/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, Federal Communications Commission (FCC, 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 multilevel security considering the physical layer as well as higher layers in the 5G/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 5G/6G wireless networks and IoT applications, enabling a reassured and immersive user experience.

The response to our call for papers for this special issue was overwhelming, as we received in total 60 submissions from all over the world. During our rigorous multiround review process, we assigned to each article at least three domain experts to ensure that each paper receives at least three professional reviews at each round. Thanks to the great support from the former Editor-in-Chief, Prof. Honggang Wang, the current Editor-in-Chief, Prof. Nei Kato, and the numerous dedicated reviewers, we were able to accept 16 excellent articles covering various topics in the integration of blockchain with 5G/6G wireless networks, enabling Endogenously Secure IoT. In the following, we briefly introduce these articles and highlight their main contributions.

Shao et al. [A1] presented a trusted framework based on blockchain technology by building a trusted software-defined content delivery network. With the insightful studies on trusted communication based on routing sandbox, service choreography based on blockchain, proxy server selection strategy based on model predictive control, and optimization consensus based on PBFT, this paper enhanced the security of network communications and established trust relationships between entities.

Xu et al. [A2] proposed a blockchain-based certificateless signcryption mechanism suitable for edge computing, which can make good use of the nontamperable feature of blockchain, prevent illegal users from substituting public key of the user, and guarantee signature nonrepudiation. Theoretical analysis and comparisons with eight schemes were given to prove the security and effectiveness of the proposed mechanism.

Diao et al. [A3] presented new multistage session key negotiation protocols for the IoT–blockchain environment by using "agents." By transferring bilinear operations to agents with strong computing capabilities, the resource of IoT devices in the key negotiation process can be reduced and more secure. The simplified BPR model and the random oracle model ID-BJM were used to test the security of requirements in different stages of the scheme.

Zhang et al. [A4] introduced a novel communication data management model based on blockchain technology, in which an "IoT ledger," a kind of blockchain-structured distributed database, was proposed to solve the problem of data reliability, scalability, and would not involve high operating costs.

Hu et al. [A5] proposed a novel mobile crowdsensing (MCS) learning framework leveraging on blockchain technology and the new concept of edge intelligence based on federated learning. Four main procedures, including task publication, data sensing and submission, learning to return final results, and payment settlement and allocation, were designed to address the major challenges in MCS, such as malicious edge servers and dishonest requestors.

Zhang et al. [A6] proposed a smart contract-based quality-driven incentive mechanism, to address the problem of secure data sharing despite the limited computing resources of IoT devices. Focusing on the AI solution vendors to obtain a wide range of IoT device data, an automatic pulling computing architecture was designed for a wide range of limited-resource devices with multiple participants. Based on the proposed scheme, sustainable incentives for user participation and high-quality data sharing can be achieved.

Digital Object Identifier 10.1109/JIOT.2023.3275289

Le et al. [A7] developed a six-layer architecture that incorporated a number of novel features, such as enhanced blockchain structures, secure interaction methods, efficient service mechanisms, and scalable transaction patterns, to establish a unified architecture with enhanced efficiency, security, compatibility, and flexibility for resource sharing and trading in blockchain radio access network. Multiple experiments were presented to verify the performance of the proposed architecture.

Yang et al. [A8] proposed a trust management model enabled by blockchain to ensure the traceability, nontampering, unforgeability, and transparency of vehicular interactions. The proposed model leveraged Dirichlet distribution, reputation regression, and revocation punishment to objectively and accurately reflect the trust status of vehicles.

Fu et al. [A9] presented an efficient and fault-tolerant blockchain consensus transform mechanism for IoT. Two consensus algorithms, namely, detectable RAFT (DRAFT) and double-layer parallel BFT (DPBFT), were designed to improve the efficiency and fault tolerance of the data sharing process in IoT.

Zhang et al. [A10] designed a federated learning trust supervision mechanism toward data sharing to restrict node behavior and guarantee the healthy operation of the data sharing system. A blockchain and federated learning-based data sharing architecture was designed to realize data value transmission and user privacy protection at the same time.

Dai et al. [A11] presented a blockchain-enabled edge resource sharing (BEERS) architecture to provide a trusted IoT resource collaboration environment to realize the trusted sharing of IoT edge resources. Based on this architecture and considering typical edge resource collaboration scenarios, the resource scheduling and task assignment problems were studied.

Li et al. [A12] proposed a privacy protection data retrieval scheme with an inverted index, termed as inverted index-based attribute-based keyword search (IABKS) scheme, to solve the data sharing problem in a blockchain network of IoT devices. The features of privacy, multikeyword ranked search, efficiency, and practicality were obtained in the proposed scheme.

Zou et al. [A13] considered how to reach blockchain consensus in wireless networks without reliable network support. Based on a physical interference communication model, a distributed and randomized consensus algorithm was proposed to reach k-times consensus among n agents within $O(k + \log n)$ time steps with high probability, which is an asymptotically optimal result in terms of time complexity.

Chen et al. [A14] proposed a data sharing privacy protection model (DS2PM) based on blockchain and a federated learning mechanism, to solve the data privacy problem, the storage burden problem, and the problem of low fairness and low efficiency in the consensus mechanism. The safety analysis and experimental results showed that the DS2PM outperformed the previously established schemes.

He et al. [A15] investigated a multichain 5G network slicing service quality computing model to calculate the service quality parameters of the network slicing. A smart contract on each blockchain was designed to reduce the frequency of information transmission and improve efficiency. To ensure the cross-chain security calculation, the signature by Cosi protocol and multisigncryption algorithms were used.

Li et al. [A16] proposed a double-layer blockchain and decentralized identifiers-assisted secure registration and authentication mechanism for decentralized VANETs. In this mechanism, a double-layer blockchain, a decentralized identifier technology, and a reputation feedback mechanism were adopted to improve the security and efficiency of the authentication and message verification process.

We would like to express our sincere thanks to all the authors for submitting their papers and all the reviewers for their valuable comments and suggestions that significantly helped to enhance the quality of the articles. We are also grateful to Prof. H. Wang, the former Editor-in-Chief, and Prof. N. Kato, the current Editor-in-Chief, of the IEEE INTERNET OF THINGS JOURNAL, for their great support throughout the whole review and publication process of this special issue. Our special thanks go to all the editorial staff for their timely and professional services. We expect that this special issue can serve as a useful reference for researchers, scientists, engineers, and academics in the field of blockchain with 5G/6G wireless networks for Endogenously Secure IoT.

APPENDIX: RELATED ARTICLES

[A1] S. Shao, W. Gong, H. Yang, S. Guo, L. Chen, and A. Xiong, "Data trusted sharing delivery: A blockchain assisted software-defined content delivery network," *IEEE Internet Things J.*, early access, Oct. 29, 2021, doi: 10.1109/JIOT.2021.3124091.

[A2] G. Xu, J. Dong, C. Ma, J. Liu, and U. G. O. Cliff, "A certificateless signcryption mechanism based on blockchain for edge computing," *IEEE Internet Things J.*, early access, Feb. 15, 2022, doi: 10.1109/JIOT.2022.3151359.

[A3] Z. Diao, Q. Wang, and B. Gong, "MSKNP: Multi-stage key negotiation protocol for IoT-blockchain environment," *IEEE Internet Things J.*, early access, Jan. 4, 2022, doi: 10.1109/JIOT.2021.3140128.

[A4] H. Zhang, X. Zhang, Z. Guo, H. Wang, D. Cui, and Q. Wen, "Secure and efficiently searchable IoT communication data management model: Using blockchain as a new tool," *IEEE Internet Things J.*, early access, Oct. 20, 2021, doi: 10.1109/JIOT.2021.3121482.

[A5] Q. Hu, Z. Wang, M. Xu, and X. Cheng, "Blockchain and federated edge learning for privacy-preserving mobile crowdsensing," *IEEE Internet Things J.*, early access, Nov. 16, 2021, doi: 10.1109/JIOT.2021.3128155.

[A6] C. Zhang, T. Shen, and F. Bai, "Toward secure data sharing for the IoT devices with limited resources: A smart contractbased quality-driven incentive mechanism," *IEEE Internet Things J.*, early access, Jan. 13, 2022, doi: 10.1109/JIOT.2022.3142786.

[A7] Y. Le et al., "Resource sharing and trading of blockchain radio access networks: Architecture and prototype design," *IEEE Internet Things J.*, early access, Dec. 14, 2021, doi: 10.1109/JIOT.2021.3135414.

[A8] Z. Yang, R. Wang, D. Wu, B. Yang, and P. Zhang, "Blockchain-enabled trust management model for the Internet of Vehicles," *IEEE Internet Things J.*, early access, Oct. 29, 2021, doi: 10.1109/JIOT.2021.3124073.

[A9] J. Fu, L. Zhang, L. Wang, and F. Li, "BCT: An efficient and fault tolerance blockchain consensus transform mechanism for IoT," *IEEE Internet Things J.*, early access, Oct. 28, 2021, doi: 10.1109/JIOT.2021.3123626.

[A10] F. Zhang, S. Guo, X. Qiu, S. Xu, F. Qi, and Z. Wang, "Federated learning meets blockchain: State channel based distributed data sharing trust supervision mechanism," *IEEE Internet Things J.*, early access, Nov. 23, 2021, doi: 10.1109/JIOT.2021.3130116.

[A11] M. Dai, S. Xu, Z. Wang, H. Ma, and X. Qiu, "Edge trusted sharing: Task-driven decentralized resources collaborate in IoT," *IEEE Internet Things J.*, early access, Oct. 27, 2021, doi: 10.1109/JIOT.2021.3123333.

[A12] W. Li, Y. Chen, F. Gao, S. Zhang, H. Zhang, and Q. Wen, "Privacy protection data retrieval scheme with inverted index for IoT based on blockchain," *IEEE Internet Things J.*, early access, Nov. 16, 2021, doi: 10.1109/JIOT.2021.3128528.

[A13] Y. Zou, M. Xu, J. Yu, F. Zhao, and X. Cheng, "A fast consensus for permissioned wireless blockchains," *IEEE Internet Things J.*, early access, Oct. 29, 2021, doi: 10.1109/JIOT.2021.3124022.

[A14] Y. Chen et al., "DS2PM:A data sharing privacy protection model based on blockchain and federated learning," *IEEE Internet Things J.*, early access, Dec. 13, 2021, doi: 10.1109/JIOT.2021.3134755.

[A15] Y. He, C. Zhang, B. Wu, Y. Yang, K. Xiao, and H. Li, "Cross-chain trusted service quality computing scheme for multi-chain model-based 5G network slicing SLA," *IEEE Internet Things J.*, early access, Dec. 3, 2021, doi: 10.1109/JIOT.2021.3132388.

[A16] X. Li, T. Jing, R. Li, H. Li, X. Wang, and D. Shen, "BDRA: Blockchain and decentralized identifiers assisted secure registration and authentication for VANETs," *IEEE Internet Things J.*, early access, Apr. 1, 2022, doi: 10.1109/JIOT.2022.3164147.

DONGXIAO YU, *Guest Editor*
School of Computer Science and Technology
Shandong University
Qingdao 266237, China

JIAN REN, *Guest Editor*
Department of Electrical & Computer Engineering
Michigan State University
East Lansing, MI 48824 USA

QING YANG, *Guest Editor*
Department of Computer Science and Engineering
University of North Texas
Denton, TX 76205 USA

SASU TARKOMA, *Guest Editor*
Department of Computer Science
University of Helsinki
00100 Helsinki, Finland

MADHURI SIDDULA, *Guest Editor*
Department of Computer Science
North Carolina A&T State University
Greensboro, NC 27411 USA

FALKO DRESSLER, *Guest Editor*
School of Electrical Engineering and Computer Science
TU Berlin
10587 Berlin, Germany