Guest Editorial
Introduction to the Special Section on Blockchain in Future Networks and Vertical Industries

BLOCKCHAIN has been successfully applied into a number of sectors, including finance, energy, logistics and supply chains, due to its ability of creating a tamper-proof digital ledger of transactions and the resulting novel trust mechanisms [1]. Future networks will be heterogeneous, connecting together satellite, 5G, the Internet, marine networks, and so on; security and trust management is a major issue in such kind of integrated converged networks [2]. Blockchain technology is a promising solution to achieve the desired level of security and trust in future networks, e.g., reliable network data collection [3] and network trust evaluation [4]. However, the application of blockchain technology in 5G, vertical industries and future heterogeneous networks is still in its infancy. Many challenging issues need to be resolved before its application can be deployed in real-world networking environments.

The special section on Blockchain in Future Networks and Vertical Industries is focused on the state-of-the-art blockchain based solutions for future networks and vertical industries. After a rigorous review process, we were able to accept 11 contributed articles (out of 34 articles submitted) covering several important topics. A brief review follows:

As 5G becomes the technology of choice by governments and telecommunication providers around the world, there is a need to support features such as authentication handover and user privacy protection. In "Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based 5G Networks," Yazdinejad *et al.* propose a novel blockchain-based authentication approach that utilizes software defined networking (SDN) techniques to avoid the need for re-authentication in repeated handover among heterogeneous cells. Such an approach can minimize delay, including when users are moving and communicating across heterogeneous networks in a privacy-preserving manner. They then evaluated and demonstrated that the delay of the authentication handover in their approach is less than 1ms, and considerably less than other Proof-of-Work (POW)-based and network-based models. Their approach also incurs less signaling overhead and energy consumption compared to other competing models.

A very large number of smart contracts has been deployed on Ethereum. Meanwhile, security flaws of contracts have led to huge pecuniary losses and destroyed the ecological stability of contract layer on Blockchain. It is thus an emerging yet crucial issue to effectively and efficiently detect vulnerabilities in smart contracts. In "ContractWard: Automated Vulnerability Detection Models for Ethereum Smart Contracts," Wang *et al.* propose an automated tool, namely ContractWard, to detect vulnerabilities in smart contracts. It extracts bigram features from simplified operation codes of smart contracts. Five machine learning algorithms and two sampling algorithms are then employed to build the detection models. ContractWard is evaluated with 49502 real-world smart contracts running on Ethereum. The experimental results demonstrate the effectiveness and efficiency of ContractWard. The predictive Micro-F1 and Macro-F1 of ContractWard are over 96% and the average detection time is 4 seconds on each smart contract with XGBoost for training the models and SMOTETomek for balancing the training sets.

In the big data environment, the heavily fragmented distribution of the Quality of Services (QoS) data for recommendation decision-making presents a large challenge when integrating the QoS data from different platforms while ensuring that the sensitive user information contained in the QoS data is secure. Furthermore, due to the common tradeoff between data availability and privacy, protecting the sensitive user information contained in the QoS data will decrease the availability of QoS data and finally produce inaccurate recommendation results. Considering these challenges, Qi *et al.* propose in "Privacy-Aware Cross-Platform Service Recommendation based on Enhanced Locality-Sensitive Hashing" an approach based on enhanced Locality-Sensitive Hashing for accurate and less-sensitive cross-platform recommendation decision-makings.

In "Beh-Raft-Chain: A Behavior-based Fast Blockchain Protocol for Complex Networks," Wang *et al.* focus on the scalability of sharding-based blockchain protocols and developed a Beh-Raft-Chain solution to reduce the traffic complexity while enhancing the transaction rates and the amount of fault-toleration for complex network applications. In detail, they replace the practical Byzantine Fault Tolerance consensus protocol with the behavior-based Raft consensus protocol to incentivize honest behaviors and neutralize malicious attacks. They design a supervisory mechanism to guarantee the security of local consensus and set a self-adaptive parameter to satisfy sustainability requirements by incentivizing honest behavior for enlarging the range of candidate nodes being chosen to resist monopoly attacks.

Digital Object Identifier 10.1109/TNSE.2021.3073636

In "User Matching on Blockchain for Computation Offloading in Ultra-dense Wireless Networks," Seng *et al.* presented a decentralized coordination scheme that exploits blockchain technology to orchestrate the computation task scheduling among mobile users and edge servers. Specifically, it develops an efficient task-VM matching algorithm that jointly considers task execution time and energy consumption. Particularly, it proves the stability of the task-VM matching achieved by the matching algorithm. Besides, the task-VM matching algorithm is implemented on the blockchain by developing a smart matching contract. Simulation results demonstrate the significant performance improvement by the decentralized coordination scheme.

In "A Blockchain-based Storage System with Financial Incentives for Load-balancing," Yin *et al.* propose a blockchain-based storage system with financial incentives for load-balancing. Users upload data to the system while nodes continuously generate a proof of storage, competing for a reward from users' leasing payment. They design an incentive mechanism to reward the nodes who store proper data but punish the nodes who store excessive data. To coordinate the reward allocation, they leverage the storage proofs in the blockchain to detect node failures and record data distribution. The simulation experiments show efficient performance, where the system can always recover to a balanced status as the blockchain grows up.

In "Consortium Blockchain for Secure Resource Sharing in Vehicular Edge Computing: A Contract-based Approach," Wang *et al.* propose a vehicular consortium blockchain for secure resource sharing in vehicular edge computing. First, multi-step smart contracts are designed to achieve secure resource sharing and defend against the malicious behaviors of service requesters and vehicles with selfish purposes. Then, a byzantine fault tolerance-based proof-of-stake consensus protocol is applied in consortium blockchain to reach consensus efficiently. Finally, a contract-based incentive mechanism is devised to motivate vehicles to share their computation resources with service requesters. The optimal contracts are derived to maximize the service requesters' expected utility as well as social welfare.

The emergence of 5G technology contributes to create more open and efficient eco-systems for various vertical industries. However, cybersecurity threats such as information leakage or piracy are more likely to occur in these open environments. Xu *et al.* propose in "Blockchain-Enabled Accountability Mechanism Against Information Leakage in Vertical Industry Services" to use interactive watermark embedding techniques for ensuring that both providers and acquirers can fairly generate watermarked content for sharing. They further utilized the blockchain system as an evidence recorder for tracing the information leakage during the content-sharing processes in vertical industry services.

In "B-Ride: Ride Sharing With Privacy-Preservation, Trust and Fair Payment Atop Public Blockchain," Baza *et al.* explore ride-sharing that enables drivers to share their trips with other riders, contributing to appealing benefits of shared travel costs. However, the majority of existing platforms rely on a central third party, which make them subject to a single point of failure and privacy disclosure issues. The authors propose a decentralized ride-sharing service based on public Blockchain, named B-Ride. Both riders and drivers can find rides match while preserving their trip data, including pick-up/drop-off location, and departure/arrival date. B-Ride introduces a time-locked deposit protocol for ride-sharing by leveraging smart contracts and zero-knowledge set membership proofs.

Popular Blockchain-based cryptocurrencies, like Bitcoin, are increasingly being used maliciously to launder money on the dark Web. However, existing Bitcoin flow analysis methods only focus on Bitcoin addresses and flow, and neglect other important information, such as transaction structure and behavior features. In order to exploit all useful features of transactions, Wu *et al.* propose in "A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation" a Bitcoin transaction network analytic method for facilitating Blockchain forensic investigation based on an extended safe Petri Net. This method not only can analyze single or multiple bitcoin transaction and flow features but also can define and analyze bitcoin trade patterns. The proposed method provides a reliable and efficient forensic investigation model which is able to enhance financial security.

Privacy, confidentiality, and data consistency are major challenges in Electronic Health Records (EHRs). Bhattacharya *et al.* propose in "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications" a framework called as Blockchain-Based Deep Learning as-a-Service (BinDaaS). It integrates blockchain and deep-learning techniques for sharing EHR records among multiple healthcare users. The obtained results are compared using various parameters such as accuracy, end-to- end latency, mining time, and computation and communication costs in comparison to the existing state-of-the-art proposals.

Our Guest Editor team is pleased with the technical depth and span of this special section in IEEE Transactions on Nework Science and Engineering. We sincerely thank all the authors and reviewers for their efforts, and the Editor-in-Chief and Staff Members for their gracious support. We hope that the readers will enjoy this special section.

Yulei Wu, *Guest Editor*
Department of Computer Science
College of Engineering, Mathematics, and Physical Sciences
University of Exeter
EX4 4QF Exeter, U.K.
e-mail: y.l.wu@exeter.ac.uk
Zheng Yan, *Guest Editor*
Aalto University
Espoo 02150, Finland
Xidian University
Xi'an 710071, China
e-mail: zyan@xidian.edu.cn

RUPPA K. THULASIRAM, *Guest Editor*
Department of Computer Science
University of Manitoba
Winnipeg, MN R3T 2N2, Canada
e-mail: tulsi@cs.umanitoba.ca

MOHAMMED ATIQUZZAMAN, *Guest Editor*
School of Computer Science
University of Oklahoma
Tulsa, OK 73019 USA
e-mail: atiq@ou.edu

REFERENCES

[1] Y. Wu, H. -N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021.

[2] Y. Wu, H. -N. Dai, H. Wang, and K. -K. R. Choo, "Blockchain-Based privacy preservation for 5G-Enabled drone communications," *IEEE Netw.*, vol. 35, no. 1, pp. 50–56, Jan./Feb. 2021.

[3] G. Liu, Z. Yan, W. Feng, X. Y. Jing, Y. X. Chen, and M. Atiquzzaman, "SeDID: An SGX-enabled decentralized intrusion detection framework for network trust evaluation," *Inf. Fusion*, vol. 70, pp. 100–114, Jun. 2021.

[4] G. Liu, H. D. Dong, Z. Yan, X. K. Zhou, and S. Shimizu, "B4SDC: A blockchain system for security data collection in MANETs," *IEEE Trans. Big Data*, vol. 7, no. 6, pp. 5329–5344, Jun. 2020.

Yulei Wu (Senior Member, IEEE) is currently a Senior Lecturer with the Department of Computer Science, College of Engineering, Mathematics, and Physical Sciences, University of Exeter, Exeter, U.K. His expertise is on intelligent networking, and his main research interests include computer networks, networked systems, software defined networks and systems, network management, and network security and privacy.

Zheng Yan (Senior Member, IEEE) is currently a Professor with Xidian University, Xi'an, China, and a Visiting Professor and Finnish Academy Research Fellow with Aalto University, Espoo, Finland. Her research interests include trust, security, and privacy, telecommunication networking, data analytics, mobile applications and services, social networking, and cloud computing.

Ruppa K. Thulasiram (Senior Member, IEEE) is currently a Professor with the Department of Computer Science, University of Manitoba, Winnipeg, MB, Canada. His current research interests include computational finance, cloud computing, data science, and blockchain technology for finance, and related areas focusing on data-driven pricing algorithms, task matching in grid or cloud Systems, and resource pricing in cloud.

Mohammed Atiquzzaman (Senior Member, IEEE) is currently the Edith Kinney Gaylord Presidential Professorship with the School of Computer Science, University of Oklahoma, Norman, OK, USA. His research interests include communications switching, transport protocols, wireless and mobile networks, ad hoc networks, satellite networks, quality of service, and optical communications.