Guest Editorial: Special Issue on Recent Advances on Blockchain for Network and Service Management

I. Introduction

WITH the rapid adoption of new technologies and applications, e.g., the Internet of Things, 5G/6G communication networks, big data analytics, and artificial intelligence, a deluge of devices are being connected to the network, thus generating a large amount of data. The collection, processing, and analysis of this vast amount of data are essential to help people and enterprises gain valuable information, make sensible decisions, and subsequently improve the quality of people's lives. However, the underlying communication networks are thus facing a new number of unprecedented challenges. Managing these large numbers of devices in a scalable and secure manner is bringing significant challenges to the infrastructure construction, maintenance, and management of the communication networks. Recurring data privacy breaches and the lack of control make Internet users and enterprises less willing to provide valuable data for processing and analysis.

In recent years, the emergence of blockchain technology has offered several salient features, including decentralization, trust, immutability, and security, that could address some of the safety, privacy, and transparency challenges. For example, the traceability of blockchain allows data to be recorded on the distributed ledgers from every step of collection and transaction, improves the quality of the data, and ensures the correctness of data analysis and mining. The decentralization of blockchain also offers a different perspective for device management in a communication network, as devices can establish and learn relationships with other devices. Thus, distributed ledger technology (DLT) offers tremendous potential to disrupt all the industrial domains which involve coordination among autonomous resources. This includes finance technology (fintech) and payment systems (e.g., Bitcoin/Ethereum, SWIFT and Central Bank Digital Currencies), but also networks (e.g., power grids or telecom networks), computing (e.g., brokering of edge resources), IoT (e.g., supply chains or industry 4.0), and other service platforms (e.g., identity management).

This Special Issue of IEEE Transactions on Network and Service Management aims to explore the research challenges in blockchain technologies, highlighting their promising capabilities to provide reliable and secure networked applications and services. It is the first special issue on this topic to appear in this journal. The collection of papers illustrates recent trends, novel solutions and approaches to leveraging blockchain and distributed ledgers in network and service management, as well as to extract insights that can guide system operators and network managers to address their pressing problems. This special issue consists of 22 papers out of 63 papers submitted to the call for novel contributions addressing the underlying challenges of embracing blockchain for network and service management.

II. Special Issue Overview

The special section papers span five central areas: storage optimization, security and privacy, services and algorithms, applications and performance measurements.

A. Storage Optimization

Three papers in this special issue focus on challenges in storage optimization in blockchains.

In [A1], Zhou et al. first perform a comprehensive statistical experiment on the Bitcoin network and showed that in nearly 95% of blocks, the number of spent transaction output (STXO) accounts for more than 67% of the total transaction output. They propose a novel storage scheme to reduce the size of blocks by deleting the transaction data with the STXO ratio over 67% and compressing some fixed-length fields in those transactions. The newly generated block files are stored in an interplanetary file system (IPFS) private network to further improve the scalability.

In [A2], Huang and Huang present a new storage structure for efficient data search based on the AVL tree. They also propose a data management scheme divided into two operations, splitting and merging and mathematically analyze the performance of their approach.

In [A3], Heo et al. propose multi-level distributed caching (MLDC) for blockchain storage optimisation, which reduces data replication based on data access patterns. MLDC introduces a hierarchical storage class (SC) in which every node is assigned to an SC with its access frequency (AF) threshold based on node availability. To reduce the number of replications shared among participant nodes, each node in an SC continues to remove unaccessed data from local storage based on a threshold time determined by the AF threshold of the SC while maintaining block hashes for consistency.

Digital Object Identifier 10.1109/TNSM.2022.3227783

B. Security and Privacy

Five papers in this special issue focus on security and privacy issues.

In [A4], Zhao et al. propose an improved change address inference method and mixing service recognition method to improve Bitcoin address clustering. This work has serious implications on privacy as the proposed methods for improving user recognition and association of user behavior and thus on privacy.

In [A5], Bai et al. present a privacy-preserving oriented no trusted third party federated learning system based on blockchain called NttpFL. The initiator of the federated learning task and the partners negotiate keys through a conference key agreement and do not need to distribute keys through a trusted third party. A double-layer encryption mechanism is adopted to ensure privacy.

In [A6], Wang et al. propose SorTEE, a service-oriented routing solution for payment channel networks, which adopts a set of service nodes to alleviate the per-node burden of routing and achieves comprehensive privacy guarantees than the state-of-the-art by leveraging trusted execution environments (TEEs). SorTEE requires that users communicate with the TEE through a secure channel to protect the privacy of transaction value.

In [A7], Garcia et al. present a decentralized data governance framework based on blockchain technology, proxy re-encryption, and Boneh, Boyen, and Shacham (BBS+) signatures to let data owners control, selectively share and track their data through privacy-enhancing, consent management, and selective disclosure mechanisms. The framework allows data consumers to understand data lineage through a blockchain-based provenance mechanism.

In [A8], Song et al. propose a general framework for privacy-preserving blockchain-based anomaly detection. The framework includes ADaaS, an anomaly detection service scheme that adopts a supervised machine learning model and achieves privacy preservation by using homomorphic encryption and matrix perturbation.

C. Services and Algorithms

Six papers in this special issue focus on novel services and algorithms for improved performance.

In [A9], Wu et al. present the design of a trustworthy and real-time decentralized computing resource allocation platform based on blockchain and smart contracts. To optimize the allocation results, they improve the non-dominated sorting genetic algorithm II (NSGA-II) for miners to reach the consensus mechanism.

In [A10], Rong and Zheng present a Federal Reconstruction Committee Raft consensus algorithm called FRCR. Based on the federation reconstruction technology, the algorithm trains, updates, and evaluates the model of the characteristic data set of the Raft node, runs the model to get the nodes with better performance, constructs the committee mechanism, and improves the quality and speed of the election.

In [A11], Scheid et al. present the design and implementation of a machine learning-based blockchain selection approach that employs four machine learning models to select the most suitable blockchain given user requirements, e.g., blockchain popularity, fast block inclusion, or smart contract support.

In [A12], Castellon et al. apply an energy-reducing algorithmic engineering technique for Merkle Tree (MT) root calculations, and the Proof of Work (PoW) algorithm, two principal elements of blockchain computations, as a means to preserve the promised security benefits but with less compromise to system availability.

In [A13], Ridhawi et al. introduce a cooperative blockchain-enabled resource and capability sharing approach to fulfil cyber-physical system tasks. The solution uses a multi-stage blockchain and federated learning to group IoT devices into clusters and a global deep model is then created on the cloud using federated aggregation.

In [A14], Botta et al. present mechanisms for securely deleting data from Bitcoin's blockchain. They take advantage of recent progress on succinct zero-knowledge proofs to design a mechanism allowing any node to delete some data from Bitcoin transactions, still preserving the public verifiability of the correctness of the spent and spendable coins.

D. Applications

Six papers in this special issue focus on novel blockchain technology applications and specific challenges presented in those industry verticals.

In [A15], Jiang et al. focus on improving patients' control over electronic health records (EHR). They propose attribute-based encryption with a blockchain protection scheme for EHR protection in an edge cloud environment called CEC-ABE. The agreement process between the patient and the hospital is added before the ABE stage, and the treatment information, including treatment time, treatment doctor and other treatment information, are confidentially transmitted through the encryption algorithm.

In [A16], Demirbaga and Aujla present a scalable computing system that provides verifiable data access mechanism for IoT-enabled health data analytics in the big data ecosystem. The approach leverages big data systems and blockchain architecture to analyze and securely store data from IoT-enabled devices and allow verified access to the stored data. A zero-knowledge protocol is used to ensure that no information is accessible to unauthenticated users.

In [A17], Qi et al. present an intelligent computing offloading model for connected, intelligent vehicles to execute computationally intensive and delay-sensitive emerging applications in multiple business scenarios. The proposed strategy can minimize the total system cost under time delay and energy consumption constraints.

In [A18], Benadla et al. propose a blockchain-based mechanism to detect Sybil attacks in VFC networks. The detection process consists of two levels; the first one is targeted towards the verification of the position of a vehicle by the fog node using the received signal strength indicator (RSSI). The second level is projected towards comparing the trajectories of the vehicles reporting an event.

In [A19], Lv et al. introduce a federated learning scheme based on blockchain to detect misbehavior in vehicular ad hoc networks, which can reduce resource utilization while ensuring data security and privacy. Furthermore, differential privacy with the Gaussian mechanism is leveraged to provide strict privacy protection.

In [A20], Zhang et al. propose an efficient and robust multidimensional data aggregation scheme based on blockchain for smart grids. A leader election algorithm in Raft protocol is used to select a mining node from all smart meters to aggregate data, and a dynamically verifiable secret sharing homomorphism scheme is adopted to realize flexible, dynamic user management.

E. Performance Measurements

Two papers in this special issue focus on empirical performance measurements on blockchain networks.

In [A21], Imtiaz et al. use an experimental testbed of twelve full nodes connected to the Bitcoin Cash blockchain for comparing the performance of block relay protocols. With the aid of novel logging tools, they contrast the performance of three specific block relay protocols, in realistic scenarios, concerning communication, delay, and block decoding success.

In [A22], Gebraselase et al. present an extensive study on the transaction characteristic of Bitcoin through a testbed. They particularly focus on understanding the impact of peer formation strategies, peer lists, and delay on node-to-node communication.

Acknowledgment

We sincerely thank the authors for contributing their papers and the reviewers for their thorough assessment and their work to improve the quality and presentation of each paper. We are very grateful to the Editor-in-Chief Hannan Lutfiyya for her continuous support throughout the process and to Janine Bruttin for their help with the administrative tasks associated with this special issue.

Appendix: Related Works

[A1] K. Zhou, C. Wang, X. Wang, S. Chen, and H. Cheng, “A novel scheme to improve the scalability of bitcoin combining IPFS with block compression,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3694–3705, Dec. 2022.

[A2] T.-L. Huang and J. Huang, “An efficient storage structure and management for distributed ledgers in blockchain systems: An exploration based on purely theoretical approach,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3706–3723, Dec. 2022.

[A3] J. W. Heo, G. Ramachandran, A. Dorri, and R. Jurdak, “Blockchain storage optimisation with multi-level distributed caching,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3724–3736, Dec. 2022.

[A4] Z. Zhao, J. Wang, K. Shi, and H. Zhang, “Improving address clustering in bitcoin by proposing heuristics,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3737–3749, Dec. 2022.

[A5] S. Bai, G. Yang, G. Liu, H. Dai, and C. Rong, “NttpFL: Privacy-preserving oriented no trusted third party federated learning system based on blockchain,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3750–3763, Dec. 2022.

[A6] Q. Wang et al., “SorTEE: Service-oriented routing for payment channel networks with scalability and privacy protection,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3764–3780, Dec. 2022.

[A7] R. D. Garcia, G. S. Ramachandran, R. Jurdak, and J. Ueyama, “Blockchain-aided and privacy-preserving data governance in multi-stakeholder applications,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3781–3793, Dec. 2022.

[A8] Y. Song, Y. Zhu, K. Zhu, and F. Wei, “Anomaly detection as a service: An outsourced anomaly detection scheme for blockchain in a privacy-preserving manner,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3794–3809, Dec. 2022.

[A9] W.-C. Wu, C.-J. Chew, Y.-C. Chen, C.-H. Wu, T. H. Chen, and J.-S. Lee, “Blockchain-based WDP solution for real-time heterogeneous computing resource allocation,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3810–3821, Dec. 2022.

[A10] B. Rong and Z. Zheng, “FRCR:Raft consensus scheme based on semi asynchronous federal reconstruction,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3822–3834, Dec. 2022.

[A11] E. J. Scheid, R. Hy, M. F. Franco, C. Killer, and B. Stiller, “On the employment of machine learning in the blockchain selection process,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3835–3846, Dec. 2022.

[A12] C. E. Castellon, S. Roy, O. P. Kreidl, A. Dutta, and L. Bölöni, “Towards a green blockchain: Engineering Merkle Tree and proof of work for energy optimization,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3847–3857, Dec. 2022.

[A13] I. A. Ridhawi, M. Aloqaily, A. Abbas, and F. Karray, “An intelligent blockchain-assisted cooperative framework for industry 4.0 service management,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3858–3871, Dec. 2022.

[A14] V. Botta, V. Iovino, and I. Visconti, “Towards data redaction in Bitcoin,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3872–3883, Dec. 2022.

[A15] Y. Jiang, X. Xu, and F. Xiao, “Attribute-based encryption with blockchain protection scheme for electronic health records,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3884–3895, Dec. 2022.

[A16] U. Demirbaga and G. S. Aujla, “MapChain: A blockchain-based verifiable healthcare service management in IoT-based big data ecosystem,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3896–3907, Dec. 2022.

[A17] J. Qi, Y. Liu, Y. Ling, B. Xu, Z. Dong, and Y. Sun, “Research on an intelligent computing offloading model for the Internet of Vehicles based on blockchain,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3908–3918, Dec. 2022.

[A18] S. Benadla, O. R. Merad-Boudia, S. M. Senouci, and M. Lehsaini, “Detecting sybil attacks in vehicular fog networks using RSSI and blockchain,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3919–3935, Dec. 2022.

[A19] P. Lv, L. Xie, J. Xu, X. Wu, and T. Li, “Misbehavior detection in vehicular ad hoc networks based on privacy-preserving federated learning and blockchain,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3936–3948, Dec. 2022.

[A20] X. Zhang, L. You, and G. Hu, “An efficient and robust multidimensional data aggregation scheme for smart grid based on blockchain,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3949–3959, Dec. 2022.

[A21] M. A. Imtiaz, D. Starobinski, and A. Trachtenberg, “Empirical comparison of block relay protocols,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3960–3974, Dec. 2022.

[A22] B. G. Gebraselase, B. E. Helvik, and Y. Jiang, “Bitcoin P2P network measurements: A testbed study of the effect of peer selection on transaction propagation and confirmation times,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3975–3987, Dec. 2022.

SALIL S. KANHERE
School of Computer Science and Engineering
UNSW Sydney
Sydney, NSW 2052, Australia
E-mail: salil.kanhere@unsw.edu.au

ANDREAS VENERIS
Department of Electrical and Computer Engineering
University of Toronto
Toronto, ON M5S, Canada

SACHIKO YOSHIHAMA
Amazon Web Services
Tokyo 153-0064, Japan

SANDIP CHAKRABORTY
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur 721302, India

ORI ROTTENSTREICH
Department of Electrical Engineering
Technion
Haifa 3200003, Israel

Department of Computer Science
Technion
Haifa 3200003, Israel

MARTA BELTRAN PARDO
School of Computer Engineering
Rey Juan Carlos University
28933 Móstoles, Spain

BRUNO RODRIGUEZ
Department of Informatics
University of Zurich
8006 Zürich, Switzerland

Salil S. Kanhere (Senior Member, IEEE) is a Professor with the School of Computer Science and Engineering, UNSW Sydney, Australia. He has held visiting appointments with I2R Singapore, TU Darmstadt, TU Graz, RWTH Aachen, and the University of Zurich. His research interests include Internet of Things, cybersecurity, distributed systems, pervasive computing, and applied machine learning. He received the Friedrich Wilhelm Bessel Research Award in 2020 and the Humboldt Research Fellowship in 2014 from the Alexander von Humboldt Foundation in Germany. He has received eight best paper awards. He is the Editor-in-Chief of *Ad Hoc Networks* and an Associate Editor of the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *Pervasive and Mobile Computing*, and *Computer Communications*. He regularly serves on the Organising Committee of many IEEE and ACM conferences. In 2022, he served as the Program Co-Chair for the IEEE International Conference on Network and Service Management. He is a Senior Member of ACM and an IEEE Computer Society Distinguished Visitor.

Andreas Veneris (Senior Member, IEEE) received the Ph.D. degree from the University of Illinois at Urbana–Champaign. He is a Connaught Scholar and a Professor with the Department of Electrical and Computer Engineering, cross-appointed with the Department of Computer Science, University of Toronto. In the past, he held joint faculty positions with the Department of Informatics, Athens University of Economics and Business from 2006 to 2016 and the Department of ECE, University of Tokyo from 2010 to 2011. For over 20 years, he worked in the field of CAD for VLSI synthesis, verification, and debugging using formal methods, where he published more than 120 conference/journal papers. Today, he focuses on Central Bank Digital Currencies, mechanism and system design, distributed oracles, formal methods for smart contract verification, IoT and distributed systems, techno-legal blockchain matters, and crypto-economics. He has received a 10-year Best Paper Retrospective Award and three other best paper awards and holds many patents. He was a Team Member in the first webcast ever (37th Grammy Awards, 1995), an event acknowledged by the American Congress. In February 2021, his work with the Bank of Canada became public, proposing Canada's Central Bank Digital Loonie—the first work of its kind that presents a comprehensive technological, regulatory/legal, and economic model for a central bank digital currency. In 2021, he was honored to be given the opportunity to comment on a classified report by the Hoover Institution, edited by Darrell Duffie and Elizabeth Economy, prefaced by Condoleezza Rice, and coauthored by an extensive list of prominent world-thinkers. This report was released on 1 March 2022 and it is titled "Digital Currencies: The U.S., China, and the World at a Crossroads." On 8 March 2022, the U.S. President Joe Biden signed an Executive Order following most of the recommendations of this report.

Sachiko Yoshihama received the Ph.D. degree in information security from Yokohama National University in 2010. Prior to her current position, she was a Senior Technical Staff Member and a Senior Manager with IBM Research-Tokyo and led several blockchain research projects with a focus on real-world industry use cases. She gave several invited talks on blockchain and served as the General Co-Chair of the Blockchain Symposium at IEEE SERVICES 2021, a Steering Committee Member of the IEEE International Conference on Blockchain and Cryptocurrency 2021, and a Program Committee Co-Chair of IEEE Blockchain 2019. She was appointed as the Director of General Affairs at the Information Processing Society of Japan in June 2021.

Sandip Chakraborty (Member, IEEE) received the bachelor's degree from Jadavpur University, Kolkata, in 2009, and the M.Tech. and Ph.D. degrees from IIT Guwahati in 2011 and 2014, respectively. He is working as an Associate Professor with the Department of CSE, IIT Kharagpur. His primary research interests are distributed systems, mobile computing, and human–computer interactions. He received various awards, including the Indian National Academy of Engineering Young Engineers' Award in 2019 and the Honorable Mention Award in ACM SIGCHI EICS 2020. He is one of the founding chairs of ACM IMOBILE, the ACM SIGMOBILE Chapter in India. He works as an Area Editor of *Ad Hoc Networks* (Elsevier) and *Pervasive and Mobile Computing* (Elsevier). Further details about his works and publications can be obtained from https://cse.iitkgp.ac.in/sandipc/index.html.

Ori Rottenstreich (Member, IEEE) received the B.Sc. degree *(summa cum laude)* in computer engineering and the Ph.D. degree from Technion, Haifa, Israel, in 2008 and 2014, respectively, where he is an Assistant Professor with the Department of Computer Science and the Department of Electrical Engineering. From 2015 to 2017, he was a Postdoctoral Research Fellow with Princeton University.

Marta Beltran Pardo (Senior Member, IEEE) received the M.S. degree from Complutense University, Madrid, Spain, in 2001, and the Ph.D. degree from Rey Juan Carlos University, Madrid, in 2005, where she is an Associate Professor with the School of Computer Engineering. She is the co-inventor of a patent in the identity and access management field. She has coauthored several books about distributed systems and cybersecurity with Prentice Hall, Paraninfo, and RaMa. Her research interests include distributed systems (cloud computing, Internet of Things, and edge computing), cybersecurity, and privacy. She has served on the organising committee of several international conferences, including ISPDC, AINA, MASCOTS, ECMS, EPEW, ITICSE, and ICBC. She serves as a member of the UN Internet Governance Forum (IGF, Spanish Chapter) advisory board and the technical committee of standardisation CTN 320 at the UNE (Cybersecurity and Personal Data Protection).

Bruno Rodriguez received the master's degree from the University of São Paulo, Brazil, in 2016, and the Doctoral degree from the Communication Systems Group, University of Zurich in 2020, under the supervision of Prof. B. Stiller. He coauthored three patents and published over 60 papers and journals in related IEEE networking conferences, such as IEEE/IFIP NOMS, IEEE/IFIP IM, and IEEE LCN and leading IEEE journals, such as IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT and *IEEE Communications Magazine*. He currently focuses his research on the automation of network security management. Further, he is actively contributing to the scientific community by actively reviewing papers and journals, acting as a guest editor, and technical program committee in networking and blockchain conferences.