NETWORKS FOR BLOCKCHAIN-ENABLED APPLICATIONS



Jelena Mišić Haisheng Guo Vojislav B. Mišić

With fast evolution of computer and networking technologies, more and more systems and applications are based on interconnecting different devices and systems to form the Internet-of-Something: things, vehicles, and even bodies. Many among those systems require permanent, distributed data storage facilities which are being increasingly implemented using replicated, tamper-proof blockchain ledgers. Most, if not all, of those problems are exacerbated, rather than solved, by blockchain technology. In addition, the use of blockchain brings many challenges that include efficient and reliable data distribution; efficient and collusion-proof consensus mechanisms; efficient coverage of wide geographical areas; and a plethora of existing security- and privacy-related constraints on the networks.

The purpose of this special issue was to bring together the latest research results related to analysis, design, and implementation of network and communication systems that support blockchain-enabled Internet-of-Anything systems and applications.

In response to the call for papers, we have received more than twenty papers, out of which we have selected seven papers introduced in more detail below.

The first three articles deal with conceptual and practical foundations of blockchain-based IoX applications. The first article, "A Decentralized Oracle Architecture for a Blockchain-based IoT Global Market," by Lorenzo Gigli, Ivan Zyrianoff, Federico Montori, Cristiano Aguzzi, Luca Roffia, and Marco Di Felice, describes the architecture in which the network of IoT devices provides the foundation for a global decentralized IoT market. A distributed oracle layer powered by smart contracts allows clients to perform operations such as data discovery, semantic location-specific or location-free queries, and selection of trustworthy data sources based on their reputation. Moreover, the architecture allows data creators to get paid for the data used by the clients. In this manner, the oracle layer provides the necessary decoupling between clients and data providers and allows seamless interoperability between the two communities. The architecture is shown to be robust and consistent, even in the presence of malicious users and/or data sources.

A different perspective is provided in the article "A Blockchain-Based Semantic Exchange Framework for Web 3.0 Toward Participatory Economy," by Yijing Lin, Zhipeng Gao, Yaofeng Tu, Hongyang Du, Dusit Niyato, Jiawen Kang, and Hui Yang. In this article, the Web 3.0 next-generation Internet principles are exploited to enable participants to read, write, and own contents in a decentralized manner. The critical success factors of the Web 3.0 paradigm are blockchain, semantic communication, edge computing, and artificial intelligence; together, they allow the construction of value networks to achieve participatory economics based on participatory decision making. The authors argue that current Web 3.0 solutions tend to focus on the blockchain while overlooking other new technologies' roles and propose a blockchain-based semantic exchange framework to realize fair and efficient interactions. In this framework, semantic information is tokenized into Non-Fungible Token (NFT) for semantic exchange while a Stackelberg game is used to maximize buying and pricing strategies for semantic trading. Sharing of authentic semantic information without revealing the information itself or its source before receiving payments is handled through Zero-Knowledge Proofs. As the result the proposed framework allows information to be shared in an efficient and privacy-preserving manner. Its feasibility is corroborated through a detailed urban planning case study.

One of the problems with blockchain-based applications that is often overlooked Is the replication of data which is rather challenging to address using traditional storage system technology. In the article "Mechanisms Design for Blockchain Storage Sustainability," authors Yunshu Liu, Zhixuan Fang, Man Hon Cheung, Wei Cai, and Jianwei Huang first present a comprehensive review of the state-of-the-art mechanisms designed to address the storage sustainability problem. Then, they introduce technological mechanisms aimed at reducing miners' storage costs and discuss the incentive mechanisms that reduce storage costs by encourage users to pay adequate transaction fees. The article concludes by discussing future challenges and open problems in this field.

Security of blockchain-based IoX applications is investigated in detail in the next two articles. The article "A Taxonomy of Blockchain Incentive Vulnerabilities for Networked Intelligent Systems, by Hector Roussille, Önder Gürcan, and Fabien Michel, presents a taxonomy of incentive vulnerabilities that can affect both public- and consortium blockchain-based networked intelligent systems. The proposed taxonomy is based on a generic multi-agent organizational model for blockchain systems, and it builds a relationship between dedicated agent roles and identified vulnerabilities which are expressed as behavior deviations. In addition, vulnerabilities are classified according to the roles and behaviors identified in agent-based model, which should help researchers and developers better understand the related threats and design more secure systems.

The article "A Dynamic Blockchain-Based Mutual Authenticating Identity Management System for Next-Generation Network," by Haikun Xu, Xuefei Zhang, Qimei Cui, and Xiaofeng Tao, describes a dynamic blockchain-based identity management system which is suitable for direct communication between service providers (SPs) and user equipment (UE) devices. System resiliency in different operations, including the process of mutual authentication of SPs and UEs, is enhanced using dynamic cryptographic key generation and dynamic chameleon hash functions. Extensive simulation-based analysis simulation and risk score calculations confirm the feasibility of the proposed system.

The last two articles address the topics of this special issue from an application-based perspective. The article "A Novel

Blockchain-Based Model for Agricultural Product Traceability System," by Shaopeng Guan, Zhenqi Wang, and Youliang Cao, proposes and analyzes a novel blockchain-based model for agricultural product traceability system which aims to provide satisfactory performance whilst protecting the privacy of agricultural product information. It utilizes a multi-channel data collection and uploading architecture in which different channels correspond to the collection and uploading of information of different types of agricultural products. The uploaded information is encrypted using a hierarchical encryption algorithm and subsequently stored in the blockchain to realize the secure sharing of agricultural product information. System performance is evaluated using the Hyperledger Fabric platform.

Finally, the article "Deep-Reuse-Enabled Common Satellite Network via Collaborative Blockchains: Architecture, Challenges, and Solutions," by Xiuyuan Chen, Chao Lin, Wei Wu, Jianting Ning, Junzuo Lai, and Debiao He, focuses on some of the most important problems encountered by satellite networks that use blockchain as storage technology. Most notably, these problems include severe congestion caused by a surge in simultaneous requests, which is particularly pronounced in applications that use satellite constellations, as well as the contentious interaction due to the unrecorded distribution and centralized management of satellite networks. To address those problems, the authors propose an architecture of Deep-reuse-enabled Common Satellite Network via Collaborative Blockchains, where the notion of deep reuse is described from resources and information. They also highlight potential security and efficiency issues faced by the architecture from the perspectives of authentication, command control, and data management, and outline the prospective blockchain- based technologies that can help offset those problems, namely, the cross-domain authentication, digital-twins-enabled edge computing, and auto-audit of data.

We believe that the articles in this collection provide a comprehensive cross-section of problems encountered in blockchain-based IoX applications and feasible solutions to those problems, both of which may serve as the foundation for building future blockchain-based applications as well as a useful reference for developers and researchers.

Biographies

Jelena Mišić [M'91, SM'08, F'18] is Professor of Computer Science at Toronto Metropolitan (formerly Ryerson) University in Toronto, Canada. She has published 4 books, over 165 papers in archival journals and about 220 papers at international conferences in the areas of computer networks and security. She is an IEEE VTS Distinguished Lecturer, and serves on editorial boards of *IEEE Transactions on Vehicular Technology*, *IEEE Internet of Things Journal*, *IEEE Transactions on Emerging Topics in Computing*, *IEEE Network*, *ACM Computing Surveys*, *Computer Networks* and *Ad Hoc Networks*.

Haisheng Guo is currently a Chief Engineer at Data Intelligence Platform Department, ZTE Corporation. He received the MS degree from Nanjing University of Aeronautics and Astronautics in March 2001. His research interests include blockchain and artificial intelligence. He has participated in and completed a number of blockchain-related standardizations, and published dozens of technical papers and patents.

Vojislav B. Mišić [M'92, SM'08] is Professor of Computer Science at Toronto Metropolitan (formerly Ryerson) University in Toronto, Canada. His research interests include performance evaluation of wireless networks and blockchain technology. He serves on the editorial boards of *IEEE Transactions on Network Science and Engineering*, *Peer-to-Peer Networks and Applications*, and *Ad Hoc Networks*.