Digital Communications and Networks 6 (2020) 145–146

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Editorial: Special issue on blockchain and communication networks

1. Introduction

With the boom of new technologies and applications, e.g., Internet of Things, big data, and artificial intelligence, a deluge of devices are being connected to the network, thus generating a large amount of data [1]. Data collection, processing and analysis are essentials to help people gain valuable information, make sensible decisions, and also make devices intelligent. The underlying communication network is thus facing unprecedented challenges. Along with the increase in devices, managing these devices in the existing centralized model will bring significant challenges to the infrastructure construction, maintenance, and management of the communication network. In addition, the current technology/protocol in communication networks cannot adequately ensure the security and privacy of user data, and the use of collected data is beyond the control of the user. Internet users and companies, therefore, are concerned for the privacy of their data, unwilling to provide valuable data for processing and analysis.

Blockchain enables transparent interactions of different parties in a more secure and reliable network [2–7]. It is a promising technology that can simplify the management of safe information over communication networks. Given that the blockchain is trustworthy, secure, and cannot be tampered with, more data are likely to be provided over the communication network. The traceability of blockchain allows data to be retained on the blockchain from every step of collection and transaction, improve the quality of the data, and ensure the correctness of data analysis and mining. The decentralization of blockchain also provides a way for device management in the communication network, which can help devices understand one another (knowing the relationships between different devices). However, employing blockchain mechanisms in communication networks still has some technical challenges and limitations.

This special issue is devoted to the most recent developments and research outcomes addressing the related theoretical and practical aspects of blockchain and communication networks and aims at presenting fresh innovative ideas targeted at the corresponding major challenges, from either a methodological or an application perspective. Considering the significance, originality, novelty and presentation of submitted articles, we selected four articles to be included in this Special Issue.

2. Articles

Taylor et al. provided in the paper entitled “A systematic literature review of blockchain cyber security” [8] a systematic review on the blockchain for cyber security and presented a breakdown of popular blockchain applications, such as networks and machine visualization, certification schemes and public-key cryptography. The paper also anticipated future directions of research, education and practices in the fields of blockchain and cyber security.

Moustapha in his paper entitled “The effect of propagation delay on the dynamic evolution of the Bitcoin's blockchain” [9], revisited the selfish-mine attack in Bitcoin networks by considering an important parameter, i.e., the propagation delay of information between any two miners in the blockchain network. This paper conducted useful results on the probabilities of reversing the public branch by attackers, in function of its computational power. The author considered that the propagation delay follows a normal distribution with mean proportional to the physical distance between the two miners, and a constant variance independent of others delays. By considering such a propagation delay, the authors proved that no guarantee could be given about the success or failure of the selfish-mine attack because of the variability of information propagation in the network.

Blockchain has been a promising solution for trust management in the supply of chain traceability, due to its characteristics of decentralization, immutability and transparency. Westerkamp, Victor and Kupper in the paper “Tracing manufacturing processes using blockchain-based token compositions” [10] carried out the research in this direction. The authors identified that current systems are limited to tracing simple goods that have not been part of a manufacturing process. They, therefore, proposed a system that can trace manufactured goods, including their components. The authors showed a prototype based on Ethereum, and the implementation for Ethereum virtual machine can be scaled linearly with the number of inputs and tracked goods.

Shrestha et al. in their paper entitled “A new-type of blockchain for secure message exchange in VANET” [11], proposed a public blockchain system to ensure the security of critical message dissemination in Vehicular Ad-hoc Networks (VANET). The blockchain treats messages as transactions and applies Proof-of-Work (PoW) consensus mechanism to generate a new block that stores node trust information and message trust information to support trustworthy message dissemination.

3. Conclusion

Blockchain plays a vital role in the cyber security and communication networks. But the study in this field is a new initiative. There remains a need to keep a watchful eye on recent advances and engage in beating off new challenges.

Acknowledgments

The work is supported in part by the National Natural Science Foundation of China under Grants 61672410 and 61802293, and the

https://doi.org/10.1016/j.dcan.2020.04.012

Academy of Finland under Grants 308087 and 314203, the Key Lab of Information Network Security, Ministry of Public Security under grant No. C18614, the open grant of the Tactical Data Link Lab of the 20th Research Institute of China Electronics Technology Group Corporation, P.R. China under grant CLDL-20182119, the Shaanxi innovation team project under grant 2018TD-007 and the 111 project under grant B16037.

References

[1] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H.N. Dai, Y. Wu, W. Wang, SCTSC: a semi-centralized traffic signal control mode with attribute-based blockchain in IoVs, IEEE Trans. Comput.Soc. Syst. 6 (6) (2019) 1373–1385, https://doi.org/10.1109/TCSS.2019.2904633.

[2] G. Liu, H.D. Dong, Z. Yan, X.K. Zhou, S. Shimizu, B4SDC: A Blockchain System for Security Data Collection in MANETs, IEEE Transactions on Big Data, 2020, https://doi.org/10.1109/TBDATA.2020.2981438.

[3] K.K.R. Choo, Z. Yan, W.Z. Meng, Blockchain in industrial IoT applications security and privacy advances, challenges and opportunities, IEEE Trans. Ind. Inf. 16 (6) (2020) 4119–4121.

[4] Z. Yan, X. Huang, A.V. Vasilakos, L.T. Yang, Special issue on blockchain and decentralization for Internet of Things, Future Generat. Comput. Syst. (2019).

[5] W. Feng, Z. Yan, MCS-Chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain", Future Generat. Comput. Syst. 95 (June 2019) 649–666.

[6] B. Yin, Y. Wu, T. Hu, J. Dong, Z. Jiang, An efficient collaboration and incentive mechanism for internet-of-vehicles (IoVs) with secured information Exchange based on blockchains, IEEE Intern. Things J. 7 (3) (2020) 1582–1593, https://doi.org/10.1109/JIOT.2019.2949088.

[7] Y. Ma, Y. Wu, J. Ge, J. Li, A flow-level architecture for balancing accountability and privacy, in: Proceedings of TrustCom/BigDataSE, 2018, pp. 984–989.

[8] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, K.-K. Raymond Choo, "A Systematic Literature Review of Blockchain Cyber Security," 6 (2) 2020 147–156.

[9] B. A. Moustapha, "The Effect of Propagation Delay on the Dynamic Evolution of the Bitcoin's Blockchain," 6 (2) 2020 157–166.

[10] M. Westerkamp, F. Victor, A. Kupper, "Tracing Manufacturing Processes Using Blockchain-Based Token Compositions," 6 (2) 2020 167–176.

[11] R. Shrestha, R. Bajracharya, A. P. Shrestha, S. Y. Nam, "A New-type of Blockchain for Secure Message Exchange in VANET," 6 (2) 2020 177–186.

Yulei Wu *
University of Exeter, UK

Weizhi Meng
Technical University of Denmark, Denmark

Zheng Yan *
Xidian University, China and Aalto University, Finland

Vijay Varadharajan
The University of Newcastle, Australia

* Corresponding author.

* Corresponding author.