Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2022.025097

EDITORIAL

Introduction to the Special Issue on Blockchain Security

Zhihong Tian[1], Yanhui Guo[2], Shen Su[1,*] and Hui Lu[1]

[1]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, 510006, China

[2]Worcester Polytechnic Institute, Worcester, 01609-2280, USA

*Corresponding Author: Shen Su. Email: sushen@gzhu.edu.cn

Received: 21 June 2022 Accepted: 23 June 2022

Motivated by the fast evolvement of blockchain technology, cloud-edge platforms, intelligent transportation systems, smart grid, vehicular networks, location based services, and other IoT applications have achieved significant breakthrough during recent years. Nowadays, blockchain based researches and projects are super-hot topics and focuses for both research and industrial communities. However, most of the current blockchain projects still suffer from insufficient security concerns. The defects of the underlying protocol make the node communication vulnerable to be hijacked, and further exacerbate the fork problem; smart contracts can hardly be fully tested before deployment because of the evolving blockchain platforms, while the smart contracts updating is impossible (or very complicated); current data privacy protection techniques are either inefficient or inaccurate; sharing and cross-chain schemes brought new security problems together with its TPS promotion. The intrinsic security vulnerabilities make the current blockchain based systems and architectures prone to be assaulted, and further do harm to the confidence of the investment on the blockchain industrial. Worse still, blockchain turns out to play a critical role in a lot of existing security solutions, which would be useless if the blockchain is insecure.

A total of 9 manuscripts were selected based on a robust peer-reviewed process. The 9 articles reflected state of the research developments and initiatives in the blockchain security.

The paper "FileWallet: A File Management System Based on IPFS and Hyperledger Fabric" by Chen et al. [1] proposes a peer-to-peer file management system to serve as a personal wallet for storing and sharing files in a secure manner.

In the paper "Unsupervised Binary Protocol Clustering Based on Maximum Sequential Patterns", Shi et al. [2] propose an unsupervised clustering algorithm based on maximum frequent sequences for binary protocols, which can distinguish various unknown protocols to provide support for analyzing unknown protocol formats.

In the paper "Ripple+: An Improved Scheme of Ripple Consensus Protocol in Deployability, Liveness and Timing Assumption", Ma et al. [3] present Ripple+ to improve Ripple from three aspects: (1) Ripple+ employs a specific trust model to make it easy to deploy; (2) the primary and view change mechanism are joined to solve the liveness problem; (3) they improve details to make it suitable for weak synchrony assumption.

In the paper "IDV: Internet Domain Name Verification Based on Blockchain", Hu et al. [4] propose a new type of anonymous communication network, which adopts a software-defined architecture to improve the programmability of the network, and adopts blockchain technology to solve the security

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

problem of the control plane. While retaining the security of anonymous communication networks, the programmability and reliability of anonymous communication networks are improved.

The fifth paper "A Deletable and Modifiable Blockchain Scheme Based on Record Verification Trees and the Multisignature Mechanism" by Han et al. [5], presents a deletable and modifiable blockchain scheme (DMBlockChain) based on record verification trees (RVTrees) and the multi-signature scheme.

In the paper "An Adversarial Smart Contract Honeypot in Ethereum", Han et al. [6] propose a type of adversarial honeypot that hides the detectable features in terms of the code and behavior of the original honeypot, which achieves a 100% ratio of bypassing the advanced detection technologies.

In the paper "Attribute-based Keyword Search over Encrypted Blockchains", Yang et al. [7] propose an attribute-based keyword search scheme on blockchain, which allows users to search encrypted files over the blockchain based on their attributes. In addition, they build a file chain structure to improve the efficiency of searching files with the same keyword.

Shen et al. [8], in their paper "Mining Bytecode Features of Smart Contracts to Detect Ponzi Scheme on Blockchain" propose a detection model for detecting Ponzi schemes in smart contracts using bytecode. Experimental results show that the proposed detection model can greatly improve the accuracy of the detection of the Ponzi scheme contracts.

In the last paper "Stereo Matching Method Based on Space-Aware Network Model", Bian et al. [9] propose to use the space-aware network to calculate the matching cost and further improve the network performance.

Acknowledgement: We would like to thank the authors for their contributions to this Special Issue. We also thank the journal of CMES for their supports for publications of this Special Issue.

Funding Statement: This editorial work was partially supported by Key-Area Research and Development Program of Guangdong Province 2020B0101090003.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Chen, J., Zhang, C., Yan, Y., Liu, Y. (2022). FileWallet: A file management system based on IPFS and Hyperledger fabric. *Computer Modeling in Engineering & Sciences, 130(2),* 949–966. DOI 10.32604/cmes.2022.017516.
2. Shi, J., Ye, L., Li, Z., Zhan, D. (2022). Unsupervised binary protocol clustering based on maximum sequential patterns. *Computer Modeling in Engineering & Sciences, 130(1),* 483–498. DOI 10.32604/cmes.2022.017467.
3. Ma, C., Zhang, Y., Fang, B., Zhang, H., Jin, Y. et al. (2022). Ripple+: An improved scheme of ripple consensus protocol in deployability, liveness and timing assumption. *Computer Modeling in Engineering & Sciences, 130(1),* 463–481. DOI 10.32604/cmes.2022.016838.
4. Hu, N., Teng, Y., Zhao, Y., Yin, S., Zhao, Y. (2021). IDV: Internet domain name verification based on blockchain. *Computer Modeling in Engineering & Sciences, 129(1),* 299–322. DOI 10.32604/cmes.2021.016839.
5. Han, D., Chen, J., Zhang, L., Shen, Y., Gao, Y. et al. (2021). A deletable and modifiable blockchain scheme based on record verification trees and the multisignature mechanism. *Computer Modeling in Engineering & Sciences, 128(1),* 223–245. DOI 10.32604/cmes.2021.016000.

6. Han, Y., Ji, T., Wang, Z., Liu, H., Jiang, H. et al. (2021). An adversarial smart contract honeypot in Ethereum. *Computer Modeling in Engineering & Sciences, 128(1),* 247–267. DOI 10.32604/cmes.2021.015809.
7. Yang, Z., Zhang, H., Yu, H., Li, Z., Zhu, B. et al. (2021). Attribute-based keyword search over the encrypted blockchain. *Computer Modeling in Engineering & Sciences, 128(1),* 269–282. DOI 10.32604/cmes.2021.015210.
8. Shen, X., Jiang, S., Zhang, L. (2021). Mining bytecode features of smart contracts to detect ponzi scheme on blockchain. *Computer Modeling in Engineering & Sciences, 127(3),* 1069–1085. DOI 10.32604/cmes.2021.015736.
9. Bian, J., Li, J. (2021). Stereo matching method based on space-aware network model. *Computer Modeling in Engineering & Sciences, 127(1),* 175–189. DOI 10.32604/cmes.2021.014635.