International Journal of Information Security (2020) 19:243–244
https://doi.org/10.1007/s10207-020-00496-6

EDITORIAL

Special issue on security and privacy of blockchain technologies

Kuo-Hui Yeh[1] · Chunhua Su[2] · Robert H. Deng[3] · Moti Yung[4] · Miroslaw Kutylowski[5]

Published online: 21 April 2020

Blockchain technology is perceived as one of the most promising techniques with its characteristics of decentralization, openness, and tamper resistance. Numerous studies have investigated blockchain technologies for specific application domains, such as Internet of Things, cyber-physical systems, edge computing, social networking, and even more other fields. However, there are neither consensus regarding their integration nor agreed-upon best practices exist for applying blockchain technology with robust security and privacy on these application domains. Therefore, this special issue invites original research that investigates state-of-the-art solutions for secure and privacy-aware blockchain technologies as well as novel blockchain-based applications with robust security and privacy.

In this special issue of International Journal of Information Security, we have two papers selected from the 2018 IEEE Conference on Dependable and Secure Computing (DSC 2018) and five papers from the Open Call-for-Papers. Note that the two papers from DSC 2018 are substantially extended, with at least 40% difference from its conference version.

In the first DSC 2018 paper, entitled *Secure Hierarchical Bitcoin Wallet Scheme Against Privilege Escalation Attacks*, in a Bitcoin-oriented environment Fan et al. propose a novel hierarchical deterministic (HD) wallet scheme that gives out a signature with trapdoor hash functions instead of directly giving private keys for signing. The proposed scheme can provide unlinkability between two public keys to achieve anonymity of user identities and high scalability to the derivations of huge amount of keys. In addition, the proposed scheme can prevent from privilege escalation attacks by concealing private keys from any child nodes in the hierarchical management manner.

In the second DSC 2018 paper, entitled *An Over-the-Blockchain Firmware Update Framework for IoT Devices*, Yohan and Lo propose a secure and verifiable blockchain-based firmware update framework for IoT environment. The proposed framework consists of a secure peer-to-peer verification mechanism on each new version of firmware released by corresponding device manufacturer, and a reliable management scheme to distribute the updated firmware to IoT devices in timely manner. Furthermore, the proposed framework utilizes the blockchain technology to ensure the integrity of firmware during its distribution through Internet.

In the paper, entitled *Enhancing Challenge-based Collaborative Intrusion Detection Networks against Insider Attacks using Blockchain*, Meng et al. propose a blockchain-based approach to help enhance the robustness ofchallenge-based collaborative intrusion detection networks (CIDNs) against advanced insider attacks like passive message fingerprint attack (PMFA), through integrating a type of blockchain-based trust. To evaluate the practicability of the proposed scheme, the authors examine the approach in both simulated and real network environments. The results demonstrate that the proposed approach is effective in defeating advanced insider attacks like PMFA and enhancing the robustness of challenge-based CIDNs.

In the paper, entitled *On the Insecurity of Quantum Bitcoin Mining*, Or Sattath argues that a crucial argument in the analysis of Bitcoin security breaks down when quantum mining is performed. Several facts (and arguments) are established: (i) There is strong evidence to suggest that, under current Bitcoin rules, quantum mining would cause a high stale rate. (ii) The author demonstrates a simple countermeasure prevent-

✉ Kuo-Hui Yeh
khyeh@gms.ndhu.edu.tw

Chunhua Su
chsu@u-aizu.ac.jp

Robert H. Deng
robertdeng@smu.edu.sg

Moti Yung
moti@cs.columbia.edu

Miroslaw Kutylowski
Miroslaw.Kutylowski@pwr.edu.pl

[1] National Dong Hwa University, Shoufeng, Taiwan

[2] University of Aizu, Aizuwakamatsu, Japan

[3] Singapore Management University, Singapore, Singapore

[4] Columbia University, New York, USA

[5] Wroclaw University of Technology, Wrocław, Poland

ing the high stale rate by prohibiting the AQMS. (iii) Unlike the classical setting, it is not clear what strategy should be suggested as the default (honest) behavior for quantumminers and, more specifically, how many Grover iterations they should apply with our countermeasure.

In the paper, entitled *An Improved FOO Voting Scheme Using Blockchain*, Zhou et al. propose an improved FOO e-voting protocol with blockchain to deal with the limitation, i.e. distrust to the center issue and the fairness and correctness of the vote issues, in the traditional FOO e-voting protocols. In the proposed protocol, the traditional trusted third party is replaced by smart contract, and the architecture is deployed with hyperledger fabric. With a real implementation, the proposed scheme is proved to satisfy the necessary requirements for an e-voting protocol; meantime, the trust assumption is reduced significantly.

In the paper, entitled *Lockmix: A Secure and Privacy-preserving Mix Service for Bitcoin Anonymity*, Bao et al. propose a secure and privacy-preserving scheme in Bitcoin-based environment. The proposed Lockmix scheme introduces mix services for users to prevent attackers linking the input address with output address by using blind signature scheme, multi-signature scheme. Based on the analysis, the Lockmix scheme can provide anonymity, scalability, Bitcoin compatibility, theft impossibility and accountability. The authors have implemented the Lockmix scheme on Bitcoin test networks, and the experimental results show that the proposed scheme is efficient.

In the paper, entitled *Chaintegrity: Blockchain-Enabled Large-Scale E-voting System with Robustness and Universal Verifiability*, Zhang et al. propose a novel blockchain-enabled voting system, named chaintegrity, fulfilling the critical issues in terms of scalability, verifiability, and robustness. In addition, the proposed system adopts a hybrid data structure which combines the counting bloom filter and the Merkle hash tree for fast authentication. A code-voting technique is also introduced to enhance robustness. Based on the analysis, the authors have demonstrated that the proposed system achieves high efficiency and enjoys low computational and communication overhead.

We are grateful to all the authors who submitted their research articles to our special issue. We highly appreciate the contributions of the reviewers for their constructive comments and suggestions. We also would like to acknowledge the guidance from the Editors-in-Chief, i.e. Dieter Gollmann, Javier Lopez, Masahiro Mambo, and staff members of International Journal of Information Security.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.