Guest Editorial: Cryptography for Secure Blockchain

Chien-Ming Chen, Kuo-Hui Yeh, Lyes Khoukhi, Chan Yeob Yeun*

Cryptographic primitives gave rise to the concept of blockchain. Blockchain underpins various cryptocurrencies and non-centralized ledger-based transactional infrastructures, which have been deployed in applications such as finance, electronic health care, legal relations, IoT, information security, signature-based smart contracts and consensus-building systems. There is a need for suitable cryptographic approaches to fulfill the existing gaps in blockchain technology. For example, fulfillment of a certain equilibrium-based consensus algorithm is undoubtedly considered as a new and disruptive technology that will shape the future of e-Commerce. On the one hand, security and trust are detrimental factors for the energy-demanding Proof(s) of Work (consensus). On the other hand, maintaining Cyber resilience through NP-hard problems is a challenging task. State-of-the-art of cryptographic techniques being deployed so far in the blockchain systems needs to be investigated as these techniques are fundamental building blocks to provide security to the blockchain. A thorough Systematization of Knowledge that offers a complete bibliographic survey of the full crypto functionalities, tools, and interactions inside the blockchain, is imperative. There is an urgent need to realize and understand the security limitations, efficacy, and performance of various types of blockchain-enabled protocols. Considering the above issues, there is a wide scope to improve the robustness of blockchain and hence utilize the blockchain for various applications.

The main goal of this special issue is to invite researchers to publish selected original manuscripts to address the above concerns. Eventually, this special issue collects three outstanding papers.

The first paper, entitled "Blockchain-Oriented Data Exchange Protocol with Traceability and Revocation for Smart Grid" by Prince Silas Kwesi Oberko, Tianang Yao, Hu Xiong, Saru Kumari, and Sachin Kumar, presents an Ethereum blockchain-oriented secured access regulation design that upholds traceability and revocability for smart grids. A refined ciphertext-policy secured access regulation built on blockchain engineering is introduced. The blockchain implements unified identity verification and saves all public keys, users' attribute sets, and revocable lists. A distinctive identification parameter is generated and implanted during the private-key formation stage to detect and thwart collusion attacks. Any user with attributes fulfilling the access policy and not on the revocable list can successfully compute the decryption key. Malevolent users would then be traced per the tracing record and revoked directly. Authors claimed that their experiments show that the proposed scheme preserves the privacy of users, is highly secure, and is efficient in terms of the public/private keys being shorter and the overhead duration being less for generating the public key, data encryption, and decryption phases.

The second paper, entitled "IoETTS: A Decentralized Blockchain-based Trusted Time-stamping Scheme for Internet of Energy" by Bin Qian, Yi Luo, Jiaxiang Ou, Yong Xiao, and Houpeng Hu proposes a novel scheme for trusted time-stamping of energy data in the Internet of Energy (IoE) applications. The proposed scheme, IoETTS, is based on a decentralized approach that eliminates the need for a trusted third party. By leveraging the immutable nature of blockchain, IoETTS ensures the integrity and authenticity of energy data by time-stamping it and storing it on the blockchain. The authors present experimental results that demonstrate the effectiveness and practicality of the proposed scheme, which eliminates the need for a trusted third party and is able to provide efficient and reliable time-stamping services for a wide range of energy applications.

The third paper, entitled "On The Impossibility of Providing Strong Anonymity in Blockchains via Linkable Ring Signatures" by Huang Zhang, Fangguo Zhang, and Ke Gu, presents a general attack to linkable ring signatures together with an analysis of how to implement it in a practical scenario. Such an attack implies a linkable ring signature with strong linkability cannot support strong anonymity even though this type of signature is widely used in blockchain systems. The main observation is if a scheme is strongly linkable, then the information of a secret key is always strongly binding in the linking tag. Consequently, even if one can design a scheme in which the secret key, handled by the true signer, cannot be computed from the public key by a resource-unbounded adversary, the denying attack in this paper still works. The other members of the signature could sign a signature with a different linking tag, but the true signer cannot. Hence, they could collude to expose the true signer so that strong anonymity is impossible. The paper is interesting, and the authors also suggested a method to avoid the denying attack in blockchain systems, which is based on breaking the necessary conditions for launching the attack.

We are confident that every paper included in this Special Issue will significantly impact future scientific research and contribute to the work of researchers, engineers, and practitioners alike. We would like to sincerely thank all authors for their valuable contributions and hard work. We would also like to extend a special thank you to Professor Han-Chieh Chao, Editor-in-Chief of the Journal of Internet Technology (JIT), for granting us the opportunity to publish

*Corresponding Author: Kuo-Hui Yeh; E-mail: khyeh@gms.ndhu.edu.tw

this Special Issue and for providing unwavering support throughout the entire publication process.

References

[1] P. S. K. Oberko, T. Yao, H. Xiong, S. Kumari, S. Kumar, Blockchain-Oriented Data Exchange Protocol With Traceability and Revocation for Smart Grid, *Journal of Internet of Technology*, Vol. 24, No. 2, pp. 509-518, March, 2023.

[2] B. Qian, Y. Luo, J. Ou, Y. Xiao, H. Hu, IoETTS: A Decentralized Blockchain-based Trusted Time-stamping Scheme for Internet of Energy, *Journal of Internet of Technology*, Vol. 24, No. 2, pp. 519-529, March, 2023.

[3] H. Zhang, F. Zhang, K. Gu, On The Impossibility of Providing Strong Anonymity in Blockchains via Linkable Ring Signatures, *Journal of Internet of Technology*, Vol. 24, No. 2, pp. 531-538, March, 2023.

Guest Editors

Chien-Ming Chen received the Ph.D. degree from National Tsing Hua University, Taiwan. He is currently an Associate Professor of Nanjing University of Information Science and Technology, Nanjing, China. He has published more than 200 research papers in refereed journals and international conferences, including 140 publications in SCI-Indexed Journals. His current research interests include network security, the mobile Internet, the IoT, and cryptography. Dr. Chen serves as an Associate Editor/Academic Editor/Executive Editor for at least seven journals. He is a Senior Member of IEEE. E-mail: chienmingchen@ieee.org

Kuo-Hui Yeh (SM'16) is a full Professor with the department of Information Management, National Dong Hwa University, Hualien, Taiwan. He received M.S. and Ph.D. degrees in Information Management from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2005 and 2010, respectively. Dr. Yeh's research interests include IoT security, Blockchain, mobile security, NFC/RFID security, authentication, digital signature, data privacy and network security. He is currently an Associate/Academic Editor of HCIS, JISA, Symmetry, SCN, MISY, JIT, JSSS and Foundations. In addition, Dr. Yeh has served as a TPC member for 50 international conferences/workshops on information security as well as holds CISSP, CISM, Security+, ISO 27001/27701 LA, IEC 62443-2-1 LA and ISA/IEC 62443 Cybersecurity Fundamentals/Risk Assessment Specialist certificates. E-mail: khyeh@gms.ndhu.edu.tw

Lyes Khoukhi is Full Professor of cybersecurity at ENSICAEN, Normandie University, with GREYC CNRS UMR lab, Caen, France. He received the Ph.D degree in computer engineering from the University of Sherbrooke, Canada, in 2006. His research interests include attacks detection and prediction and malicious behaviors modeling. He is also the SIG leader of "Machine Learning for IoT and ad hoc networks" of the IoT ASHN ComSoc Committee of IEEE Communications Society since 2020. E-mail: lyes.khoukhi@ensicaen.fr

Chan Yeob Yeun received the M.Sc. and Ph.D. degrees in information security from Royal Holloway, University of London, in 1996 and 2000, respectively. He is currently a Researcher in cybersecurity, including the IoT/USN security, cyber-physical system security, cloud/fog security, and cryptographic techniques, an Associate Professor with the Department of Electrical Engineering and Computer Science, and the Cybersecurity Leader of the Center for Cyber-Physical Systems (C2PS). He also enjoys lecturing for M.Sc. degree in cyber security and Ph.D. degree in engineering courses at Khalifa University. He has published more than 140 journal articles and conference papers, nine book chapters, and ten international patent applications. He also works on the editorial board of multiple international journals and on the steering committee of international conferences. E-mail: chan.yeun@ku.ac.ae