symmetry

MDPI

Editorial

Special Issue Editorial "Blockchain-Enabled Technology for IoT Security, Privacy and Trust"

Kuo-Hui Yeh [1,2], Chunhua Su [3] and Shi-Cho Cha [4,*]

[1] Department of Information Management, National Dong Hwa University, Hualien 974301, Taiwan; khyeh@gms.ndhu.edu.tw
[2] Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 804201, Taiwan
[3] Department of Computer Science and Engineering, The University of Aizu, Fukushima 965-0006, Japan; chsu@u-aizu.ac.jp
[4] Department of Information Management, National Taiwan University of Science and Technology, Taipei 106335, Taiwan
* Correspondence: csc@mail.ntust.edu.tw

check for updates

Citation: Yeh, K.-H.; Su, C.; Cha, S.-C. Special Issue Editorial "Blockchain-Enabled Technology for IoT Security, Privacy and Trust". *Symmetry* **2023**, *15*, 1059. https://doi.org/10.3390/sym15051059

Received: 3 April 2023
Accepted: 3 April 2023
Published: 10 May 2023

The Internet of Things (IoT) is an emerging paradigm, seamlessly integrating a great quantity of smart objects that are connected to the Internet. With the rise in interest regarding IoT, the research community and industry must devote further attention to overcoming related trust, security and privacy challenges, to unleash the full potential of IoT. The industry has introduced a variety of technologies for IoT security, privacy, and trust, such as trust management, data confidentiality, authentication and authorization, secure communication and computation, and individual privacy protection. Recently, blockchain technology has been perceived as a promising solution for the management of distributed IoT devices because it has the characteristics of decentralization, openness and tamper-resistance. Although numerous studies have addressed various applications of blockchain technology in the IoT, there is neither consensus regarding their integration nor agreed-upon best practices for applying blockchain technology in the IoT with robust security and privacy. As things stand, employing blockchain technologies in the IoT is still particularly challenging. Hence, in this Special Issue, we invite original research that investigates blockchain-enabled technologies involving the concept of symmetry for IoT security, privacy, and trust. Eventually, after a rigorous peer-review process, we choose five high-quality pieces of research to be published in this Special Issue:

1. Building Trusted Federated Learning on Blockchain (belongs to the topic of trust management for blockchain technology in the IoT).
2. Toward Data Integrity Architecture for Cloud-Based AI Systems (belongs to the topic of blockchain-based applications for IoT security and privacy).
3. Trusting Testcases Using Blockchain-Based Repository Approach (belongs to the topic of trust management for blockchain technology in the IoT).
4. Revisited—The Subliminal Channel in Blockchain and Its Application to IoT Security (belongs to the topic of new cryptographic algorithms for blockchain technology in the IoT).
5. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model (belongs to the topic of fraud detection and forensics for blockchain technology in the IoT).

First, in the paper "Building Trusted Federated Learning on Blockchain" [1], Oktian et al. adopted the blockchain technology as a trusted federated learning platform for the vanilla-federated learning (VFL) model. To support the assumed trusted running environment of the VFL model, the authors first designed an integrated solution consisting of an incentive mechanism, reputation system, peer-reviewed model, commitment hash

and model encryption. Based on the designed conceptual solution, the authors then implemented a full-fledged blockchain-based federated learning protocol, including client registration, training, aggregation and reward distribution. To guarantee the reliability and feasibility of the proposed protocol, evaluations were delivered in which the proposed system was shown to successfully motivate participants to be honest and perform best-effort training to obtain higher rewards. Second, in the paper "Toward Data Integrity Architecture for Cloud-Based AI Systems" [2], Witanto et al. investigated the potential cybersecurity risks of Artificial Intelligence (AI)-based computing architecture operated with modern innovative technologies, such as Cloud computing and Blockchain. The authors claimed that compromised training data integrity during model training indicates a compromised the AI-based application system. Thus, it is indispensable to guarantee data integrity when data training in AI systems. For this reason, the authors presented a data integrity scheme guided by the National Institute of Standards and Technology (NIST) cybersecurity framework. The natural characteristics, i.e., a shared and decentralized communication, of blockchain make it suitable to overcome the data integrity issue. The authors thus utilized the smart contracts technique to guarantee resistance against data forgery and ensure automatic policy enforcement and data integrity. The proposed solution can fulfill the NIST cybersecurity framework requirements and ensure continuous and consistent data integrity.

The Internet of Vehicles (IoV) domain has concentrated on supporting connected and self-driving capabilities, including connected driving, cooperative driving, and intelligent transportation systems While this innovation increases conveniences, it has subsequently created new information security risks such as software bugs and vulnerable remote updates. Hence, in the paper "Trusting Testcases Using Blockchain-Based Repository Approach" [3], Zaabi et al. proposed a blockchain-based approach as a trusted testcase repository to support test-based software and security testing. A new concept, called Proof-of-Validation, is proposed as a non-incentivized consensuses mechanism with global state information, which can be used to manage updates to the repository under the adoption of test suite provided by Linux Test Project (LTP). Every node of the blockchain can contribute to the validation of testcases once they are either selected by other peers or have successfulky created and added blocks to the public ledger of the blockchain platform. Next, in the paper "Revisited—The Subliminal Channel in Blockchain and Its Application to IoT Security" [4], Chen et al. enhanced the security of blockchain using a novel subliminal channel concept. The authors first revisited the subliminal channel corresponding to some existing digital signatures and then reviewed its potential risk regarding abuse of the constructor's private key. A concept named the chamber of secrets is proposed for blockchains, whereby a secret may be hidden and later recovered by the constructor from the common transactions in a blockchain. Two benefits of their proposed solution are then provided: (1) avoiding the high maintenance cost of the chain with certificated authority or a public key infrastructure, and (2) seamlessly integration with blockchains using the chamber of secrets property. Finally, in the paper "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model" [5], Steingartner et al. explored the possibility of using cyber deception to design a novel conceptual model of hybrid threats' analysis. The authors first investigated the current state of the art in deception technology and provide an overview of detection as a powerful support when creating an active defense. A novel hybrid threats model is then presented, in which several concepts, i.e., corruption, critical information infrastructure, criminal elements, social, subversion/terrorism, information operations, politics, ideology, cyber threat, intelligence activities, civic clubs, and the economic and physical environment, are introduced. In addition, the authors suggested military education in detecting, identifying, and responding to cybersecurity threats. An important claim, that deception should be used strategically to stop advanced attackers, is argued.

The Guest Editors, i.e., Kuo-Hui Yeh, Chunhua Su and Shi-Cho Cha, hope that this Special Issue will benefit the scientific community and contribute to the extant knowledge

base and would like to thank the authors for their contributions. In addition, we highly appreciate the constructive comments and suggestions of the reviewers. Finally, the Guest Editors would like to acknowledge the guidance from *Symmetry's* Editor-in-Chief and other staff members.

Author Contributions: K.-H.Y., C.S. and S.-C.C., are responsible for the organization, promotion and manuscript processing of this special issue. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Science and Technology Council, Taiwan under Grants NSTC 111-2221-E-259-006-MY3, NSTC 111-2218-E-011-012-MBK, NSTC 111-2926-I-259-501 and NSTC 110-2634-F-A49-004.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Oktian, Y.E.; Stanley, B.; Lee, S.-G. Building Trusted Federated Learning on Blockchain. *Symmetry* **2022**, *14*, 1407. [CrossRef]
2. Witanto, E.N.; Oktian, Y.E.; Lee, S.-G. Toward Data Integrity Architecture for Cloud-Based AI Systems. *Symmetry* **2022**, *14*, 273. [CrossRef]
3. Al Zaabi, A.; Yeun, C.Y.; Damiani, E. Trusting Testcases Using Blockchain-Based Repository Approach. *Symmetry* **2021**, *13*, 2024. [CrossRef]
4. Chen, T.-H.; Lee, W.-B.; Chen, H.-B.; Wang, C.-L. Revisited—The Subliminal Channel in Blockchain and Its Application to IoT Security. *Symmetry* **2021**, *13*, 855. [CrossRef]
5. Steingartner, W.; Galinec, D.; Kozina, A. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. *Symmetry* **2021**, *13*, 597. [CrossRef]