This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2966068, IEEE Transactions on Industrial Informatics



# Blockchain in Industrial IoT Applications: Security and Privacy Advances, Challenges and Opportunities

Kim-Kwang Raymond Choo, *Senior Member, IEEE*, Zheng Yan, *Senior Member, IEEE*, and Weizhi Meng

***Abstract* — Is Blockchain a hype or a trend that is here to stay? Based on the increasing interest of blockchain in industry, governments and academia, one might tend to be inclined to think that blockchain has moved beyond a hype and a buzzword to something that is here to stay, somewhat analogous to cloud computing and Internet of Things (IoT) in their early days. While there are many (potential) applications of blockchain including in industrial IoT (IIoT), there are a number of ongoing challenges. In this special issue, we present existing state-of-the-art advances reported by the nine accepted papers. We then conclude the special issue with a number of potential research agenda.**

***Index Terms*— Blockchain Security, Blockchain Privacy, Industrial Internet of Things Security, Industrial Internet of Things Privacy**

## I. Introduction

Blockchain is an emerging technology that has widespread applications, such as those relating to Internet of Things (IoT) and Industrial IoT (IIoT). The interest in exploring the application of Blockchain in the many different domains is partly because of its capability to offer transparent and integrity properties (e.g., due to the underlying consensus mechanism), where recorded data in any given block cannot be modified retroactively without modifying all subsequent blocks. Other applications of blockchain include the secure and efficient tracking and managing of digital identities to facilitate seamless sign-on. Blockchain-based authentication systems are generally based on irrefutable identity verification using digital signatures, based on public key cryptography. In blockchain identity authentication, the only check performed is to determine whether the transaction was signed by the correct private key.

While there are many (potential) applications of blockchain in IIoT (the focus of this special issue), there are a number of ongoing challenges. For example, blockchain technology provides a solution to ensure a trust relationship without a centralized entity. However, such technology is still under development and suffers from a number of limitations and challenges during implementation, such as computational costs (e.g., mining), security (e.g., attacks such as distributed denial-of-service – DDoS attacks, and theft of content). In an IIoT application, such as smart cities, Industry 4.0 and in military and battlefield context (also referred to as Internet of Battlefield Things (IoBT) and Internet of Military Things (IoMT)), there are more factors that need to be taken into consideration in the design of blockchain-based solutions.

Therefore, in the next five sections we will describe the advances presented in the papers accepted in this special issue, designed to address different security and privacy challenges associated with the deployment of blockchain-based solutions in an IIoT setting.

## II. Smart Transportation

Given the popularity of smart cities, it is not surprising that a number of submissions to this special issue focused on the various systems that underpin a smart city, such as smart transportation systems and vehicular networks.

Seeking to improve urban traffic condition, Chen, Xiao, Qiu, Lv, and Pei [1] designed a selection scheme that can be used to provide an incentive (based on cryptocurrency) for participating vehicles to act as the cluster head (referred to as a platoon head in the paper). The latter is also tasked with the dynamic update of the respective platoons.

Feng, He, Zeadally, and Liang [5] explored the utility of blockchain in a Vehicular Ad-Hoc Network (VANET) setting. Specifically, the authors proposed a blockchain-assisted privacy-preserving authentication system (BPAS) to allow one to transmit messages securely without relying on any centralized third-party.

## III. Crowdsourcing

Crowdsourcing is a concept that is increasingly prevalent, and is related to concepts such as sharing economy. For

K.-K.R. Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA (e-mail: raymond.choo@fulbrightmail.org).

Z. Yan is with the State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, China. She is also with the Department of Communications and Networking, Aalto University, Finland. (Email: zheng.yan@aalto.fi)

W. Meng is with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Lyngby, Denmark (Email: weme@dtu.dk).

1551-3203 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2966068, IEEE Transactions on Industrial Informatics



example, the World Economic Forum [1] classified crowdsourcing as one of the economic models powered by the crowd, and sharing economy as the sharing of underutilized assets with the aims of improving efficiency, sustainability and community wellbeing. However, similar to other IIoT applications there are underpinning security and privacy considerations [12, 13]. For example, Zhu, Cai, Hu, Li, and Li [10] proposed a blockchain-based crowdsourcing platform, which comprises a hybrid blockchain structure, smart contract, dual ledgers, and dual consensus protocols. The platform is designed to facilitate secure communications, verification of transactions, and privacy preserving features.

Zou, Xi, Wang, and Xu [11] also highlighted the importance of ensuring quality of crowdsourced data. Specifically, they focused on crowdsensing data quality and its location privacy, and presented a blockchain-based location privacy-preserving crowdsensing model.

## IV. Data Sharing

The need for secure and privacy-preserving data(set) sharing is increasingly important in our big data-era [4], and this is also reinforced by Lu, Huang, Dai, Maharjan, and Zhang [8]. The authors presented a blockchain-based data sharing architecture for distributed multiple parties. To ensure the privacy of the shared data, the authors integrated federated learning in the consensus process of the underpinning permissioned blockchain.

## V. Edge Computing

There have been attempts to mitigate some of the limitations in a cloud computing deployment by moving the computational resources closer to the edge of the network (i.e., edge computing). Hence, it is no surprise that there have been attempts to utilize blockchain-based solutions in an edge computing environment.

Xu, Zhang, Gao, Xue, Qi, and Dou [9] designed a blockchain-enabled computation offloading method, which can be deployed in an edge computing setting to ensure data integrity.

Gai, Wu, Zhu, Zhang, and Qiu [6] proposed a blockchain-based Internet-of-Edge model, in order to provide for a scalable and controllable IoT system. The authors also explored the potential of using such a model to achieve privacy-preserving feature.

## VI. General IIoT Applications

Not all technical solutions need to be domain-specific, as demonstrated by Kurte, Salcicy, and Wang [7], and Cui, Yang, Chen, Pan, Xu, and Xu [3].

In the first paper [7], the authors presented an open-source platform that is designed to support the specification and provision of trustworthy and privacy preserving distributed applications, such as blockchain, in an IoT and IIoT context.

In the second paper [3], the authors presented a blockchain protocol, based on compacted directed acyclic graph, and a related IIoT architecture to improve the efficiency of typical IIoT systems.

## VII. Future Work

While the research presented in this special issue contributed to improving Blockchain security and privacy in IIoT applications, there are many more research challenges and opportunities, partly due to the constant evolution of the technologies underpinning Blockchain, IIoT and our cyber threat landscape. Potential research agenda include:

- Theories underpinning Blockchain and IIoT security and privacy
- Distributed consensus and fault tolerance mechanisms
- Blockchain schemes for decentralization
- Blockchain for trust management and trusted computing
- Security, privacy, trust and performance optimization of blockchain and decentralized schemes
- Blockchain-based IIoT applications
- Lightweight protocols and algorithms based on blockchain
- Blockchain based lightweight data structures for IoT data
- IIoT and cyber physical systems
- Blockchain in crowdsourcing and crowdsensing
- Blockchain and IIoT in 5G, edge and cloud computing, and trust management
- Vulnerability identification and exploitation of Blockchain and IIoT

One observation we made in this special issue is that the proposed solutions either used simulations and/or a laboratory-based testbed to evaluate the performance of the schemes. As posited in a previous editorial published in this same journal two years ago [2], it is important to bridge research and practice, such as designing secure yet real-world efficient technical solutions, for example by establishing public-private partnerships in the collaborative design, development and evaluation of future solutions.

## References

[1] Chen Chen, Tingting Xiao, Tie Qiu, Ning Lv, and Qingqi Pei. Smart-Contract based Economical Platooning in Blockchain Enabled Urban Internet of Vehicles. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2954213]

[2] Kim-Kwang Raymond Choo, Stefanos Gritzalis, and Jong Hyuk Park. Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities. IEEE Trans. Industrial Informatics 14(8): 3567-3569 (2018)

[3] Laizhong Cui, Shu Yang, Ziteng Chen, Yi Pan, Mingwei Xu, and Ke Xu. An Efficient and Compacted DAG-based Blockchain Protocol for Industrial Internet of Things. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2931157]

[4] Weiqi Dai, Chunkai Dai, Kim-Kwang Raymond Choo, Changze Cui, Deqing Zou, and Hai Jin. SDTE: A Secure Blockchain-Based Data Trading Ecosystem. IEEE Trans. Information Forensics and Security 15: 725-737 (2020)

[1] https://www.weforum.org/agenda/2017/12/when-is-sharing-not-really-sharing/ (last accessed Jan 6, 2020)

1551-3203 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2966068, IEEE Transactions on Industrial Informatics



[5] Qi Feng, Debiao He, Sherali Zeadally, and Kaitai Liang. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad-Hoc Networks. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2948053]

[6] Keke Gai, Yulu Wu, Liehuang Zhu, Zijian Zhang, and Meikang Qiu Differential Privacy-based Blockchain for Industrial Internet of Things. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2948094]

[7] Ryan Kurte, Zoran Salcicy, and Kevin I-Kai Wang. A Distributed Service Framework for the Internet of Things. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2948046]

[8] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. Blockchain and Federated Learning for Privacy-preserved Data Sharing in Industrial IoT. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2942190]

[9] Xiaolong Xu, Xuyun Zhang, Honghao Gao, Yuan Xue, Lianyong Qi, and Wanchun Dou. BeCome: Blockchain-Enabled Computation Offloading for IoT in Mobile Edge Computing. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2936869]

[10] Saide Zhu, Zhipeng Cai, Huafu Hu, Yingshu Li, and Wei Li. zkCrowd: A Hybrid Blockchain-based Crowdsourcing Platform. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2941735]

[11] Shihong Zou, Jinwen Xi, Honggang Wang, and Guoai Xu. CrowdBLPS: A Blockchain-based Location Privacy-Preserving Mobile Crowdsensing System. IEEE Trans. Industrial Informatics [In press; https://doi.org/10.1109/TII.2019.2957791]

[12] Wei Feng, Zheng Yan, Hengrun Zhang, Kai Zeng, Yu Xiao, and Thomas Y. Hou. A Survey on Security, Privacy and Trust in Mobile Crowdsourcing. IEEE Internet of Things Journal, Vol. 5 No. 4, pp. 2971-2992, August 2018.

[13] Wei Feng, and Zheng Yan. MCS-Chain: Decentralized and Trustworthy Mobile Crowdsourcing Based on Blockchain. Future Generation Computer Systems, Vol. 95, pp. 649-666, June 2019.

1551-3203 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.