Theme Article:
Innovations Using Blockchain—Part 2

# The Convergence of IoE and Blockchain: Security Challenges

**Lijun Wei**
Shanghai Jiao Tong University

**Chengnian Long**
Shanghai Jiao Tong University

**Jing Wu**
Shanghai Jiao Tong University

**Yi-Bing Lin**
National Chiao Tung University

***Abstract*—To build a large-scale distributed Internet of Things (IoT), a feasible prototype for Internet of Everything, blockchain can provide strong support with its excellent characteristics such as traceability and openness. Despite that the blockchain technology ideally enhances the reliability and security of IoT systems, emerging new security challenges remain to be resolved. This article details the security vulnerabilities in the convergence of blockchain and IoT as well as corresponding feasible solutions.**

**As a worldwide** network structure, Internet of Things (IoT) paradigm integrates numerous heterogeneous objects and sensors that surround us and facilitates the information exchange among all participants (also referred to as nodes). With the continuous expansion of the network scale and the intelligent evolution of hardware devices, traditional isolated IoT solutions may no longer satisfy advanced requirements for security and efficiency, particularly in the setting of the high degree of heterogeneity of devices and complex data formats.

*Digital Object Identifier 10.1109/MITP.2019.2923602*
*Date of current version 11 September 2019.*

First, burdensome connectivity and maintenance costs brought by centralized architecture result in its low scalability. Second, centralized systems are more vulnerable to targeted attacks by adversaries under the network expansion.[1]

Intuitively, a decentralized approach based on blockchain (see Figure 1) may solve the above problems occurring in conventional centralized IoT. Roughly, there are three reasons. First, an autonomous decentralized system is feasible for trusted participants to join independently, which enhances the system's task-processing capability. Second, multiparty cooperation helps to guarantee the state consistency of nodes that system crash caused by a single-point failure



Published by the IEEE Computer Society

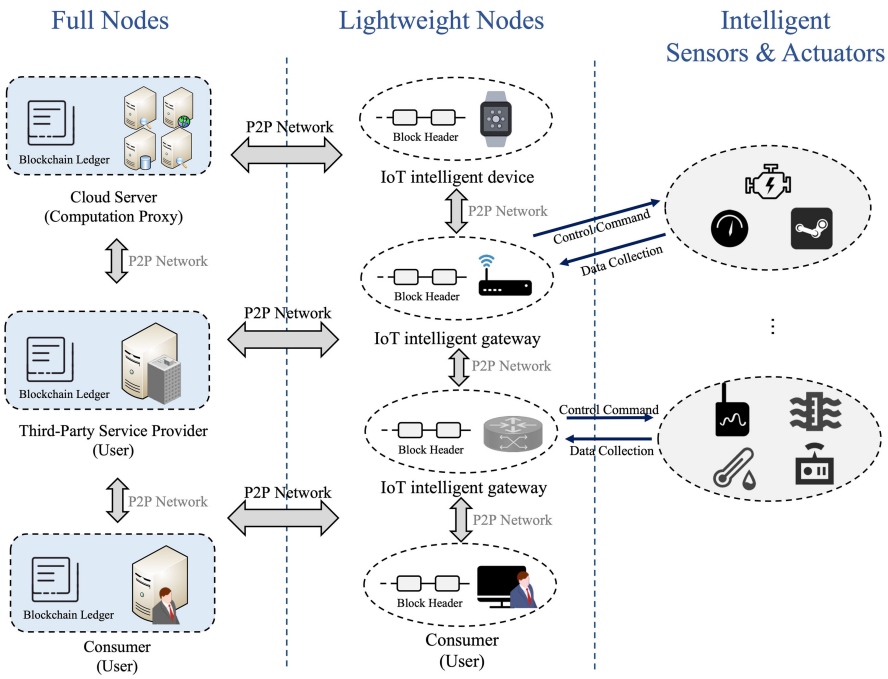


**Figure 1.** Distributed IoT architecture based on blockchain technology.

may be avoided. Third, nodes could synchronize the entire system state merely by copying the blockchain ledger to reduce the computational and storage load. Research in recent years also to some extent proved such advantages of the blockchain-based IoT architecture in various fields, for example, smart city and health care.[2]

In a blockchain-based system, nodes can be divided into two categories based on the difference in computing and storage capabilities, which are namely full nodes and lightweight nodes. The full node saves the entire distributed ledger and synchronizes all data in real time. The lightweight node only saves the block headers of distributed ledger, which serves to validate the transactions and deal with issues by querying neighbors. With the combination of 1) computing resources of both full nodes and lightweight nodes and 2) data collected by the intelligent sensing devices, the distributed IoT system can provide services to all users in the entire network.

Despite the potential of blockchain technology, certain serious security issues have been raised during its convergence with IoT.[3] Based on different attack types in classified layers, Table 1 presents an overview of challenges in system design and corresponding promising solutions.

This article particularly focuses on the following security concerns in designing distributed IoT:

1) communication and network security;
2) identity management and authentication;
3) reliable distributed consensus protocol;
4) decentralized cooperation and trust establishment;
5) transaction data privacy and security.

## COMMUNICATION AND NETWORK SECURITY

A distributed IoT pattern majorly applies the peer-to-peer (P2P) mode, which allows nodes to interact with each other autonomously without a central server platform. Within an open network environment, the P2P mode highly promotes the interpersonal collaboration. However, openness may lead to adverse consequences. By launching eavesdropping, node capture, or message spoofing, the adversary can successfully grab partial system data to compromise the stability of the IoT system.

Cryptographic algorithm is one of the key technologies to solve the above security problem. Highly recommended by the National Institute of Standards and Technology, the Elliptic Curve Digital Signature Algorithm (ECDSA) has great

**Table 1. Possible security risks of distributed IoT and promising solutions.**

| Layers | Attack Types | Challenges in System Design | Promising Solutions |
|---|---|---|---|
| Physical Layer | Physical damage<br>Jamming<br>Firmware replacement attack | Device connection<br>Device recovery<br>Condition monitoring of devices | State detection scheme<br>Data recovery mechanism |
| Network & Transport Layer | Eavesdropping<br>Information stealing | Cryptography algorithm for messages | Lightweight cryptography algorithm |
| | Message spoofing | Data privacy and security | Zero-knowledge proof<br>Homomorphic encryption technology access control |
| | Byzantine attack<br>Denial of service<br>Collusion | Consensus protocol | Hierarchical consensus protocol<br>Dynamic committee |
| Application Layer | Sybil attack<br>Identity forgery<br>Selfish attack | Identity management<br>Authentication and authorization<br>Admission control<br>Coalition and trust establishment | Lightweight authentication protocol based on lightweight cryptography algorithm<br>Customized smart contracts for admission<br>Reputation assessment model based on blockchain data |

advantages in network secure protocol.[4] Compared with the Rivest–Shamir–Adelman-based algorithm and other cryptographic algorithms, the elliptic curve cryptography (ECC)-based algorithm is more superior for its smaller calculation parameters, shorter key size, and faster operation.[5] Safety and reliability of the ECC-based algorithm have also been witnessed by its use in the blockchain platforms such as Bitcoin and Ethereum.

Nevertheless, a great deal of IoT sensing and smart devices are energy constrained and are of limited computation and storage capacity. Therefore, it remains uncertain whether ECDSA can indeed meet both the requirements on computational load and memory under the limitation of energy consumed. The study in the report by Liu[6] selected a family of lightweight elliptic curves, i.e., curves P159, P191, P223, and P255, and compared their security performance in IoT application at different security levels. Furthermore, in view of the limited-energy concern of IoT devices, the authors evaluated the energy consumption of each cryptographic algorithm based on the performance and communication cost between nodes and reached the conclusion that ECC-based algorithm can realize the balance between energy and memory consumption.

As discussed before, future tests and examinations need to put more emphasis on applying cryptographic algorithms to the real-world and complex IoT trial scenario. Specific characteristics of IoT devices must be considered when applying the lightweight cryptographic algorithm to IoT devices. Moreover, in the case of cyber attacks such as timing and replay attacks, we should verify whether the implementation can be resistant to such potential security risks.

## IDENTITY MANAGEMENT AND AUTHENTICATION

Public Key Infrastructures (PKIs) facilitate identity management and authentication in the IoT system. Currently, the most commonly engaged PKIs fall into two categories: certificate authorities (CAs) and web of trust based on pretty good privacy. However, since the increasing number of devices would require substantial computing and storage resources to realize the constant message exchange and identity authentication, these typical methods may not be able to meet the requirements of identity management in Internet of Everything (IoE). Moreover, due to the high degree of heterogeneity of IoT devices, the original blockchain platform that merely uses "address" to represent node cannot be well applied to IoT devices.

To address such challenges, a promising research idea is to combine the smart contract

**Table 2. Comparison of the different categories of consensus protocols.**

| Consensus Protocol | PoW | PoS | PoS+PoW | BFT-based | Raft-based | DPoS | Hybrid |
|---|---|---|---|---|---|---|---|
| **Prominent Platform** | Bitcoin Ethereum | Cardano Algorand | PPcoin Blackcoin | Hyperledger Tendermint | R3 Corda Tangaroa | Bitshare EOS | N/A |
| **System Type** | Permissionless | Permissionless | Permissionless | Permissioned | Permissioned | Permissioned | Permissionless |
| **Energy Consumption** | High | Low | Medium | Low | Low | Low | Low |
| **Block Confirmation** | Probabilistic | Probabilistic | Probabilistic | Deterministic | Deterministic | Deterministic | Deterministic |
| **Transaction Rate** | Low | Medium | Medium | High | High | High | High |
| **Committee Election** | N/A | Dynamic | Dynamic | Static | Static | Static | Dynamic |
| **Fault Tolerance** | $<=50\%$ | Unknown | Unknown | $<=33\%$ | N/A | Unknown | Unknown |
| **Anonymity** | High | Medium | Medium | Low | Low | Low | High |
| **Scalability** | Medium | Medium | Medium | Low | Low | High | High |
| **Openness** | High | Medium | Medium | Low | Low | Medium | High |
| **Fairness** | Medium | Medium | Medium | Low | Low | Low | Medium |

with lightweight encryption algorithms to automatically manage identities. When a new IoT device joins the network, we can implement the reliable identity management by designing dedicated smart contracts, including device registration (including device type, manufacturer, expiration date, public key, etc.), identity verification, information update (including firmware upgrade, expiration date, report of device loss, etc.), and device obsolescence.[7] Moreover, by synchronizing the data recorded in the blockchain, the full node can synchronize the state of identity-related smart contract to implement identity authentication. Similarly, after querying the full node, the lightweight node can effectively authenticate other IoT devices.

By exploiting the blockchain immutability and the automated execution of smart contracts, the decentralized identity management scheme not only prevents identity forgery but also reduces the cost of building trust compared to CA-based approaches in IoT system.

## RELIABLE DISTRIBUTED CONSENSUS PROTOCOL

To ensure the normal operation of the entire system in the P2P network, the distributed consensus protocol plays a critical role in affecting the security, scalability, and practicality. The Bitcoin platform employs the proof-of-work (PoW) protocol to solve the consensus problem, where the node calculates a hash puzzle to compete for the right of block generation. Nevertheless, PoW-based consensus may still be under potential attacks such as 51% attacks and selfish mining. Therefore, to fulfill the ever-growing security and efficiency requirements, experts and scholars have proposed other state-of-the-art consensus protocols. Table 2 presents different types of consensus protocols and elaborates their characteristics with regards to openness, costs, and updating rules. Moreover, we also compare their performance in efficiency, security, and scalability aspects. Among them, proof-of-stake (PoS) and hybrid consensus protocol are the most representative ones.

Compared with PoW, PoS saves more energy since it doesn't need to rely on the computing power of the node. Participants to generate the new block are selected according to the node's stake such as virtual currency or coin age. Ouroboros, a provably secure PoS consensus protocol proposed by Kiayias,[8] selects the leader based on the node's stake, and this leader will be responsible for packing the new block. Simulation tests show that Ouroboros has its distinguished

characteristics in practicability. Moreover, Ouroboros is proved to be secure in the perspective of blockchain forks, incentives, and attack behaviors.

Hybrid consensus, another consensus protocol proposed by Rafael,[9] divides the entire consensus agreement into two layers, namely the small-scale committee election and the Byzantine fault tolerance (BFT) algorithm. The committee is selected from the nodes in P2P network and executes the BFT algorithm in order to implement the packing, verification, and disseminating of the new block.

Nevertheless, the complexity and heterogeneity of the distributed IoT network bring further attention that certain scenarios have demanding requirements on real time for state synchronization. Based on the above two hierarchical consensus protocols, we can further combine the characteristics of the IoT devices to design specific smart contracts to implement a hierarchical admission control module for consensus protocol of IoT devices. Such layered procedures will be critical to select the nodes with excellent performances and, finally, to form the dynamic committee. The committee that applies the regular rotation for blockchain maintenance will serve to guarantee the real-time state update.

## DECENTRALIZED COOPERATION AND TRUST ESTABLISHMENT

While true collaboration is essential to accomplish certain services and functions, it would be challengeable to establish the reliable cooperation and trust in the IoT system since each node can enter and leave the system freely at any time, and the identity can be anonymous between nodes. The reputation assessment model is effective to enhance cooperation and trust between nodes in the P2P network, which has achieved great success in IoT applications such as vehicular ad hoc networks and crowdsourcing.[10] However, the entity-centric trust models based on object evaluation have privacy leakage and free-riding problems.[11] Also, data-centric models are deficient in the lack of data and latency of information confirmation.

Based on blockchain technology, we can build a globally consistent reputation assessment model to enhance the effectiveness of the above trust models. At present, there is not much research regarding the assessment of node reputation based on blockchain technology in a completely anonymous environment. One potential solution is to establish a node assessment model based on irreversible and transparent block data. First, any node can extract the behavior data of other nodes recorded in the block under blockchain technology. After inputting their behavior data to the reputation assessment model, the credibility of the nodes would be calculated automatically. Type of behaviors and timeliness should be considered during credibility calculation since these two aspects reflect the performance of the node over a period of time and influence the final reputation distribution. Hence, when selecting the proper type of behavior and suitable time scale, it is essential to further consider the incentives and preferences of the nodes to better regulate the node behavior and build trust.

## TRANSACTION DATA PRIVACY AND SECURITY

Privacy security is critical to system safety. In the blockchain system, all transactions are shared, and the transaction history may reveal the frequency, content, and destination of transactions, which increases the potential risks that adversaries can infer the actual identity of participants. In the convergence of blockchain and IoE, adversaries can even obtain the IP or physical address of IoT devices. What's worse, it will likely eventually cause device crash and system destabilization via denial-of-service attack or node capture. Therefore, sensitive information that may reflect actual physical location, device type, network address, and other important private information about nodes should be protected, in particular when recording the transaction data.

Zero knowledge proof and homomorphic encryption technology are potentially useful for privacy protection in the blockchain system.[12,13] Zero knowledge proof helps to ensure the confidentiality of transactions in public blockchain. On the one hand, detailed privacy information, including transaction amount and transaction destination address, could be protected in an anonymous way. On the other hand, users can still validate a transaction despite the hidden information. A fully homomorphic encryption scheme

allows the simple computation on encrypted data. For example, in the healthcare field, users can request the service provider to compute and analysis individual medical data on ciphertexts without leaking their electronic medical records.

Although zero-knowledge proof and homomorphic encryption are outstanding ways to release the burden on privacy and security protection, additional computation overload on the IoT devices is an overwhelming barrier to their practicality. Uncertainties remain regarding whether these two approaches are suitable for IoT scenarios, and if so, what types of IoT scenarios are they are suitable for? Therefore, we need to further verify the impact of these two approaches on device performance, including energy consumption and response time.

## CONCLUSION

In the face of a series of problems occuring in the centralized IoT system such as single-point attack, privacy leakage, and poor scalability, blockchain technology offers a greater potential for developing IoE. Nevertheless, because IoT environments are characterized by constrained resources, a high degree of heterogeneity, and mobility of network topology, numerous new challenges have arisen. Cryptography algorithm, authentication protocol, consensus protocol, and reputation assessment model are essential technologies to boost the convergence of blockchain and IoE. This article has shown that hierarchical and lightweight protocols and schemes will be constructive to enhance the efficiency and stability of the IoE system. Moreover, this article proposes a feasible trust model that will promote cooperation and participants' contribution to the decentralized system in order to ultimately realize IoE.

## ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation under Grants 61873166, 61673275, and 61473184.

## REFERENCES

1. F. A. Alaba *et al.*, "Internet of things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, 2017.
2. T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
3. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.
4. N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
5. M. Suárez-Albela *et al.*, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors*, vol. 17, no. 9, 2017, Art. no. 1978.
6. Z. Liu *et al.*, "On emerging family of elliptic curves to secure internet of things: ECC comes of age," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 3, pp. 237–248, May/Jun. 2017.
7. M. T. Hammi *et al.*, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, 2018.
8. A. Kiayias *et al.*, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.*, 2017, pp. 357–388.
9. R. Pass and E. Shi, "Hybrid consensus: Efficient consensus in the permissionless model," in *Proc. 31st Int. Symp. Distrib. Comput.*, 2017, pp. 39:1–39:16.
10. A. Satsiou and L. Tassiulas, "Reputation-based resource allocation in P2P systems of rational users," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 4, pp. 466–479, 2010.
11. Z. Lu *et al.*, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
12. E. B. Sasson *et al.*, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, 2014, pp. 459–474.
13. Q. Lin *et al.*, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

**Lijun Wei** is currently working toward the Ph.D. degree at the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. His current research interests include distributed consensus protocol, blockchain technology, and IoT architecture. Contact him at sjtu_weilijun@sjtu.edu.cn.

**Jing Wu** has been with Shanghai Jiao Tong University, Shanghai, China, since 2011 and is currently an Associate Professor. She is a registered Professional Engineer in Alberta, Canada. Her current research interests include robust model predictive control, security control, and stability analysis and estimations for cyber-physical systems. She received the B.S. degree from Nanchang University, Nanchang, China, in 2000; the M.S. degree from Yanshan University, Qinhuangdao, China, in 2002; and the Ph.D. degree from University of Alberta, Edmonton, AB, Canada, in 2008, all in electrical engineering. Contact her at jingwu@sjtu.edu.cn.

**Chengnian Long** has been with Shanghai Jiao Tong University, Shanghai, China, since 2009 and has been a Full Professor since 2011. He was a Research Associate with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, and a Killam Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada. His current research interests include Internet of things, blockchain technology, deep learning, and cyber-physical system security. He received the B.S., M.S., and Ph.D. degrees from Yanshan University, Qinhuangdao, China, in 1999, 2001, and 2004, respectively, all in control theory and engineering. Contact him at longcn@sjtu.edu.cn (**Corresponding Author**).

**Yi-Bing Lin** (M'96–SM'96–F'03) was a Research Scientist with Bellcore (Telcordia) from 1990 to 1995. He has since been with the National Chiao Tung University (NCTU) in Taiwan. In 2010, he became a Lifetime Chair Professor of NCTU and, in 2011, the Vice President of NCTU. During 2014–2016, he was a Deputy Minister, Ministry of Science and Technology, Taiwan. Since 2016, he has been appointed as a Vice Chancellor, University System of Taiwan (for NCTU, NTHU, NCU, and NYM). He received the Bachelor's degree from National Cheng Kung University, Tainan, Taiwan, in 1983 and the Ph.D. degree from the University of Washington, Seattle, WA, USA, in 1990. He is an Adjunct Research Fellow, Institute of Information Science, Academia Sinica, Research Center for Information Technology Innovation, Academia Sinica, and a member of board of directors, Chunghwa Telecom. He serves on the editorial board of the IEEE Transactions on Vehicular Technology. He has been General or Program Chair for prestigious conferences, including ACM MobiCom 2002. He is Guest Editor for several journals, including the IEEE Transactions on Computers. He is the author of the books *Wireless and Mobile Network Architecture* (Wiley, 2001), *Wireless and Mobile All-IP Networks* (Wiley, 2005), and *Charging for Mobile All-IP Telecommunications* (Wiley, 2008). He has been the recipient of numerous research awards, including 2005 NSC Distinguished Researcher, the 2006 Academic Award of Ministry of Education and 2008 Award for Outstanding contributions in Science and Technology, Executive Yuen, the 2011 National Chair Award, and the TWAS Prize in Engineering Sciences in 2011 (The Academy of Sciences for the Developing World). He is on the advisory boards or the review boards of various government organizations, including the Ministry of Economic Affairs, Ministry of Education, Ministry of Transportation and Communications, and National Science Council. He is an AAAS Fellow, ACM Fellow, and IET Fellow. Contact him at liny@cs.nctu.edu.tw.