The Scanning the Literature column provides concise summaries of selected papers that have recently been published in the field of networking. Each summary describes the paper's main idea, methodology, and technical contributions. The purpose of the column is to bring the state of the art of networking research to readers of *IEEE Network*. Authors are also welcome to recommend their recently published work to the column, and papers with novel ideas, solid work, and significant contributions to the field are especially appreciated. Authors wishing to have their papers presented in the column should contact the Editor.

Xiaohua Tian, Shanghai Jiao Tong University
xtian@sjtu.edu.cn

Blockchain is essentially a decentralized ledger, that is, a technique to collectively maintain a reliable database in a distributed and immutable manner. It is seen as potentially disruptive in areas such as finance, business process management, data provenance, supply chain management, and healthcare. Blockchain also can be applied in networking systems for purposes such as authentication, privacy preservation, wireless communication, and access control. The column in this issue focuses on such networking systems integrated with blockchain technique, which can serve scenarios such as smart farming and Industrial Internet of Things (IIoT) networks.

A smart farming system allows providing agricultural data instantly to farmers. Usage of blockchain in agriculture can reduce uncertainty of the output by increasing its predictability and expected profit, while also reducing resource waste. There have been some authentication schemes in smart farming, precision agriculture, and IoT-related works; however, they still have some constraints such as vulnerability to user impersonation, privileged insider attacks, and inability to support anonymity. To address these challenges, Anusha *et al.* propose a smart-contract-based blockchain-envisioned authenticated key agreement mechanism in the following paper.

Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming

Anusha Vangala, Anil Kumar Sutrala, Ashok Kumar Das, and Minho Jo, *IEEE Internet of Things J.*, vol. 8, no. 13, pp. 10,792–806, July 2021.

A blockchain-based smart farming technology provides agricultural data to farmers and other users associated with smart farming on a single integrated platform. Moreover, persistence and auditability of stored data in blocks into the blockchain provide the confidence of using the correct data when needed later and adds transparency, anonymity, and traceability at the same time. To fulfill such a goal, in this article, the authors design a new smart contract-based blockchain-envisioned authenticated key agreement mechanism in a smart farming environment. The device-to-device (D2D) authentication phase and device-to-gateway (D2G) authentication phase support mutual authentication and key agreement between two Internet of Things (IoT)-enabled devices and between an IoT device and the gateway node (GWN) in the network, respectively. The blocks are created by the edge servers on the authenticated data of IoT devices received from the GWNs and then sent to the cloud server (CS). The smart contract-based consensus mechanism allows verification and addition of the formed blocks by a peer-to-peer (P2P) CS network. The security of the proposed scheme is done through formal and informal security analysis, and also using a formal security verification tool.

Machine learning (ML) plays a significant role in Industry 4.0, enabling predictive analytics and uncovering essential insights to transform industries. With the advancement of computing and communication technologies, ML enables the analysis of massive quantities of data such as those produced by an IIoT-based system, and can use the extracted knowledge (e.g., trained models) to aid real-time decision making in complex situations. However, industries such as smart healthcare and open banking are massively convoluted with human-specific sensitive private data, and ML models trained on sensitive data are vulnerable to attacks. In the following paper, Pathum *et al.* present a framework named PriModChain (Privacy-preserving trustworthy ML model training and sharing framework based on blockchain) that addresses the privacy and trust issues of ML in IIoT systems.

A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems

Pathum Chamikara Mahawaga Arachchige, Peter Bertok, Ibrahim Khalil, Dongxi Liu, Seyit Camtepe, and Mohammed Atiquzzaman, *IEEE Trans. Industrial Informatics*, vol. 16, no. 9, pp. 6092-6102, Sept. 2020.

Industrial Internet of Things (IIoT) is revolutionizing many leading industries such as energy, agriculture, mining, transportation, and healthcare. IIoT is a major driving force for Industry 4.0, which heavily utilizes machine learning (ML) to capitalize on the massive interconnection and large volumes of IIoT data. However, ML models that are trained on sensitive data tend to leak privacy to adversarial attacks, limiting its full potential in Industry 4.0. This article introduces a framework named PriModChain that enforces privacy and trustworthiness on IIoT data by amalgamating differential privacy, federated ML, Ethereum blockchain, and smart contracts. The feasibility of PriModChain in terms of privacy, security, reliability, safety, and resilience is evaluated using simulations developed in Python with socket programming on a general-purpose computer.

Effort has been made on protecting wireless applications using blockchain technology, for example, mobile edge computing (MEC), intelligent 5G, vehicular networking, and wireless sensor networking (WSN). The common idea of applying blockchain in wireless networks is to introduce trustlessness with blockchain so that functions such as identity management and data sharing become more efficient and secure. However, previous studies on blockchain-enabled wireless applications mostly focus on developing practical applications or proposing architectures based on existing blockchain protocols, which were originally designed for wired network applications and thus are not suitable for wireless scenarios. To address this problem, Xu *et al.* design a messagepassing-based blockchain protocol for wireless networks in the following paper.

wChain: A Fast Fault-Tolerant Blockchain Protocol for Multihop Wireless Networks

Minghui Xu, Chunchi Liu, Yifei Zou, Feng Zhao, Jiguo Yu, and Xiuzhen Cheng, *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6915–26, Oct. 2021.

This paper presents wChain, a blockchain protocol specifically designed for multihop wireless networks that deeply integrates wireless communication properties and blockchain technologies under the realistic signal-to-interference-plus-noise ratio (SINR) model. The authors adopt a hierarchical spanner

as the communication backbone to address medium contention and achieve fast data aggregation. Furthermore, wChain employs data aggregation and reaggregation as well as node recovery mechanisms to ensure efficiency, fault tolerance, persistence, and liveness. To validate their design, the authors conduct both theoretical analysis and simulation studies. The results not only demonstrate the nice properties of wChain, but also point to a large new space for the exploration of blockchain protocols in wireless networks.

The blockchain radio access network (B-RAN) is a decentralized, secure architecture for sharing network access and authentication among inherently untrusted network entities. B-RAN connects distinct groups and constructs a multi-sided platform by leveraging the blockchain principle. The participants in a B-RAN can self-organize, self-form, and self-configure into a dynamic network without trusted intermediaries. Most existing investigations focus on the applications and evaluations of B-RAN in cellular network settings, with few in mobile ad hoc networks (MANETs). Ling *et al.* design a multihop routing protocol named Data Broker as a data transport mechanism for self-organizing, non-cooperative MANETs in the following paper.

Data Broker: Dynamic Multi-Hop Routing Protocol in Blockchain Radio Access Network

Xintong Ling, Pengcheng Chen, Jiaheng Wang, and Zhi Ding, *IEEE Commun. Letters*, vol. 25, no. 12, pp. 4000–04, Dec. 2021.

A mobile ad hoc network (MANET) is an infrastructure-less extended scenario of a B-RAN; meanwhile, the decentralization of B-RAN befits MANETs. In the framework of B-RAN, the authors propose a blockchain-based multi-hop routing protocol, namely Data Broker, for non-cooperative MANETs. To incentivize the collaboration among selfish peers, they record the identity information of participating brokers on a ledger list. However, blockchain cannot guarantee the integrity of such a routing ledger directly. Therefore, they design a ledger safeguard mechanism, along with reward policies, to avoid the ledger list being tampered with or modified by dishonest brokers. The experimental results show that the proposed Data Broker can significantly improve the network performance of non-cooperative MANETs regarding latency and loss rate.

A wireless blockchain network is proposed to enable a robust and distributed wireless network for different blockchain applications. With the evolution of wireless networks, the nodes of a network become denser, and to meet the needs of a surge of service requests, the block generation rate should be accelerated to improve the transaction throughput. In this case, the forking problem will become more serious, since the frequent collisions occurring on the channel prolong the backoff counter, and the new block arrives very fast, which increase the forking probability considerably. To address this forking problem and improve B-WLAN performance, in the following paper, Li *et al.* propose mining strategies to reduce the forking probability, and a discard strategy to remove the forking blocks that already exist in carrier sense multiple access with collision avoidance (CSMA/CA) backoff procedure.

Block Access Control in Wireless Blockchain Network: Design, Modeling and Analysis

Yixin Li, Bin Cao, Liang Liang, Deming Mao, and Lei Zhang, *IEEE Trans. Vehic. Tech.*, vol. 70, no. 9, pp. 9258-9272, Sept. 2021.

A wireless blockchain network is proposed to enable a decentralized and safe wireless network for various blockchain applications. To achieve blockchain consensus in a wireless network, one of the important steps is to broadcast new blocks using a wireless channel. Under wireless network protocols, block transmitting will be affected significantly. In this work, we focus on the consensus process in the blockchain-based wireless local area network (B-WLAN) by investigating the impact of the medium access control (MAC) protocol, CSMA/CA. With the randomness of the backoff counter in CSMA/CA, it is possible for later blocks to catch up with or outpace an earlier one, which complicates the blockchain forking problem. In view of this, the authors propose mining strategies to pause mining for reducing the forking probability, and a discard strategy to remove the forking blocks that already exist in the CSMA/CA backoff procedure. Based on the proposed strategies, they design block access control (BAC) approaches to effectively schedule block mining and transmitting for improving the performance of B-WLANs. Then Markov chain models are presented to conduct performance analysis in B-WLANs. The results show that BAC approaches can help the network to achieve a high transaction throughput while improving block utilization and saving computational power.

Blockchain can be used to record transactional data without the requisition of a trusted authority or central server in the peer-to-peer network. The mining process of verifying transactional legitimacy requires a large amount of intensive computing, which leads to some plights such as heavy equipment and fixed access nodes in traditional blockchain systems. To break these barriers, mobile blockchain networks with large-scale IoT devices would be a better choice in the future. Deploying MEC servers in mobile blockchain networks is a feasible way to handle the low computing power dilemma. However, a trusted MEC server will have an opportunity to profit from the usage of information of IoT users. The MEC server will likely allocate more computing resources to some selfish users in order to obtain more revenue. To address this problem, Zuo *et al.* propose an untrusted MEC proof of work (PoW) scheme in the following paper.

Computation Offloading in Untrusted MEC-Aided Mobile Blockchain IoT Systems

Yiping Zuo, Shi Jin, and Shengli Zhang, *IEEE Trans. Wireless Commun.*, vol. 20, no. 12, pp. 8333-–47, Dec. 2021.

Deploying a mobile edge computing (MEC) server in the mobile blockchain-enabled IoT system is a promising approach to improve system performance; however, it imposes a significant challenge on the trust of the MEC server. To address this problem, the authors first propose an untrusted MEC proof of work (PoW) scheme in mobile blockchain networks where plenty of nonce hash computing demands can be offloaded to the MEC server. Then they design a nonce ordering algorithm for this scheme to provide fairer computing resource allocation for all mobile IoT devices/users. Specifically, they formulate the user's nonce selection strategy as a non-cooperative game, where utilities of the individual user are maximized in the untrusted MEC-aided mobile blockchain networks. They also prove the existence of Nash equilibrium, and analysis shows that cooperative behavior is unsuitable for blockchain-enabled IoT devices by using the repeated game. Finally, the authors design the blockchain's difficulty adjustment mechanism to ensure stable block times during a long period of time.