Guest Editorial Special Issue on AI and Blockchain-Powered IoT Sustainable Computing

DUE TO advancements in semiconductor technologies, Internet of Things (IoT) applications have penetrated into a wide spectrum of aspects of human lives. This widespread penetration is also thanks to significant contributions from many emerging technologies, e.g., artificial intelligence (AI) and blockchain [1], [2]. The fast development of AI technologies like deep learning is a promising approach for extracting accurate information from massive raw sensor data in IoT applications [3]. In addition, due to its tamper-proof characteristic and distributed nature, blockchain has received increasing attentions in emerging IoT applications to tackle security and privacy issues [4], [5]. AI and blockchain have become killer technologies to advance the fast development of IoT ecosystems with incredible growth, impact, and potential.

Sustainable computing, providing the environment for the reduction of energy requirement, is a key factor for energy-constrained IoT devices [6]. However, the AI and blockchain paradigms were not originally developed for this kind of IoT environment. Both technologies are computationally expensive and can introduce high bandwidth overhead and delays. These demanding performance and power requirements are not suitable for most IoT devices [7]. Although emerging computing paradigms like edge computing have been introduced to offload computation-intensive tasks from low-power IoT devices [8], many deep learning models still require to be executed in IoT devices due to security and privacy concerns (i.e., keep data locally) [9], [10]. The research on new computing architecture, lightweight deep learning, and blockchain technologies has received increasing attention in recent years.

The Special Issue on AI and Blockchain-Powered IoT Sustainable Computing focuses on the state-of-the-art AI and/or blockchain-based solutions for sustainable computing. After a rigorous review process, we were able to accept 21 contributed articles (out of 65 articles submitted) covering several important topics grouped as follows. In what follows, we briefly review these accepted articles.

Sustainable Data Collection and Processing

Wang et al. [A1] propose a digital twin management architecture for IoT services that utilizes blockchain technology to regulate IoT devices and ensure the accuracy and timely reveal of digital twin information. To encourage efficient and shareable data collection, the authors introduce a blockchain system to incentivize contributors. The results of their simulation performance demonstrate the superiority of the decentralized blockchain system, not only in terms of shared information but also in terms of shared lower costs.

Wang et al. [A2] propose a novel blockchain-supported hierarchical digital twin IoT framework, which combines the digital twin to edge network and adopts blockchain technology to achieve secure and reliable real-time computation.

Federated learning (FL) is one popular AI trend, and the article by Xu et al. [A3] demonstrates how blockchain can be leveraged to support a fully decentralized FL system, by developing 1) an accuracy-based malicious node detection mechanism to facilitate the identification and removal of malicious nodes upon detection of their dishonest/malicious effects on model accuracy during the training process; 2) a contribution-based incentive mechanism with a token-based reward scheme to motivate nodes to participate in FL and contribute to model training; and 3) an algorithm to coordinate both malicious node detection and contributing node incentive/selection.

Zhang et al. [A4] propose a model migration-based FL training acceleration approach for resource-limited IoT devices. By transferring feature extractors from fast to slow devices, the approach reduces training costs and enables sustainable computing. Blockchain is also being introduced to solve the security issues of migrating models between IoT devices. A blockchain-based incentive mechanism and a clustering-based malicious device identification method are used to encourage fast devices to actively share models and exclude malicious devices.

Wang et al. [A5] present a novel deep-learning-based method for predicting influence parameters for critical node detection in Social IoT (SIoT). The proposed method learns dual-task network embeddings to jointly predict influence probabilities and cascade sizes, thus improving the efficiency of critical node detection in SIoT. This AI-powered architecture can be further applied to link prediction, community detection, and many other applications in real-world SIoT, providing a sustainable computing architecture for SIoT.

Computation Offloading and Lightweight AI Models

Existing blockchain-based computation offloading schemes usually focus on network performance improvements and neglect the gas fee for computation offloading. Liu et al.

Digital Object Identifier 10.1109/JIOT.2023.3246806

[A6] present a gas-oriented computation offloading scheme that guarantees a low degree of dissatisfaction of sensors while reducing energy consumption.

Panda et al. [A7] propose an application-deadline-aware data offloading scheme using deep reinforcement learning and dynamic voltage and frequency scaling in an edge computing environment to reduce the energy consumption of IoT devices.

Zhou et al. [A8] investigate a UAV-aided mobile-edge computing network for computation offloading. To maximize the utility of all participants, the interaction among them is modeled by using the Stackelberg game, and the approximate optimal solution is obtained. This article proposes a new approach to solve the computation offloading problem of the mobile edge network, which promotes the development of IoT sustainable computing. In addition, the application of smart contract technology to ensure the reliability of transactions and the application of deep reinforcement learning method to solve the offloading problem in the dynamic event environment show that the combination of AI and blockchain with the proposed model is effective and can be easily expanded.

Akter et al. [A9] propose a blockchain-integrated lightweight convolution neural-network-based intelligent framework for the identification and tracking illegal UAV in the Internet-of-Military-Things (IoMT) system.

Deebak et al. [A10] propose a lightweight blockchain-based remote mutual authentication (B-RMA) method for AI-empowered IoT computing systems. The proposed work integrates blockchain and attribute-based signature technique to perform authentication for the gateways while using smart contracts to authorize a service request within an IoT ecosystem. The methods are integrated in a way that the execution time for authorization is reduced, which in turn, improves the throughput and by extension, the scalability of the system. The computational efficiency and improved security provide a long-term sustainable solution for AI-enabled IoT devices.

Efficient Consensus Algorithms

The leader election procedure in a consortium blockchain becomes important for the transaction prioritization process to take place honestly. Sanghami et al. [A11] propose a machine learning algorithm to achieve efficient leader election, based on which a novel dynamic block creation algorithm is designed.

Anagnostakis et al. [A12] investigate the process of building and sustaining scalable consensus policies over the trivial atomic capacities of the IoT ecosystems. They deploy the IoT micro-blockchain framework as an atomic-consistency tier and define a primary set of validity rules that every node can easily carry out.

Wei et al. [A13] present a new scheme on integrating the heavy matrix computing tasks in AI training into the process of blockchain mining, and thus provide an efficient computing pattern for AI and blockchain-enabled IoT applications. Detailed techniques are designed to realize the computing integration, and experiments corroborate the proposed scheme yield. Possible directions for future work include the further optimization of the latency, the security, and the energy consumption of the whole system, and realizing the logical coordination node in a distributed way.

Privacy Preserving

Wu et al. [A14] propose an innovative smart home and cross-cloud-and-edge computing-based nursing system in IoT to provide activities of daily life to the people who need care in smart home. The authors introduce the blockchain to verify data identities and differential privacy to protect the healthcare takers' data privacy. They design a patient context-aware online learning system which is a typical sustainable computing paradigm. The proposed framework with a top-down infinitely expanding cover tree can support big data analytics with a recommendation accuracy improvement from 30% to 70%.

Yin et al. [A15] propose a novel blockchain-based distributed identity aimed at establishing a self-sovereign identity and providing strong privacy preservation.

Zhang et al. [A16] propose a numerical splitting and adaptive privacy budget allocation-based local differential privacy (LDP) mechanism to conduct data perturbation for blockchain. It aims to address the issues of small sample volume, unfixed input range, and diverse privacy demands in IoT usage scenarios.

Zhang et al. [A17] develop a mobile intelligent application that can collect a large amount of real-time data while protecting the privacy and conducted a feasibility study by defining a new COVID-19 mathematical model.

Spectrum has become a precious resource due to the massive access requests of IoT systems. Data-driven dynamic spectrum-sharing schemes can significantly improve the spectrum utilization although conventional centralized spectrum-sharing schemes are less-transparent, costly, and vulnerable to both malicious attacks and single-point failures. To address these challenges, Zhu et al. [A18] propose a blockchain-based dynamic spectrum-sharing scheme with consideration of the privacy and transaction dynamics. Moreover, a privacy-preserving double auction mechanism based on differential privacy is developed to incentivize spectrum sharing. Both theoretical analysis and simulation results verify the effectiveness of the proposed scheme for supporting future IoT sustainable computing.

Security Issues

Rahman et al. [A19] propose efficient AI-powered advanced persistent threats detection at the edge and transparent recording of the detection history in an immutable blockchain ledger.

Masuduzzaman et al. [A20] propose a deep learning model integrated automated and secure garbage management scheme using unmanned any vehicle (UxV) to minimize the human effort in terms of the traditional garbage management system.

Ravi et al. [A21] propose a thorough investigation for using machine learning (ML) algorithms to analyze and detect anomaly communications based on real-world datasets of wangiri frauds. Benefiting from different ML algorithms, the proposed methods in this article can effectively detect anomaly communications which can automatically mitigate the potential malicious communications and support the sustainable computing and communication requirements for various networks.

ACKNOWLEDGMENT

Our Guest Editor team is pleased with the technical depth and span of this special issue in IEEE INTERNET OF THINGS JOURNAL. We sincerely thank all the authors and reviewers for their efforts, and the Editor-in-Chief and staff members for their gracious support. We hope that the readers enjoy this special issue.

APPENDIX: RELATED ARTICLES

[A1] C. Wang, Z. Cai, and Y. Li, "Sustainable blockchain-based digital twin management architecture for IoT devices," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6535–6548, Apr. 15, 2023.

[A2] D. Wang, B. Li, B. Song, Y. Liu, K. Muhammad, and X. Zhou, "Dual-driven resource management for sustainable computing in the blockchain-supported digital twin IoT," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6549–6560, Apr. 15, 2023.

[A3] Y. Xu et al., "BESIFL: Blockchain empowered secure and incentive federated learning paradigm in IoT," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6561–6573, Apr. 15, 2023.

[A4] C. Zhang et al., "A blockchain-based model migration approach for secure and sustainable federated learning in IoT systems," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6574–6585, Apr. 15, 2023.

[A5] F. Wang, J. She, G. Wang, Y. Ohyama, and M. Wu, "Dual-task network embeddings for influence prediction in Social Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6586–6597, Apr. 15, 2023.

[A6] Y. Liu, Z. Su, and Y. Wang, "Energy-efficient and physical layer secure computation offloading in blockchain-empowered Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6598–6610, Apr. 15, 2023.

[A7] S. K. Panda, M. Lin, and T. Zhou, "Energy efficient computation offloading with DVFS using deep reinforcement learning for time-critical IoT applications in edge computing," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6611–6621, Apr. 15, 2023.

[A8] H. Zhou, Z. Wang, G. Min, and H. Zhang, "UAV-aided computation offloading in mobile edge computing networks: A stackelberg game approach," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6622–6633, Apr. 15, 2023.

[A9] R. Akter, M. Golam, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "IoMT-Net: Blockchain integrated unauthorized UAV localization using lightweight convolution neural network for Internet of Military Things," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6634–6651, Apr. 15, 2023.

[A10] B. D. Deebak et al., "Lightweight blockchain based remote mutual authentication for AI-empowered IoT sustainable computing systems," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6652–6660, Apr. 15, 2023.

[A11] S. V. Sanghami, J. J. Lee, and Q. Hu, "Machine-learning-enhanced blockchain consensus with transaction prioritization for smart cities," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6661–6672, Apr. 15, 2023.

[A12] A. G. Anagnostakis, C. Naxakis, N. Giannakeas, M. G. Tsipouras, A. T. Tzallas, and E. Glavas, "Scalable consensus over finite capacities in multiagent IoT ecosystems," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6673–6688, Apr. 15, 2023.

[A13] Y. Wei, Z. An, S. Leng, and K. Yang, "Evolved PoW: Integrating the matrix computation in machine learning into blockchain mining," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6689–6702, Apr. 15, 2023.

[A14] J. Wu, P. Zhou, Q. Chen, Z. Xu, X. Ding, and J. Hao, "Blockchain-based privacy-aware contextual online learning for collaborative edge-cloud-enabled nursing system in Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6703–6717, Apr. 15, 2023.

[A15] J. Yin, Y. Xiao, Q. Pei, Y. Ju, L. Liu, M. Xiao, and C. Wu, "SmartDID: A novel privacy-preserving identity based on blockchain for IoT," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6718–6732, Apr. 15, 2023.

[A16] K. Zhang, J. Tian, H. Xiao, Y. Zhao, W. Zhao, and J. Chen, "A numerical splitting and adaptive privacy budget allocation based LDP mechanism for privacy preservation in blockchain-powered IoT," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6733–6741, Apr. 15, 2023.

[A17] S. Zhang et al., "Privacy-preserving enabled lightweight COVID-19 simulation model for mobile intelligent application," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6742–6755, Apr. 15, 2023.

[A18] K. Zhu et al., "Privacy-aware double auction with time-dependent valuation for blockchain-based dynamic spectrum sharing in IoT systems," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6756–6768, Apr. 15, 2023.

[A19] Z. Rahman, X. Yi, and I. Khalil, "Blockchain based AI-enabled industry 4.0 CPS protection against advanced persistent threat," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6769–6778, Apr. 15, 2023.

[A20] M. Masuduzzaman, T. Rahim, A. Islam, and S. Y. Shin, "UxV-based deep-learning-integrated automated and secure garbage management scheme using blockchain," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6779–6793, Apr. 15, 2023.

[A21] A. Ravi, M. Msahli, H. Qiu, G. Memmi, A. Bifet, and M. Qiu, "Wangiri fraud: Pattern analysis and machine-learning-based detection," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6794–6802, Apr. 15, 2023.

REFERENCES

[1] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021, doi: 10.1109/JIOT.2020.3025916.

[2] R. Han, Z. Yan, X. Q. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? A survey," *ACM Comput. Surveys*, vol. 55, no. 7, pp. 1–38, 2023. [Online]. Available: https://doi.acm.org?doi=3539604

[3] L. Zhang, F. Li, P. Wang, R. Su, and Z. Chi, "A blockchain-assisted massive IoT data collection intelligent framework," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14708–14722, Aug. 2022, doi: 10.1109/JIOT.2021.3049674.

[4] Y. Wu, Z. Wang, Y. Ma, and V. C. M. Leung, "Deep reinforcement learning for blockchain in industrial IoT: A survey," *Comput. Netw.*, vol. 191, May 2021, Art. no. 108004. [Online]. Available: https://doi.org/10.1016/j.comnet.2021.108004

[5] Y. J. Liu, J. Wang, Z. Yan, Z. G. Wan, and R. Jäntti, "A survey on blockchain-based trust management for Internet of Things," *IEEE Internet Things J.*, early access, Jan. 18, 2023, doi: 10.1109/JIOT.2023.323789.

[6] X. Wang and Y. Lu, "Sustainable and efficient fog-assisted IoT cloud based data collection and delivery for smart cities," *IEEE Trans. Sustain. Comput.*, vol. 7, no. 4, pp. 950–957, Oct.–Dec. 2022, doi: 10.1109/TSUSC.2022.3188330.

[7] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane, and Y. Wu, "A platform-free proof of federated learning consensus mechanism for sustainable blockchains," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3305–3324, Dec. 2022, doi: 10.1109/JSAC.2022.3213347.

[8] J. Zhang, Y. Wu, G. Min, F. Hao, and L. Cui, "Balancing energy consumption and reputation gain of UAV scheduling in edge computing," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 4, pp. 1204–1217, Dec. 2020, doi: 10.1109/TCCN.2020.3004592.

[9] Z. Huang, Y. Wu, N. Tempini, H. Lin, and H. Yin, "An energy-efficient and trustworthy unsupervised anomaly detection framework (EATU) for IIoT," *ACM Trans. Sensor Netw.*, vol. 18, no. 4, p. 56, 2022. [Online]. Available: https://doi.org/10.1145/3543855

[10] L. Peng, W. Feng, Z. Yan, Y. F. Li, X. K. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 295–307, Aug. 2021.

YULEI WU, *Guest Editor*
University of Exeter
EX4 4PY Exeter, U.K.
E-mail: y.l.wu@exeter.ac.uk

NING ZHANG, *Guest Editor*
University of Windsor
Windsor, ON N9B 3P4, Canada
E-mail: ning.zhang@uwindsor.ca

ZHENG YAN, *Guest Editor*
Xidian University
Xi'an 710071, China
E-mail: zyan@xidian.edu.cn

MOHAMMED ATIQUZZAMAN, *Guest Editor*
University of Oklahoma
Norman, OK 73019 USA
E-mail: atiq@ou.edu

YANG XIANG, *Guest Editor*
Swinburne University of Technology
Hawthorn VIC 3122, Australia
E-mail: yxiang@swin.edu.au

Yulei Wu received the Ph.D. degree in computing and mathematics from the University of Bradford, Bradford, U.K., in 2010.

He is a Senior Lecturer with the Department of Computer Science, Faculty of Environment, Science and Economy, University of Exeter, Exeter, U.K. His main research interests include networking, connected systems, edge intelligence, digital twin, and ethical AI.

Ning Zhang received the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2015.

After that, he was a Postdoctoral Research Fellow with the University of Waterloo and the University of Toronto, Toronto, ON, Canada. Since 2020, he has been an Associate Professor with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, Canada. His research interests include connected vehicles, mobile-edge computing, and wireless networking.

Zheng Yan received the D.Sc. degree in technology from the Helsinki University of Technology, Espoo, Finland, in 2007.

She is currently a Full Professor with the School of Cyber Engineering, Xidian University, Xi'an, China. Her research interests are in trust, security, privacy, and security-related data analytics.

Dr. Yan was a recipient of several awards include the N^2Women: Stars in Computer Networking and Communications, the Nokia Distinguished Inventor Award, the IEEE TCSC Award for Excellence in Scalable Computing, the Aalto ELEC Impact Award, the Best Journal Paper Award issued by IEEE Communication Society Technical Committee on Big Data, and the Outstanding Associate Editor of 2017 and 2018 for IEEE ACCESS. She is an Area Editor or an Associate Editor of IEEE INTERNET OF THINGS JOURNAL, *Information Fusion*, IEEE NETWORK, and *Information Sciences*. She served as the General Chair or Program Chair for numerous international conferences, including IEEE TrustCom 2015 and IFIP Networking 2021. She is a Founding Steering Committee Co-Chair of IEEE Blockchain Conference.

Mohammed Atiquzzaman received the M.S. and Ph.D. degrees in electrical engineering and electronics from the University of Manchester, Manchester, U.K., in 1984 and 1987, respectively.

He currently holds the Edith Kinney Gaylord Presidential Professorship with the School of Computer Science, The University of Oklahoma, Norman, OK, USA. He has over 450 refereed technical publications, most of which can be accessed at www.cs.ou.edu/∼atiq.

Dr. Atiquzzaman received the NASA Group Achievement Award, the IEEE Satellite and Space Communications Technical Recognition Award, the IEEE Distinguished Technical Achievement Award, and the IEEE Distinguished Service Award. He is the Editor-in-Chief of the *Journal of Networks and Computer Applications*, the Founding Editor-in-Chief of *Vehicular Communications*, and the former Co-Editor-in-Chief of *Computer Communication*, and has served/serving on the editorial boards of many highly ranked journals, such as IEEE TRANSACTIONS ON MOBILE COMPUTING and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.

Yang Xiang (Fellow, IEEE) received the Ph.D. degree in computer science from Deakin University, Melbourne, VIC, Australia, in 2007.

He is currently a Full Professor and the Dean of Digital Research with Swinburne University of Technology, Melbourne, VIC, Australia. In the past 20 years, he has published more than 300 research papers in many international journals and conferences. His research interests include cyber security, which covers network and system security, data analytics, distributed systems, and networking.

Dr. Xiang is the Editor-in-Chief of the *SpringerBriefs on Cyber Security Systems and Networks*. He serves as an Associate Editor for IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, and *ACM Computing Surveys*. He is the Coordinator, Asia for IEEE Computer Society Technical Committee on Distributed Processing, and the Chair of the Australia and New Zealand, IEEE Blockchain Technical Community.