Editorial: Blockchain Ecosystem—Technological and Management Opportunities and Challenges

***Abstract*—Blockchain is increasingly deployed in a broad range of sectors, ranging from banking and finance to manufacturing to energy to transportation, and so on. While many technological and business related blockchain developments and challenges have been identified, many of these engineering and management challenges have not been addressed. The ongoing interest in this topic is also partly evidenced by the large number of submissions we received in this special issue. Of the 200 submissions, only 39 articles were eventually accepted after several rounds of rigorous reviews (i.e., acceptance rate of 19.5%). In this editorial, we report on the findings from the first 36 articles on a broad range of topics (e.g., supply chain, financial technology, Internet of Things, smart city, healthcare, security, privacy, and blockchain building blocks such as consensus algorithms). Hopefully, the findings reported in these 36 accepted articles will provide sustainable solutions for existing and future blockchain systems and platforms.**

***Index Terms*—Blockchain, consensus, distributed ledger, privacy, security, smart contracts, technology management.**

I. Introduction

Since the success of bitcoin (a blockchain-based cryptocurrency), there has been increasing interest in blockchain from governments [1], standard bodies [2], [3], and the research and practitioner communities, partly evidenced by the number of blockchain-based startups [4], [5] and the number of literature review and survey articles on the topic [6]–[14]. For example, in this special issue Müßigmann *et al.* [15] presented a bibliometric analysis of 613 articles on the application of blockchain in supply chain management. In their analysis, the authors adopted both the citation network and cocitation analyses, and categorized existing approaches into five different research clusters (i.e., theoretical sensemaking, conceptualizing and testing blockchain applications, adopting blockchain in supply chains, the technical design of blockchain applications in real-world applications, and the role of blockchain in digital supply chains). Also in this special issue, Kuperberg [16] surveyed existing blockchain-based identity management solutions and presented a comparative summary of blockchain-based identity management solutions and existing identity management solutions, in terms of end-user functionality, mobility and overhead aspects, compliance/liability, regulations, standardization, and integration. The survey could potentially facilitate identity management solution selection.

Given the diversity of blockchain solutions in the current ecosystem, it can be challenging for decision- and policy-makers to select and decide on the blockchain solutions to use in their organization as explained by Leonardos *et al.* [17] in this special issue. Thus, the authors proposed a 5-D design space with a modular structure, designed to facilitate the comparison and selection of different blockchain solutions by different stakeholders and stakeholder groups.

In addition to the three above accepted articles, we will now present the findings from the other accepted 33 articles in this editorial. There were a total of 200 articles submitted to this special issue, and after several rounds of rigorous reviews (i.e., between two to four rounds), a total of 39 were accepted (i.e., an acceptance rate of 19.5%). The remaining three accepted articles will be included in a future issue of IEEE Transactions on Engineering Management.

II. Management

A. Supply Chain and Logistics

One of the most popular areas where blockchain is used within the management domain is supply chain and logistics, which is also driven by industry interests. For example, Du *et al.* [18] built a blockchain-based supply chain financial platform to manage the financing model. Their platform aims to facilitate trust among the participants, as well as ensuring financial efficiency, knowledge flow, and availability of financial services. The authors also proposed using homomorphic encryption in the blockchain to achieve user privacy.

Epiphaniou *et al.* [19] presented a decentralized data management platform (Cydon) for supply chain. Specifically, their approach utilizes a smart distributed ledger to regulate data sharing and to provide authorized and fast access to secure distributed data that avoids a single point of failure by securely distributing encrypted data across different nodes while maintaining an always-on chain of custody.

Guggenberger *et al.* [20] analyzed how and to what extent blockchain can facilitate information sharing for vendor managed inventory by designing a software prototype based on Hyperledger Fabric using the design science research approach. They contributed to the supply chain by improving interorganizational information sharing for vendor managed inventory by implementing a decentralized information hub using blockchain.

B. Financial Technology (Fintech)

Blockchain implementation for fintech generally seeks to provide banking efficiency, for example by reducing costs

Digital Object Identifier 10.1109/TEM.2020.3023225

and minimizing bureaucracies whilst also improving security. Hence, there is a broad range of fintech applications to replace traditional solutions and to provide alternative or game-changing approaches. Guerar *et al.* [21], for example, focused on invoice financing and proposed a blockchain-based platform to support open and group-restricted auctioning of invoices. To ensure confidentiality, confidential data are encrypted and stored in IPFS and the corresponding hash in the smart contract is hosted on the Ethereum blockchain. In addition to confidentiality, the authors claimed their approach also achieves transparency, immutability, trustworthiness, and security.

Bogusz *et al.* [22] focused on entrepreneurial finance by analyzing crowdfunding, blockchain technologies, cryptocurrencies, and initial coin offerings (ICOs). Drawing upon social media data (comprising a total of 19 7770 captured posts), they examined the interplay between these four entrepreneurial financing solutions. Their study examined the public discussions concerning the selected areas, categorized them by themes, and illustrated the shift between them by identifying three different key periods.

C. Decision Support Systems

Blockchain could be used to improve decision support mechanisms to gather knowledge from a distributed hub. Also, studies could help the development of blockchain with decision support system (DSS) to facilitate selection and implementation of blockchain. In this special issue, Farshidi *et al.* [23] provided a DSS to facilitate blockchain platform selection process in software production. The decision model was evaluated and the findings suggested that this approach may provide significantly more insight into the blockchain platform selection process, provide a richer prioritized option list, and reduce the time and cost of the decision-making process.

Dozier and Montgomery [24] also focused on the utility of DSS for blockchain selection and examined the blockchain innovation evaluation process by utilizing a grounded theory approach. Their study illustrated how organizations applied a specific process to determine the value of blockchain and this investigation led to the proof-of-value model. They suggested that financial service organizations tend to view blockchain innovation as a lower priority due to the lack of a clear path to value. They also found that financial service organizations consistently leverage industry consortium to link to external knowledge and help with the decision-making process.

Gourisetti *et al.* [25] developed the blockchain applicability framework to understand what kind of blockchain and consensus is most appropriate for an application. They developed certain questions with their model to perform a weighted evaluation that is built on mathematical constructs to determine the ideal combination of blockchain.

Osmanoglu *et al.* [26] provided a DSS for agricultural products for an effective yield estimation system using blockchain. Their system may help decision-making actors to develop effective and stable production and price policies. Their proposed system allows farmers to share their farming plans for the oncoming harvest season with the other players of the market whilst allowing them to observe other farmers' plans.

D. Implications of Blockchain on the Economy, Technologies and Ecosystems

As blockchain is considered to be a general purpose technology (GPT) and can be adopted for various management and business functions. For example, Schweizer *et al.* [27] studied the extent of blockchain's impact in the machine economy, using a Delphi study involving 50 blockchain and machine economy experts. Their findings show that for blockchain to be able to drive the machine economy, it needs to overcome issues related to scalability, standardization, legal frameworks, security, blockchain and its linkage with other technologies, and blockchain–human interface and dominant machine currencies.

Schneider *et al.* [28] developed a theoretical framework to examine blockchain's effects on business models and ecosystems. They found that blockchain resembles a symbiosis of human and/or organizational and technological actors that join forces and thereby achieve a new form of agency that is distinct from human or machine agency.

Ur Rehman *et al.* [29] presented a detailed analysis of trust issues in the cryptocurrency ecosystem, including a detailed taxonomic discussion of the key trust aspects including price manipulation, price volatility, insider trading, parallel economy, shadow economy, reputation systems, transparency, centrality, token economy, governance, regulations, design, usability, privacy, and security. They presented a detailed summary of the key trust issues in blockchain and their potential immediate, short-term, and long-term solutions.

III. Technological

A. Internet of Things (IoT)

One of the most popular applications of blockchain is IoT, which is also evidenced by the number of blockchain-IoT related articles in this special issue. For example, Yu *et al.* [30] designed a blockchain-integrated IoT system compatible with attribute-based encryption (ABE), and fine-grained access control using Chameleon Hash algorithms. Their proposed system operates in an update-oriented manner to provide secure access control by restricting historical on-chain data to different members.

In a more gamification-centric sense, Fortino *et al.* [31] proposed a reputation model focused on building the reputation capital of software and device agents in IoT environments. Their work grounds in the adoption of the blockchain technology to certify the reputation capital. The simulation results from this research demonstrated the promising capability of the model in dealing with the misleading agents, and its potential to benefit the IoT community.

Within the IoT-specific distributed ledger, IOTA, Shafeeq *et al.* [32] proposed a new approach to strengthen its underlying cryptographic signature scheme. Their approach employs the cuckoo filter in the IOTA core client to avoid address reuse, particularly when multiple outgoing transfers take place. Their evaluation results, implemented in the IOTA architecture, showed that the filter integration could boost the current security and efficiency of the IOTA platform.

Lockl *et al.* [33] developed a blockchain-based IoT sensor data logging and monitoring system applying design principles to provide better modularity, data parsimony, and availability. Their findings suggest that employing design principles and coupled with the cooperation with organizations could lead to developing more trustworthy blockchain-based IoT ecosystems.

B. Smart Cities

Smart technologies are increasingly playing a critical role in our day-to-day activities. Smart metering and sensing technologies are key to supporting a number of critical functions in our cities, ranging from power generation to autonomous vehicles and even trustworthy voting systems. Securing these technologies in metropolitan smart cities is a particularly interesting application domain for blockchain technologies. In this special issue, Olivares-Rojas *et al.* [34] proposed a blockchain-based architecture to enhance the data security of smart metering systems. The system is optimized to enhance performance by incorporating edge and cloud computing technologies.

Ferrag and Maglaras [35] proposed a blockchain-based deep learning framework, DeepCoin, to facilitate energy exchange in smart grids. DeepCoin is a peer-to-peer energy system that uses the Byzantine fault tolerance algorithm and deep neural networks for attack detection in blockchain-based energy networks.

Developing an interoperable architecture for blockchain is a long lasting challenge that is also emphasized by Hardjono *et al.* [36]. Then, the authors used the design philosophy of the Internet as the basis to identify key design principle to develop an interoperable architecture for blockchain-based autonomous systems to reduce development costs and improve reusability.

Geneiatakis *et al.* [37] attempted to identify suitable blockchain technologies for e-government services. Then, they deployed an existing cross-border e-government goods exchange service that is used in the European Union in an emulated blockchain-based architecture to evaluate its performance. Their results suggested the potential of leveraging the blockchain in various e-government services as they increased both throughput and transactions speed.

Finally, Panja *et al.* [38] developed an Ethereum-based self-tallying decentralized e-voting protocol, which does not require any trusted setup or tallying authority. Voters are required to provide noninteractive zero-knowledge proofs, to assure that they have followed the proposed protocol without revealing their identities. Using such an approach, any third-party observer may compute the tally without involving a tallying authority.

C. Healthcare

Healthcare is another popular application domain for blockchain, partly due to the latter's secure tamper-resistant feature and capability to support decentralized accessibility [10], [39], [40]. In this special issue, Stafford and Treiblmaier [41] qualitatively studied electronic medical records users in the US using the grounded theory (GT) approach, with the aim of developing insights from industry and academia on the characteristics and the suitability of blockchain for secure recording and storage of patients' healthcare information.

Biswas *et al.* [42] presented an approach to facilitate the migration of traditional e-health systems to blockchain-based services. Specifically, the authors attempted to ensure interoperability due to data structure differences for relational databases and blockchain storage. Based on their evaluation results, the authors claimed to achieve improvements in data storage and secure access control during the migration process.

Meng *et al.* [43] used blockchain to build a trust management scheme to mitigate insider attacks on medical IoT. Their work largely focuses on medical smartphone networks (MSNs), due to their popularity and widespread usage in healthcare systems. The authors' evaluation results in two different healthcare environments suggested that their blockchain-based approach may be capable of improving efficiency in detecting malicious actors in such networks.

D. Building Blocks

There are a number of building blocks in a blockchain, and these include consensus algorithms [44], [45]. In this special issue, Kwak *et al.* [46] explained that the use of the byzantine agreement protocol may limit the scalability of the blockchain system, and therefore designed a hierarchical consensus approach. Specifically, in their approach, they use service-zone sharding which allows a disjoint set of transactions to be locally processed by a secure consensus subgroup or globally processed between consensus subgroups. Findings from their evaluation suggested that their approach allows for the forming of secure consensus subgroups with minimal number of communication messages.

The hash algorithm used in the blockchain plays a crucial role in the security and performance of the blockchain-based system, as demonstrated by Wang *et al.* [47] in this special issue. Specifically focusing on Ethereum, they studied the selection of hash functions and evaluated the performance implications of changing the underpinning hash function.

Patsonakis *et al.* [48] reinforced the importance of public key infrastructures (PKIs) in (secure) communications, including those involving blockchain-based systems. Then, the authors presented a construction of their earlier smart contract-based PKI [49] on Ethereum, which omits the reliance for trusted setup without sacrificing its security.

To address one of the key limitations in smart contracts, Nelaturu *et al.* [50] proposed a decentralized oracle to facilitate the querying of information external to the blockchain. Specifically, the authors used a voting-based game to respond to binary queries (e.g., True or False). They also presented a mathematical proof to demonstrate that their approach incentivizes a Nash equilibrium for truthful reporting.

E. Security

Security and privacy (see Section III-F) are generally two key concerns in most popular technologies, and blockchain is no exception. Blockchain-based cybersecurity has been subject to active research and development [51]. For example, the Australian Government [52] warned that

> "[t]here are additional risks and considerations when using permissioned consortium blockchains, where leading users often in effect control the blockchain. This usually removes the perceived benefits of decentrali[z]]ation"

Angieri *et al.* [53] presented their distributed autonomous approach using Ethereum, designed to facilitate the decentralized management of IP addresses (while achieving the same objectives as those fulfilled by the current IP address allocation organizations, namely: uniqueness, fairness, conservation, aggregation, registration, and minimal overheads). To avoid stockpiling and other wasteful practices in their proposed approach, a one-off fee and annual renewal fees are charged to the registered entity.

There have also been attempts to utilize the blockchain to facilitate data sharing between different entities, including those located in different jurisdictions [54]. The challenges are not just technical, but also legal and regulatory. In this special issue, Rahman *et al.* [55] focused on the technical aspects of achieving secure data sharing. Specifically, the authors presented a blockchain-based platform to provide an accountable data sharing function, where misbehaving entities can be penalized. Also focusing on data sharing, Yeh *et al.* [56] proposed a decentralized blockchain-based data exchange platform. However, their platform was designed to facilitate the exchange of distributed denial of service (DDoS) data among different cybersecurity operation centers. To encourage the sharing of such sensitive data, contributing centers will be rewarded with some cryptocurrency. At the same time, to avoid the leakage of the information to the public (or unauthorized entities), the authors devised a dual-level Bloom filter for privacy-preserving searches.

F. Privacy

There is often a tradeoff between security (see Section III-E) and privacy, and hence there have been attempts to design privacy-preserving schemes. Casino and Patsakis [57], for example, presented a blockchain-based recommender system and introduced a decentralized architecture, in order to facilitate locality sensitive hashing classification and recommendation approaches based on how user-managed data.

Wang *et al.* [58] focused on achieving anonymous reporting and anonymous rewarding using both blockchain and elliptic curve public key cryptography. In addition, the authors formally proved that their blockchain-based approach realizes both anonymous reporting and rewarding. They also evaluated the performance of the prototype implementation of the proposed approach.

IV. Conclusion

While this special issue has reported on various technological and management aspects of blockchain and its adoption in a broad range of settings, there are many research problems with seemingly conflicting requirements that need to be explored and addressed. Examples include the following:

Technological themes:

1) Blockchain + Cybersecurity;
2) Blockchain + Artificial Intelligence;
3) Blockchain + Data Science;
4) Blockchain + IoT;
5) Blockchain + Fintech;
6) Blockchain tools, platforms, and methods.

Management themes

1) Blockchain enabled new business systems, models, and applications;
2) Blockchain-based trust and regulation mechanisms;
3) New business relationships and activities based on smart contracts and distributed ledger;
4) Blockchain for decentralization and distributed systems;
5) Management processes and methods based on blockchain;
6) Blockchain for crowdsourcing;
7) Blockchain-based knowledge and innovation management;
8) Financial systems and blockchain;
9) New policies for blockchain.

Acknowledgment

This special issue would not have been possible without the support of the authors who submitted their high quality work to this special issue, the hundreds of experts who selflessly devoted their time to review the submissions, and the Editor-in-Chief (Tugrul U Daim) and the journal staff for their guidance and patience throughout the process.

Kim-Kwang Raymond Choo
Department of Information Systems
and Cyber Security, Department of
Electrical and Computer Engineering
Department of Computer Science
University of Texas at San Antonio
San Antonio, TX 78249 USA
raymond.choo@fulbrightmail.org

Sercan Ozcan
Portsmouth Business School
University of Portsmouth
PO1 2UP Portsmouth, U.K.
Department of Engineering Management
Bahcesehir Universitesi
Istanbul 34349, Turkey
National Research University
Higher School of Economics
101000 Moscow, Russia
sercan.ozcan@port.ac.uk

Ali Dehghantanha
Cyber Science Lab
University of Guelph
Guelph, ON N1G 2W1, Canada
adehghan@uoguelph.ca

Reza M. Parizi
Department of Software Engineering
and Game Design and Development
Kennesaw State University
Marietta, GA 30061 USA
rparizi1@kennesaw.edu

References

[1] D. J. Yaga, P. M. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *NIST Interagency/Internal Rep.*, vol. 8202, 2018.

[2] *Roadmap for blockchain standards*, Standards Australia, 2017, [Online]. Available: https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a 2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx

[3] *Iso/tc 307: Blockchain and distributed ledger technologies*, International Organization for Standardization, 2016. [Online]. Available: https://www.iso.org/committee/6266604/x/catalogue/

[4] "10 of the most promising european blockchain startups to watch," 2020. [Online]. Available: https://www.eu-startups.com/2020/06/10-of-the-most-promising-european-blockchain-startups-to-watch/
[5] "31 blockchain companies paving the way for the future," 2020. [Online]. Available: https://builtin.com/blockchain/blockchain-companies-roundup
[6] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IOT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–32, 2020.
[7] S. K. Lo *et al.*, "Analysis of blockchain solutions for IoT: A systematic literature review," *IEEE Access*, vol. 7, pp. 58822–58835, 2019.
[8] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, 2019.
[9] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain technology for cloud storage: A systematic literature review," *ACM Comput. Surv.*, vol. 53, no. 4, pp. 1–32, 2020.
[10] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, 2020, Art. no. 101966.
[11] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, 2020.
[12] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: A systematic literature review and research agenda," *Supply Chain Manage.*, vol. 24, no. 1, pp. 62–84, 2019.
[13] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.
[14] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep./Oct. 2019.
[15] B. Müßigmann, H. Von Der Gracht, and E. Hartmann, "Blockchain technology in logistics and supply chain management-A bibliometric literature review from 2016 to January 2020," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 988–1007, Nov. 2020.
[16] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020.
[17] S. Leonardos, D. Reijsbergen, and G. Piliouras, "Presto: A systematic framework for blockchain consensus protocols," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1028–1044, Nov. 2020.
[18] M. Du, Q. Chen, J. Xiao, H. Yang, and X. Ma, "Supply chain finance innovation using blockchain," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1045–1058, Nov. 2020.
[19] G. Epiphaniou, P. Pillai, M. Bottarelli, H. Al-Khateeb, M. Hammoudeh, and C. Maple, "Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1059–1073, Nov. 2020.
[20] T. Guggenberger, A. Schweizer, and N. Urbach, "Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1074–1085, Nov. 2020.
[21] M. Guerar, A. Merlo, M. Migliardi, F. Palmieri, and L. Verderame, "A fraud-resilient blockchain-based solution for invoice financing," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1086–1098, Nov. 2020.
[22] C. I. Bogusz, C. Laurell, and C. Sandström, "Tracking the digital evolution of entrepreneurial finance: The interplay between crowdfunding, blockchain technologies, cryptocurrencies, and initial coin offerings," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1099–1108, Nov. 2020.
[23] S. Farshidi, S. Jansen, S. España, and J. Verkleij, "Decision support for blockchain platform selection: Three industry case studies," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1109–1128, Nov. 2020.
[24] P. D. Dozier and T. A. Montgomery, "Banking on blockchain: An evaluation of innovation decision making," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1129–1141, Nov. 2020.
[25] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and demonstration of blockchain applicability framework," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1142–1156, Nov. 2020.
[26] M. Osmanoglu, B. Tugrul, T. Dogantuna, and E. Bostanci, "An effective yield estimation system based on blockchain technology," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1157–1168, Nov. 2020.
[27] A. Schweizer, P. Knoll, N. Urbach, H. A. Von Der Gracht, and T. Hardjono, "To what extent will blockchain drive the machine economy? Perspectives from a prospective study," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1169–1183, Nov. 2020.
[28] S. Schneider, M. Leyer, and M. Tate, "The transformational impact of blockchain technology on business models and ecosystems: A symbiosis of human and technology agents," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1184–1195, Nov. 2020.
[29] M. H. Ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1196–1212, Nov. 2020.
[30] G. Yu *et al.*, "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1213–1230, Nov. 2020.
[31] G. Fortino, F. Messina, D. Rosaci, and G. M. Sarne, "Using blockchain in a reputation-based model for grouping agents in the Internet of Things," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1231–1243, Nov. 2020.
[32] S. Shafeeq, S. Zeadally, M. Alam, and A. Khan, "Curbing address reuse in the iota distributed ledger: A cuckoo-filter-based approach," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1244–1255, Nov. 2020.
[33] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1256–1270, Nov. 2020.
[34] J. C. Olivares-Rojas, E. Reyes-Archundia, J. A. Gutiérrez-Gnecchi, J. Cerda-Jacobo, and J. W. González-Murueta, "A novel multitier blockchain architecture to protect data in smart metering systems," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1271–1284, Nov. 2020.
[35] M. A. Ferrag and L. Maglaras, "Deepcoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020.
[36] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1298–1309, Nov. 2020.
[37] D. Geneiatakis, Y. Soupionis, G. Steri, I. Kounelis, R. Neisse, and I. Nai-Fovino, "Blockchain performance analysis for supporting cross-border e-government services," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1310–1322, Nov. 2020.
[38] S. Panja, S. Bag, F. Hao, and B. Roy, "A smart contract system for decentralized Borda count voting," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1323–1339, Nov. 2020.
[39] J. Bao, D. He, M. Luo, and K.-K. R. Choo, "A survey of blockchain applications in the energy sector," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2020.2998791.
[40] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 8, pp. 2146–2156, Aug. 2020.
[41] T. F. Stafford and H. Treiblmaier, "Characteristics of a blockchain ecosystem for secure and sharable electronic medical records," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1340–1362, Nov. 2020.
[42] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, "Interoperability and synchronization management of blockchain-based decentralized e-health systems," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1363–1376, Nov. 2020.
[43] W. Meng, W. Li, and L. Zhu, "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1377–1386, Nov. 2020.
[44] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst. Man Cybern.*, 2017, pp. 2567–2572.
[45] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surv. Tut.*, vol. 22, no. 2, pp. 1432–1465, Apr./-Jun. 2020.
[46] J.-Y. Kwak, J. Yim, N.-S. Ko, and S.-M. Kim, "The design of hierarchical consensus mechanism based on service-zone sharding," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1387–1403, Nov. 2020.
[47] F. Wang *et al.*, "An experimental investigation into the hash functions used in blockchains," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1404–1424, Nov. 2020.
[48] C. Patsonakis, K. Samari, A. Kiayias, and M. Roussopoulos, "Implementing a smart contract PKI," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1425–1443, Nov. 2020.
[49] C. Patsonakis, K. Samari, M. Roussopoulos, and A. Kiayias, "Towards a smart contract-based, decentralized, public-key infrastructure," in *Proc. Int. Conf. Cryptology Netw. Secur.*, 2017, pp. 299–321.
[50] K. Nelaturu *et al.*, "On public crowdsource-based mechanisms for a decentralized blockchain oracle," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1444–1458, Nov. 2020.

[51] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, 2020.
[52] "Blockchain overview: Australian government guide," [Online]. Available: https://www.dta.gov.au/help-and-advice/technology/blockchain/blockchain-overview-australian-government-guide, Australian Government Digital Transformation Agency
[53] S. Angieri, A. García-Martínez, B. Liu, Z. Yan, C. Wang, and M. Bagnulo, "A distributed autonomous organization for internet address management," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1459–1475, Nov. 2020.
[54] W. Dai, C. Dai, K.-K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A secure blockchain-based data trading ecosystem," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 725–737, 2019.
[55] M. S. Rahman, A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and G. Wang, "Accountable cross-border data sharing using blockchain under relaxed trust assumption," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1476–1486, Nov. 2020.
[56] L.-Y. Yeh, P. J. Lu, S.-H. Huang, and J.-L. Huang, "SOChain: A privacy-preserving DDoS data exchange service over soc consortium blockchain," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1487–1500, Nov. 2020.
[57] F. Casino and C. Patsakis, "An efficient blockchain-based privacy-preserving collaborative filtering architecture," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1501–1513, Nov. 2020.
[58] H. Wang, D. He, Z. Liu, and R. Guo, "Blockchain-based anonymous reporting scheme with anonymous rewarding," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1514–1524, Nov. 2020.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. degree in information security from Queensland University of Technology, Brisbane, Australia, in 2006.

He currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio (UTSA), San Antonio, Texas.

Prof. Choo is the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP JWCN Best Paper Award, Korea Information Processing Society's JIPS Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, Inscrypt 2019 Best Student Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. His research has been funded by NASA, National Security Agency, National Science Foundation, CPS Energy, LGS Innovations, Texas National Security Network Excellence Fund, Australian Government National Drug Law Enforcement Research Fund, Australian Government Cooperative Research Centre for Data to Decision, auDA Foundation, Government of South Australia, BAE Systems stratsec, Australasian Institute of Judicial Administration Incorporated, Australian Research Council, etc. In 2015, he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg.

Sercan Ozcan received the Ph.D. degree in innovation management from Aberystwyth University, U.K., in 2014.

He is a Reader in Innovation and Technology Management with the University of Portsmouth, Portsmouth, U.K. He is also affiliated with Bahcesehir University, Istanbul, Turkey and Higher School of Economics, Moscow, Russia. His work is published in some of the top journals in Innovation Management and Engineering Management. He has over 30 journal articles and conference proceedings in Innovation Management and Text Intelligence areas. He worked as a Consultant and Principal Investigator in collaborative research projects with private and public organizations in various innovation management, product development, and text intelligence-related areas where he raised over £600,000. His current research interests include text intelligence, social network analysis, and machine learning approaches using patents, publications, and social media data.

Dr. Ozcan is also on the Editorial Review Board of the Journal the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT.

Ali Dehghantanha (Senior Member, IEEE) received the Ph.D. degree in security in computing from Universiti Putra Malaysia, Seri Kembangan, Malaysia, in 2011.

He is a leader in the field of cybersecurity and threat intelligence. He has achieved a strong track record of innovation and excellence throughout his career as an independent researcher. He is currently the Director of Cyber Science Lab and the Director of the Master of Cybersecurity and Threat Intelligence Program at the University of Guelph, Guelph, ON, Canada. He has been an invited or keynote speaker in many national and international conferences and is a well-known media contributor in cybersecurity. He has authored or coauthored more than 100 peer-reviewed papers in top journals and conferences in the field.

Dr. Dehghantanha was awarded a Tier 2 NSERC Canada Research Chair in Cybersecurity and Threat Intelligence, in 2020. These Chairs are awarded to exceptional emerging researchers, acknowledged by their peers as having the potential to lead in their field. In 2015, he was awarded a prestigious EU Marie Curie International Incoming Research Fellowship in "Privacy Respecting Digital Forensics." The Marie-Curie Fellowships are Europe's most competitive and prestigious research awards.

Reza M. Parizi (Senior Member, IEEE) received the Ph.D. degree in software engineering from Universiti Putra Malaysia, Selangor, Malaysia, in 2012.

He is currently the Director with the Decentralized Science Lab (dSL), Kennesaw State University (KSU), Kennesaw, Georgia, USA. Prior to joining KSU, he was with the New York Institute of Technology, Old Westbury, New York, USA. His current research interests include R&D in decentralized artificial intelligence, blockchain, smart contracts, Internet of Things, and emerging issues in the practice of secure software-run world applications.

Dr. Parizi is also a member of the Georgia FinTech Academy, SunTrust Fellow, and Global Digital Economy Leadership Council (GDELC), and ACM.