A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges

Tuan-Vinh Le[1], Chien-Lung Hsu[1-5]

[1] Graduate Institute of Business and Management, Chang Gung University, Taiwan
[2] Dept. Information Management, Chang Gung University, Taiwan
[3] Healthy Aging Research Center, Chang Gung University, Taiwan
[4] Dept. Visual Communication Design, Ming Chi University of Technology, Taiwan
[5] Dept. Nursing, Taoyuan Chang Gung Memorial Hospital, Taiwan
tvle.cgu@gmail.com, clhsu@mail.cgu.edu.tw

Abstract

Blockchain technology has been known as a cryptocurrency platform since the emergence of its first and largest application, bitcoin. Blockchain contributes to the process of changing low-trust centralized transaction ledger held by a single third party, to high-trust decentralized form held by different verifying nodes. Due to its decentralized nature and security robustness, blockchain has big potentials to be applied in various fields beyond cryptocurrency. This paper aims to provide readers a more complete literature review of blockchain, compared with existing works. We introduce and explain various security properties of blockchain, provide a taxonomy of blockchain-based applications, and discuss challenges of blockchain in terms of security and performance. Furthermore, some research directions are given in the last section of the paper.

Keywords: Blockchain, Systematic review, Security, Applications, Challenges

1 Introduction

Blockchain was invented by an unknown person, named Satoshi Nakamoto in 2008, to serve as the public transaction ledger of the cryptocurrency Bitcoin [1]. The invention of the blockchain for Bitcoin made it the first digital currency to solve double spending problem without the need of a trusted authority or central server. Bitcoin blockchain provides Peer-to-Peer (P2P) network, which timestamps transactions by hashing them into an ongoing chain of hash-based Proof of Work (PoW), a consensus algorithm. This forms a record that cannot be changed without redoing the PoW [2]. The blockchains readable by the public are widely used by cryptocurrencies, and the Bitcoin design has inspired other applications [1, 3]. Security and privacy in communication networks are big concerns in any information systems. Blockchain with robust security features, for instance confidentiality, integrity, availability [4-9], as well as P2P communication mechanism, can address these issues. Figure 1 depicts the decentralization mechanism of blockchain in various information systems. Blockchain applications cover a lot of domains, such as healthcare [10], internet of vehicle data trading [11], voting [12], etc.

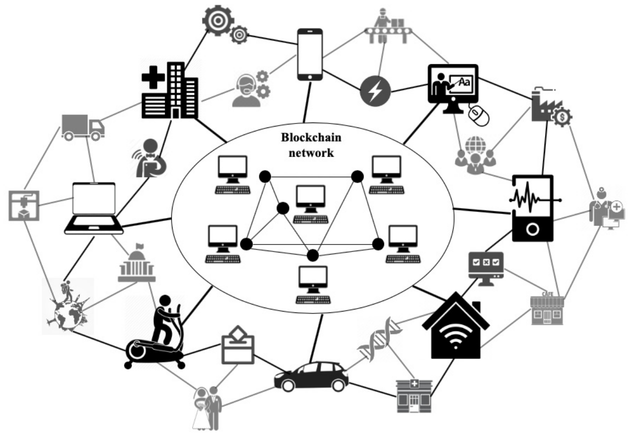

Figure 1. Blockchain with the decentralization in various communication environments

Many reviews and surveys, such as [13-16], have been introduced to provide readers general knowledge as well as various application aspects of blockchain. However, their works did not explain security properties of blockchain in a detailed manner. Classification of blockchain applications in existing works does not specifically discuss domain-oriented applications. In addition, few blockchain challenges and solutions were given in their reviews. In this paper, we make a systematic literature review of blockchain technology, which provides specific discussion on security, applications and challenges. Our contributions can be summarized as follows.

---

*Corresponding Author: Chien-Lung Hsu; E-mail: clhsu@mail.cgu.edu.tw
DOI: 10.53106/160792642021072204007

(1) We introduce and explain various security properties of blockchain. The relations and connections of these properties constitute the decentralized trust and enable distinct security features of blockchain.

(2) Our work provides a specific taxonomy of domain applications enabled with blockchain technology. We include seven domains and aspects, in which healthcare and energy gain the highest blockchain research attention.

(3) We present the challenges of blockchain regarding security and performance. Our work also reviews and recommends several solutions for specific issues.

(4) Future research directions of blockchain technology are given based on the current research status inherent from our findings.

The remainder of the paper is organized as follows. Blockchain basics are provided in Section 2. Research methodology is described in Section 3. Section 4 presents discussion and explanation of blockchain security properties. We provide an in-depth taxonomy of blockchain-based applications in Section 5. Section 6 discusses challenges of blockchain, and recomend corresponding solutions. Some concluding remarks and research directions are given in Section 7.

2 Blockchain Basics

Blockchain is a growing list of records, called blocks, that are linked using cryptography [1]. Each block in the sequence points to the immediately previous block via a reference that is essentially a cryptographic hash value of the previous block called *parent block*. The first block of a blockchain is called *genesis block* which has no parent block [13]. As shown in Figure 2, design structure of blockchain is mainly composed of block header and block body which contains a list of transactions. The block header contains various fields including version number, previous block hash, Merkle root, timestamp, difficulty target and nonce [17]. Moreover, a single digest generated by Merkle tree using secure hash algorithms, for instance SHA-256 hash algorithm [18], is uploaded. This digest is to cover the integrity of the origin evidence. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority [19]. In other words, blockchain is resistant to modification of data structure. The consensus mechanism of blockchain is guaranteed by the algorithms, for instance PoW used in bitcoin [20]. It guarantees that a new block can be verified by all nodes within the network.

Based on the nature of data accessibility, we categorize blockchain into four types: public, private, hybrid blockchain, and consortium blockchain. In a public blockchain, everything recorded in the chain is known to everyone. On the other hand, only the authorized parties or users are allowed access to the data stored in the private blockchain. The hybrid blockchain is the design integrating public and private ones in a single system. Whereas the consortium blockchain is designed by the combination of multiple private chains.

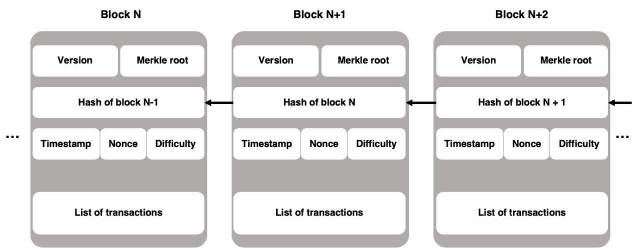

Figure 2. Blockchain data structure

3 Research Methodology

We adopt the methodology introduced by Okoli [21] to conduct a qualitative review in this paper. Using the terms “blockchain” or “distributed ledger”, we searched the literature in well-known scientific databases including Scopus, IEEE Xplore, Google scholar, ScienceDirect, SpringerLink, and Web of Science. The initial total number of the searched records is n = 2229. Only English-written and original research papers were selected. In addition, for making a high-quality review with rigorous works, we only consider journal articles over conference papers, book chapters, etc. The number of records excluded based on these criteria is 1771 (n = 458). Next, 24 papers were removed due to the duplicates and unavailable articles (n = 434). A careful abstract screening was then made in accordance with the scope of our paper that includes three aspects (security properties, applications, and challenges). There were 89 articles excluded at this stage (n = 345), most of which primarily discuss the blockchain in terms of cryptocurrency development, consensus algorithm categorization, user perception, short comments, criticism, and so on. In order to avoid reinventing the wheel, only the original works were included in the literature of our paper, which results in a removal of nine review articles (n = 336). Finally, at the quality appraisal stage, we made a thorough assessment in which only the papers providing high blockchain-centric contents or giving high blockchain-related research results were selected. After this full-text screening, 210 articles were excluded (n = 126). Specific flowchart of the literature search is described in Figure 3. The 126 selected articles were published during the period between 2016 and 2019. As shown in Figure 4, majority of the selected papers were published in 2018. The number of articles published in 2017 is an approximately eightfold increase compared with 2016. In 2018, this number is a more than threefold increase compared to 2017. Blockchain research attention remained relatively high up to the April of 2019.

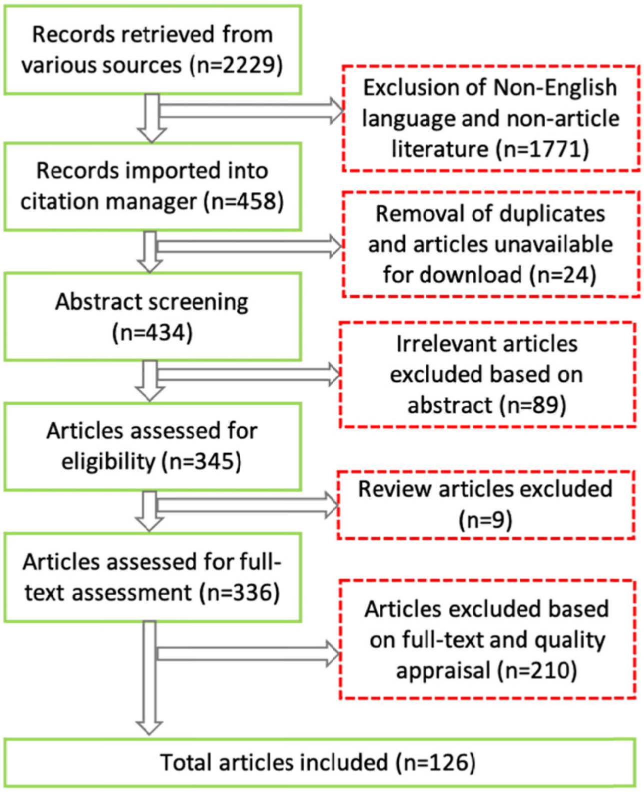

Figure 3. Flowchart of the literature search

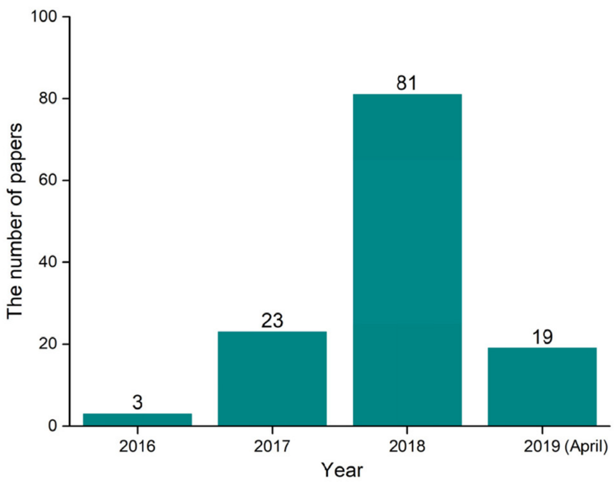

Figure 4. Year-wise description of selected articles

4 Security Properties

This section explains six security properties of blockchain including integrity, transparency, traceability, accountability, anonymity, and unforgeability. These security features are frequently recognized in blockchain-related works.

Integrity is the property that makes sure sent data is received at the destination without any change [6]. Integrity can enable the availability of the services. Accuracy, authenticity and tamper resistance are the properties related to integrity [22-27]. Integrity property of blockchain guarantees data cannot be altered once recorded. This feature was discussed and employed in many approaches [5, 28-31], for instance electricity trading data [29].

Transparency of the blockchain is provided by the type of sequence-appending hash-chained data structure [32-34]. Transparency is achieved when something is uploaded publicly onto blockchain and is available to everyone. Transparency is a determinant element in bringing about trust mechanism of blockchain. Blockchain transparency can be applied in various fields [22, 35-40], for instance healthcare [38].

Research in [41] analyzes the importance of integrity and traceability. Traceability of data is generally achieved by recording data in blockchains and referencing that data by means of a specific identity like a hash value [25]. In [42], traceability is the property where identity of signers can be figured out when some group members work together. In addition, integrity and transparency of blockchain have connection with its traceability property [35]. This blockchain feature has become more prevalent and been used as a security solution in a lot of works [30, 38, 43].

Integrity and non-repudiation are important features in [44]. Accountability is similar to non-repudiation where the actor cannot deny a committed transaction, which is the ability to attribute certain actions to a particular actor [28, 33]. Bitcoin blockchain employs elliptic curve digital signature to achieve accountability of the transactions.

Anonymity of a user is assured that nobody can link the pseudonym to his/her real identity, such as his identity-card number, telephone number and so on [45]. Anonymity of users is the primary threat discussed in [45]. Also, this is a very important feature of blockchain applied in various sectors [22, 46-47]. In these works, anonymity can be regarded as privacy protection where identity and personal information of users are preserved. Moreover, blockchain address representing a destination for cryptocurrency payment can be used as a pseudonym.

Furthermore, unforgeability of blockchain ensure that an adversary cannot pose as the user or corrupt the network. To this end, unforgeability in blockchain inherent from the data integrity combined with digitally signed transactions was adopted and employed in several works [31, 48-49].

The above-discussed security properties are primarily achieved by the public blockchain. The private one does not assure the integrity where the full immutability cannot be achieved due to the collusion attacks probably caused by the internal verifying nodes. Moreover, the anonymity can also not be warranted by the private chain, since the users within it may be identified by some certain nodes. Despite these shortcomings, the private blockchain with single centralized node is still helpful in some cases, since it provides efficient private communication and low energy consumption.

5 Taxonomy of Blockchain-based Applications

Since the emergence of bitcoin, blockchain technology attracts more and more research interests due to its huge potential in various domains and sectors. We include 96 articles for the taxonomy of blockchain applications. The applications are categorized into seven domains and aspects: finance, achievement records, energy, healthcare, manufacturing and supply chain, shipping and delivery, and sustainability. Based on categorization result depicted in Figure 5, we can see that most domains have increasing numbers of research during 2016 to 2018. Healthcare and energy have rapidly increased research papers and present the largest portions in 2018. As we observe, blockchain research on manufacturing and supply chain also gains a significant attention with various branches. It can be inferred that blockchain would be an essential part of Industry 4.0. Figure 6 further describes various applications of blockchain technology.

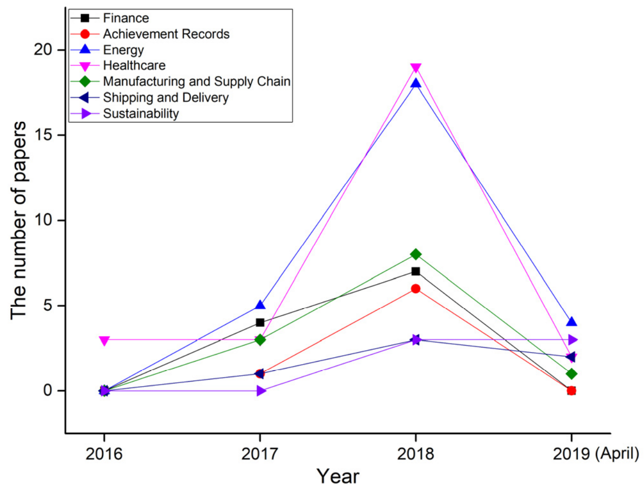

Figure 5. Distribution of selected papers according to identified domains

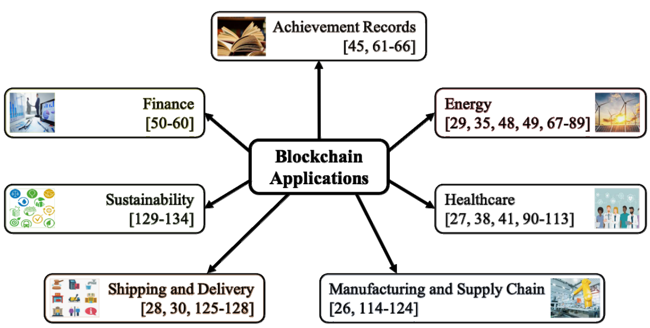

Figure 6. Blockchain-based applications in various domains and aspects

5.1 Finance

Several new blockchain-based systems were proposed for detecting financial fraud [50-52] and preventing money laundering efforts [53]. Post office banking augmented with blockchain technology is one way to implement the transition from fractional reserve banking to full reserve banking [54]. A real-time cryptocurrency price monitoring system can allow investor to constantly check the cryptocurrency market (using a computer or a smart phone) [55]. Blockchain was also employed to simplify and enable trustless channel for funding [56-57]. In addition, payment fairness based on blockchain was introduced in some other works [58-60].

5.2 Achievement Records

A theoretical model that can offer a potential solution for academic certificate issuing and verification using blockchain technology was proposed by [61]. Blockchain also enables a global higher education record platform [62]. Due to a blockchain-based infrastructure [63], we can also document, store and manage learners' credentials, and provides sustainable record of achievements.

Peer review procedure is enabled with blockchain for currency exchange [64]. Blockchain also presents an opportunity to develop a token-based peer-review payment system [65]. Another new architecture called secure pub-sub (SPS) provides blockchain-based fair payment with reputation [45]. Furthermore, a practical implementation of a research data right management solution uses the blockchain as a mean of recording and verifying reuse [66].

5.3 Energy

The trends to solar power storage will emerge as the future grid building block using blockchain support in the new distributed, bi-directional energy system [67-68]. Secure blockchain-based IoT-enabled smart grid networks were proposed in many articles [35, 69-72]. The networks allow to interact in a credible and auditable manner for achieving a greater degree of efficiency, security, reliability, resilience, and sustainability. Due to blockchain, tampering with smart metering have also been addressed [73-74]. Micro-generation of in-house energy with blockchain models provides the possibility of exchanging energy at a community level [75-76]. Users now can monitor how the electricity is used based on a blockchain-based system [77]. Their privacy was also addressed by the support of a blockchain-based data aggregation scheme [78]. Furthermore, security models for electric vehicle charging management have been proposed in blockchain ecosystems [79-81].

The concept of a blockchain-based microgrid energy market was proposed to eliminate the need for central intermediaries [82]. Integrated with blockchain, smart contracts were employed in the energy transaction models [29, 83-84]. In particular, smart contracts enable P2P token bill system for energy assumption [84]. P2P electricity transaction platforms for smart grid were further proposed with blockchain [29, 48, 68, 85-86]. Energy trading systems with the solutions to various security challenges were introduced for IoT [49], multi-signatures [87-88], and double auction mechanism [81, 89].

5.4 Healthcare

Blockchain-based healthcare ecosystem was proposed for electronic medical record (EMR)/electronic health record (EHR)/personal health record (PHR) [41, 90-94], to secure health data and patient information during communication process. Along with that, personal data security of patients was addressed in some other works [95-96]. Health data, user anonymity and user privacy [97] in specific healthcare applications such as diagnosis improvements [98], remote cancer care [99], nail analysis management system [100], are strongly preserved by blockchain mechanism. Healthcare data and access control models enabled with blockchain and smart contract ensure patient own and control their healthcare data, as well as prevent unwanted assets from entering the wrong area [38, 101]. On the other hand, several blockchain-based IoT frameworks allows patients, providers, and third parties to have efficient interoperable access to medical records for specific purposes [27, 102]. Several similar medical data sharing systems were proposed in [103-105]. By the help of blockchain, sensing data produced by wearable sensors was securely stored for real-time monitoring and medical interventions [106-107]. Blockchain also helps in root exploit detection and feature optimization for medical data systems [108]. Transparency of clinical trial data can be improved by blockchain [109-110]. Health data contribution [111], multi-level location sharing [112], and surgery chain [113] in healthcare systems was also introduced in the integration with blockchain.

5.5 Manufacturing and Supply Chain

Blockchain helps to prevent counterfeiting in additive manufacturing was presented by coupling lanthanide nanomaterial chemical signatures [114]. An agriculture supply chain system was proposed with double chain architecture based on public blockchain [115]. On the other hand, a private blockchain-based intelligent agriculture network was also proposed for enhancing security of the system [26]. Blockchain can also be a sustainable solution for the fashion apparel manufacturing industry [116]. An innovative blockchain-based system was designed to ensure information visibility of blood cold chain and to minimize blood transfer time in special situations [117]. Coffee supply chain is energized by blockchain to streamline the supply chain process [118]. In addition, secure blockchain-enabled M2M communications were also designed for cotton spinning production [119]. Blockchain can be employed to protect pharmaceutical supply chain [120]. Transparent transaction data in drug supply chain is enhanced with Gcoin blockchain [121]. Blockchain-based credit evaluation system was provided to strengthen the effectiveness of supervision and management in the food supply chain [122]. Based on RFID sensors and open source technology, a wood chain electronic traceability system was introduced with blockchain architecture [123]. Furthermore, a novel blockchain-enabled ownership management system of RFID-attached products for anti-counterfeits can be used in post supply chain [124].

5.6 Shipping and Delivery

Online shipment tracking framework enabled with blockchain can be used to complement current enterprise-based supply chain management solutions [125]. Employing blockchain and smart contract, information transparency between shipping lines, the shippers and efficient shipment management are achieved [126-127]. Moreover, blockchain-based distributed service with an incentive system allows faithfully transporting the patches to the recipient devices through wireless sensor networks (WSN) and IoT environments [128]. Based on permissionless Ethereum blockchain, a general framework was presented to create a trusted, decentralized proof of delivery system that ensures accountability and integrity [28]. Blockchain-based delivery framework was also proposed for drone-delivered services [30].

5.7 Sustainability

Blockchains can provide sustainable practices in various aspects. For economic sustainability, thanks to the decentralized nature, blockchains can reduce costs and transaction times, reducing waste in manufacturing and production processes, for instance supply chain [129]. Blockchains also provide real-time communications, fast payment with reduced transaction fees, low product costs, and reduced delivery times [130]. It builds an innovative business model and contributes to a sustainable economy. In terms of social aspect of the sustainability, blockchains could solve inequality with the guarantee of the human rights and ethical acts [130-131]. The fairness can also be enabled by blockchains, for instance, a number of products collected in a period of time is immutably recorded for a specific payment [132]. Along with the technological development, environment related issues should also be taken into account. Due to the immutable data recorded in blockchains, the vehicles that emit the highest level of greenhouse gases can be identified for the sudden measures [133]. In addition, blockchains and smart contract were used for a constant monitoring, which avoids drivers from driving faster (that increases emissions and fuel consumption) and saves energy resources [134]. Blockchain technique was also used in identifying materials and products that use significant non-renewable resources [129], thus expediting environment preservation process.

6 Challenges

In this section, we discuss challenges of blockchain in terms of two aspects: security and performance. The detailed discussion is presented in the following.

6.1 Security

Majority (51%) attack is the most well-known attack with blockchain [135]. Majority is not enough and the 51% attack was the chief concern [136]. Majority attacks also threaten to lightweight and manageable digital evidence preservation system on Bitcoin [18]. Majority attack in public blockchain is prone to be caused by powerful quantum computing. Another attack, called distributed denial of service (DDoS), is inherent from denial of service (DoS) attack, where attacker can flood inbound connection of a node with invalid large-sized data [87]. We recommend several solutions to deal with majority attacks and DDoS attacks in blockchain, which are provided in Table 1.

Table 1. Security issues of blockchain and the solutions

Issues	Solutions
Cyber attacks	
Majority (51%) attacks: is performed if attackers obtain control majority of computational power. They may reverse and alter past transaction, as well as generate blocks with malicious transactions (may or may not be caused by *double spending*) [87]. Majority attack in public blockchain is prone to be caused using *quantum computers*.	• Quantum-safe blockchain platform that utilizes quantum key distribution across an urban fiber network for information-theoretically secure authentication [137]. • Novel anti-quantum transaction authentication scheme in the blockchain to construct lightweight non-deterministic wallets [138]. • Applying Grover's quantum search algorithm to the general blockchain technology (for mining) [139].
DDoS attacks: is inherent from denial of service (DoS) attack, where attacker can flood inbound connection of a node with invalid large-sized data [87].	• Dynamically limit the maximum amount of creation transaction using Least Mean Square, in order to prevent DDoS attack in blockchain [140].
Illegal interests	
Selfih mining: happens when the malicious nodes aim to earn greater gains against honest nodes. Selfish mining has a variant, called, *stalker attack*, and results in *mining centralization* problem [141].	• Proposing a practical modification to the Bitcoin protocol with a coalition that command less than 1/4 of the resources [136], which is better than the current reality where a coalition of any size can compromise the system. • Gamification-based approach for increasing participants' motivation to participate in mining work [142].
Fraud transactions: is almost impossible to be changed, which is harmful to the entire economic environment [143].	• Novel polynomial-based modifiable blockchain structure for removing fraud transactions [143].
Anomalous behavior patterns: is caused by some nodes who attempt to cheat in the networks while the majority nodes behaves normally [144].	• A novel algorithm for behavior pattern clustering, which leads to deeper insights into the blockchain network and helps maintainers manage and organize the nodes [144]. This helps in preventing some nodes from having anomalous behavior patterns illegal interests.

In addition to cyber-attacks, illegal interests in blockchain should also be taken into account. Selfish mining attack is performed if the malicious nodes does not disclose their newly mined blocks for gaining more rewards, especially if they have a significant processing power. Selfish mining can result in mining centralization, which breaks the decentralization in blockchain. In addition, fraud transactions and anomalous behavior patterns must also be prevented, so as to guarantee equality for all nodes in the blockchain. The illegal interests and corresponding recommended solutions are also provided in Table 1.

6.2 Performance

We discuss performance issues of blockchain in terms of three aspects namely, resource and energy, throughput and latency, and capacity. Resource, energy, throughput and latency are the biggest issues for blockchain implementations. When blockchains are designed with a cost-effective solution that can reduce the energy consumption in the mining, the environmental sustainability would be promoted. Capacity management is also very important, which helps in avoiding congestion, thereby improving mining efficiency. Table 2 presents the description of these issues along with our recommended solutions.

Table 2. Performance issues of blockchain and the solutions

Issues	Solutions
Resource and energy	• Economic approach for resource management of mobile blockchain, in which the PoW puzzle can be offloaded to the edge computing server, and the miners are priced by the provider [145]. • Reinforcement learning method embedded in a smart contract to minimize the energy cost [146]. • Defining five gas-wasteful patterns for smart contract in Ethereum and propose the improvement methods [147]. • Scalable practical byzantine fault tolerance (BFT) algorithm applied to large-scale distributed blockchain systems for reducing the communication costs [148]. • Proof of kernel work, a low-energy consensus for distributed access-control protocols [149]. • The provable data possession that carries out the mining and storage of new blocks, which greatly reduces computational cost compared to the PoW [150].
Throughput and latency	• Presenting a performance analysis and suggesting using Hyperledger Fabric version 1.0 (over version 0.6), in which throughput, execution time, and latency are improved [151]. • The dynamic modified BFT consensus protocol in [148] allowing decrease in the latency and increase in the throughput. • A directed acyclic graph-based distributed ledger, called PowerGraph, is employed to deal with efficiency and latency issues of blockchain [72].
Capacity	• Network coded distributed storage framework for blockchains [152]. • A novel parallel mining method adjusting the mining capacity based on the transaction load [153].

7 Conclusions and Future Directions

Blockchain changes the traditional way of storing data in the central cloud to a trustless decentralized way. Inherent security properties of blockchain pave the way for massive applications, integrated with advanced technologies like mobile networks, edge computing or IoT. In this paper, we aim to make a systematic literature review of blockchain technology. To this end, we introduce and explain various security properties of blockchain. A taxonomy of blockchain applications in various aspects is provided in some depth. Our work also discusses blockchain challenges in terms of security and performance, then recommend several solutions.

We give some future directions of blockchain research based on our findings throughout the review as follows:

- *More security properties of blockchain should be recognized:* Apart from integrity, transparency and traceability, other security properties of blockchain including accountability, anonymity and unforgeability needs more attention and adoption in specific information systems.
- C*ontinue working on blockchain-enabled secure healthcare and energy applications:* Future direction for healthcare sector may include genomic data sharing system or telecare medicine information system enabled with blockchain security. Blockchain features can also be considered for emission trading systems or green systems of energy sector.
- *Blockchain research on education and publication systems should be promoted:* Education and research are essential parts in our life. The authenticity of education and research records enables the stable and sustainable development of our society.
- *Conduct more rigorous studies on security issues of blockchain*: Although we found out certain security risks to blockchain, especially cyber-attacks, existing solutions to deal with these issues are very few. We encourage the experts on the related field to design more and better mechanisms that can preserve the decentralized nature and functionalities of blockchain.
- *Environmental unsustainability issue of blockchain should further be addressed*: Massive energy consumption of the mining in blockchain may cause a negative effect to the environment. Based on our review, very few articles included this problem with an explicit outcome (except some solutions for resource and energy issues specified in Section 6.2). This paper encourages researchers, practitioners, lawmakers as well as governors to promote the related research and implement reasonable policies to address this important issue.
- *Hybrid blockchain is encouraged to be more widely designed*: although the public blockchain achieves all security properties specified in Section 4, its efficiency is very low compared to the private chain. The public chain also cannot address privacy issues where the data is uploaded publicly. Therefore, we encourage practitioners to design the hybrid one integrating these two types of blockchain, which can achieve a high-security and high-efficiency system. The consortium chain that improves security of the private chain, due to multiple verifying nodes, is

also a good solution.

- *Deal with the legality of blockchain*: To the best of our knowledge, the legality of some types of digital signature used in blockchain is uncertain and could not be used for the purpose of criminal justice. During our thorough review, there exists no solution that addresses the signature legality. A new security system with novel ideas should be proposed to deal with this important issue.

Acknowledgements

This work was supported in part by the Chang Gung Memorial Hospital under Grant CMRPG5D0183 and Grant CMRPD3D0063; in part by the Ministry of Science and Technology in Taiwan under Grant MOST-105-2923-E-182-001-MY3, Grant MOST-107-2221-E-182-006, and Grant MOST-108-2221-E-182-011; in part by the Healthy Aging Research Center, Chang Gung University from the Featured Areas Research Center Program within the Framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan under Grant EMRPD1I0481, Grant EMRPD1H0421, Grant EMRPD1H0551, Grant EMRPD1K0461, and Grant EMRPD1K0481; and in part by the Ministry of Health and Welfare in Taiwan under Grant I1090604.

References

[1] D. Parkins, *Blockchains: The Great Chain of Being Sure about Things*, Report by The Economist, October, 2015.

[2] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Report by Cryptography Mailing List, 2009.

[3] N. Popper, *A Venture Fund With Plenty of Virtual Capital, but No Capitalist*, Report by The New York Times, May, 2016.

[4] J. Mendling, I. Weber, W. M. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. Di Ciccio, M. Dumas, S. Dustdar, A. Gal, L. García-Bañuelos, G. Governatori, R. Hull, M. La Rosa, H. Leopold, F. Leymann, J. Recker, M. Reichert, and L. Zhu, Blockchains for Business Process Management - Challenges and Opportunities, *ACM Transactions on Management Information Systems*, Vol. 9, No. 1, Article No. 4, February, 2018.

[5] B. Zhao, P. Fan, M. Ni, Mchain: A Blockchain-Based VM Measurements Secure Storage Approach in IaaS Cloud With Enhanced Integrity and Controllability, *IEEE Access*, Vol. 6, pp. 43758-43769, August, 2018.

[6] Z. Li, A. V. Barenji, G. Q. Huang, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, *Robotics and Computer-Integrated Manufacturing*, Vol. 54, pp. 133-144, December, 2018.

[7] G. Peters, E. Panayi, Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, in: P. Tasca, T. Aste, L. Pelizzon, N. Perony (Eds.), *Banking Beyond Banks and Money*, Springer, Cham, 2015, pp. 239-278.

[8] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, J. Xie, ShadowEth: Private Smart Contract on Public Blockchain, *Journal of Computer Science and Technology*, Vol. 33, No. 3, pp. 542-556, May, 2018.

[9] N. Gouru, N. L. Vadlamani, CoPS - Cooperative Provenance System with ZKP using Ethereum Blockchain Smart Contracts, *International Journal of Distributed Systems and Technologies*, Vol. 9, No. 4, pp. 40-53, October, 2018.

[10] V. Misic, J. Mišić, X. Chang, Towards a Blockchain-Based Healthcare Information System, *IEEE/CIC International Conference on Communications*, Changchun, China, 2019, pp. 1-6.

[11] K. Liu, W. Chen, Z. Zheng, Z. Li, W. Liang, A Novel Debt-Credit Mechanism for Blockchain-Based Data-Trading in Internet of Vehicles, *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp. 9098-9111, October, 2019.

[12] H. Yi, Securing e-voting based on blockchain in P2P network, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, Article No. 137, May, 2019.

[13] Z. Zheng, S. Xie, H. N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, *International Journal of Web and Grid Services*, Vol. 14, No. 4, pp. 352-375, January, 2018.

[14] F. Casino, T. K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics and Informatics*, Vol. 36, pp. 55-81, March, 2019.

[15] J. Zhang, S. Zhong, T. Wang, H.-C. Chao, J. Wang, Blockchain-based Systems and Applications: A Survey, *Journal of Internet Technology*, Vol. 21, No. 1, pp. 1-14, January, 2020.

[16] A. El Azzaoui, J. H. Park, Post-Quantum Blockchain for a Scalable Smart City, *Journal of Internet Technology*, Vol. 21, No. 4, pp. 1171-1178, July, 2020.

[17] G. Ma, C. Ge, L. Zhou, Achieving reliable timestamp in the bitcoin platform, *Peer-to-Peer Networking and Applications*, Vol. 13, No. 6, pp. 2251-2259, November, 2020.

[18] M. Wang, Q. Wu, B. Qin, Q. Wang, J. Liu, Z. Guan, Lightweight and Manageable Digital Evidence Preservation System on Bitcoin, *Journal of Computer Science and Technology*, Vol. 33, No. 3, pp. 568-586, May, 2018.

[19] M. Iansiti, K. R. Lakhani, The Truth About Blockchain, *Harvard Business Review*, pp. 118-127, January-February, 2017.

[20] M. Khan, K. Salah, IoT Security: Review, Blockchain Solutions, and Open Challenges, *Future Generation Computer Systems*, Vol. 82, pp. 395-411, May, 2018.

[21] C. Okoli, A Guide to Conducting a Standalone Systematic Literature Review, *Communications of the Association for Information Systems*, Vol. 37, Article No. 43, November, 2015.

[22] D. Kumar, D. Chandini, B. Reddy, D. Bhattacharyya, T.-h. Kim, Secure Electronic Voting System using Blockchain

Technology, *International Journal of Advanced Science and Technology*, Vol. 118, pp. 13-22, 2018.

[23] V. Lemieux, Trusting Records: Is Blockchain Technology the Answer?, *Records Management Journal*, Vol. 26, No. 2, pp. 110-139, July, 2016.

[24] S. Huckle, M. White, Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains, *Big Data*, Vol. 5, No. 4, pp. 356-371, December, 2017.

[25] A. Nakadaira, S. Ohashi, H. Watanabe, S. Fujimura, S. Sakuma, S. Kinoshita, Initiatives concerning development of applications utilizing blockchains, *NTT Technical Review*, Vol. 15, No. 12, pp. 1-7, December, 2017.

[26] H. Wu, C. Tsai, An intelligent agriculture network security system based on private blockchains, *Journal of Communications and Networks*, Vol. 21, No. 5, pp. 503-508, October, 2019.

[27] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data, *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp. 8770-8781, October, 2019.

[28] H. R. Hasan, K. Salah, Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters, *IEEE Access*, Vol. 6, pp. 46781-46793, August, 2018.

[29] F. Luo, Z. Y. Dong, G. Liang, J. Murata, Z. Xu, A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain, *IEEE Transactions on Power Systems*, Vol. 34, No. 5, pp. 4097-4108, September, 2019.

[30] M. A. Ferrag, L. Maglaras, DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services, *Computers*, Vol. 8, No. 3, Article No. 58, September, 2019.

[31] X. Li, J. Niu, J. Gao, Y. Han, Secure Electronic Ticketing System based on Consortium Blockchain, *KSII Transactions on Internet and Information Systems*, Vol. 13, No. 10 pp. 5219-5243, October, 2019.

[32] Q. Xing, B. Wang, X. Wang, BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution, *Symmetry*, Vol. 10, No. 9, Article No. 408, September, 2018.

[33] N. Kshetri, Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy, *Telecommunications Policy*, Vol. 41, No. 10, pp. 1027-1038, November, 2017.

[34] E. Bertino, A. Kundu, Z. Sura, Data Transparency with Blockchain and AI Ethics, *Journal of Data and Information Quality*, Vol. 11, No. 4, pp. 1-8, September, 2019.

[35] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks, *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp. 7992-8004, October, 2019.

[36] H. Zhang, E. Deng, H. Zhu, Z. Cao, Smart Contract for Secure Billing in Ride-Hailing Service via Blockchain, *Peer-to-Peer Networking and Applications*, Vol. 12, No. 5, pp. 1346-1357, September, 2019.

[37] A. Kakrania, K. A. Kumar, Secure E-Donation System using Blockchain Technology, *International Journal of Engineering and Advanced Technology*, Vol. 9, No. 1, pp. 2676-2681, October, 2019.

[38] S. Figueroa, J. Añorga, S. Arrizabalaga, An Attribute-Based Access Control Model in RFID Systems Based on Blockchain Decentralized Applications for Healthcare Environments, *Computers*, Vol. 8, No. 3, Article No. 57, September, 2019.

[39] I. Ali, M. Gervais, E. Ahene, F. Li, A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs, *Journal of Systems Architecture*, Vol. 99, Article No. 101636, October, 2019.

[40] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 27, No. 12, pp. 2792-2801, Decemer, 2019.

[41] H. Wang, Y. Song, Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain, *Journal of Medical Systems*, Vol. 42, No. 8, Article No. 152, August, 2018.

[42] L. Huang, G. Zhang, A. Fu, Privacy-Preserving Public Auditing for Non-manager Group Shared Data, *Wireless Personal Communications*, Vol. 100, No. 4, pp. 1277-1294, June, 2018.

[43] R.-Y. Chen, A traceability chain algorithm for artificial neural networks using T–S fuzzy cognitive maps in blockchain, *Future Generation Computer Systems*, Vol. 80, pp. 198-210, March, 2018.

[44] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, E. Kaldoudi, A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval, *Computational and Structural Biotechnology Journal*, Vol. 16, pp. 288-297, 2018.

[45] Y. Zhao, Y. Li, Q. Mu, B. Yang, Y. Yu, Secure Pub-Sub: Blockchain-Based Fair Payment With Reputation for Reliable Cyber Physical Systems, *IEEE Access*, Vol. 6, pp. 12295-12303, January, 2018.

[46] Y. Liu, X. Liu, C. Tang, J. Wang, L. Zhang, Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin, *IEEE Access*, Vol. 6, pp. 23261-23270, April, 2018.

[47] J. M. Kang, B. Kim, S.-j. Kim, A Study on Privacy Protection Method Applying Blockchain Technology for Big Data Utilization, *Journal of Engineering and Applied Sciences*, Vol. 13, No. 3, pp. 691-695, 2018.

[48] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains, *IEEE Transactions on Industrial Informatics*, Vol. 13, No. 6, pp. 3154-3164, December, 2017.

[49] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3690-3700, August, 2018.

[50] Y. Wang, A. Kogan, Designing confidentiality-preserving Blockchain-based transaction processing systems, *International Journal of Accounting Information Systems*,

Vol. 30, pp. 1-18, September, 2018.

[51] S. Mamais, G. Theodorakopoulos, Behavioural Verification: Preventing Report Fraud in Decentralized Advert Distribution Systems, *Future Internet*, Vol. 9, No. 4, Article No. 88, December, 2017.

[52] E. Ducas, A. Wilner, The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada, *International Journal: Canada's Journal of Global Policy Analysis*, Vol. 72, No. 4, pp. 538-562, December, 2017.

[53] M. Campbell-Verduyn, Bitcoin, crypto-coins, and global anti-money laundering governance, *Crime, Law and Social Change*, Vol. 69, No. 2, pp. 283-305, March, 2018.

[54] R. E. Krainer, Economic stability under alternative banking systems: Theory and policy, *Journal of Financial Stability*, Vol. 31, pp. 107-118, August, 2017.

[55] S.-I. Park, J.-W Jang, An implement of real-time cryptocurrency price monitoring system, *Journal of Engineering and Applied Sciences*, Vol. 13, No. 4, pp. 1002-1005, 2018.

[56] K.-J. Kim, S.-P. Hong, Design and Implementation of System for Reliable Application using Blockchain: A Case Study in P2P Crowdfunding, *International Journal of Grid and Distributed Computing*, Vol. 10, No. 12, pp. 81-92, 2017.

[57] C. Burchert, C. Decker, R. Wattenhofer, Scalable Funding of Bitcoin Micropayment Channel Networks, *Royal Society Open Science*, Vol. 5, No. 8, Article No. 180089, August, 2018.

[58] Y. Zhang, R. H. Deng, J. Shu, K. Yang, D. Zheng, TKSE: Trustworthy Keyword Search Over Encrypted Data With Two-Side Verifiability via Blockchain, *IEEE Access*, Vol. 6, pp. 31077-31087, June, 2018.

[59] M. Conoscenti, A. Vetro, J. C. De Martin, F. Spini, The CLoTH Simulator for HTLC Payment Networks with Introductory Lightning Network Performance Results, *Information*, Vol. 9, No. 9, Article No. 223, September, 2018.

[60] W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou, H. Jin, SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone, *IEEE Access*, Vol. 6, pp. 40638-40648, July, 2018.

[61] O. Ghazali, O. S. Saleh, A Graduation Certificate Verification Model via Utilization of the Blockchain Technology, *Journal of Telecommunication, Electronic and Computer Engineering*, Vol. 10, No. 3-2, pp. 29-34, September, 2018.

[62] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, A. Kamišalić, EduCTX: A Blockchain-Based Higher Education Credit Platform, *IEEE Access*, Vol. 6, pp. 5112-5127, January, 2018.

[63] M. Jirgensons, J. Kapenieks, Blockchain and the Future of Digital Learning Credential Assessment and Management, *Journal of Teacher Education for Sustainability*, Vol. 20, No. 1, pp. 145-156, 2018.

[64] M. Spearpoint, A proposed currency system for academic peer review payments using the blockchain technology, *Publications*, Vol. 5, No. 3, Article No. 19, September, 2017.

[65] M. Avital, Peer Review: Toward a Blockchain-enabled Market-based Ecosystem, *Communications of the Association for Information Systems*, Vol. 42, pp. 646-653, May, 2018.

[66] A.-T. Pãnescu, V. Manta, Smart Contracts for Research Data Rights Management over the Ethereum Blockchain Network, *Science & Technology Libraries*, Vol. 37, No. 3, pp. 235-245, May, 2018.

[67] J. Green, P. Newman, Citizen utilities: The emerging power paradigm, *Energy Policy*, Vol. 105, pp. 283-293, June, 2017.

[68] A. Lüth, J. M. Zepter, P. Crespo del Granado, R. Egging, Local Electricity Market Designs for Peer-to-Peer Trading: The Role of Battery Flexibility, *Applied Energy*, Vol. 229, pp. 1233-1243, November, 2018.

[69] Z. Y. Dong, F. Luo, G. Liang, Blockchain: A Secure, Decentralized, Trusted Cyber Infrastructure Solution for Future Energy Systems, *Journal of Modern Power Systems and Clean Energy*, Vol. 6, No. 5, pp. 958-967, September, 2018.

[70] S. Noor, W. Yang, M. Guo, K. H. Van Dam, X. Wang, Energy Demand Side Management within Micro-Grid Networks Enhanced by Blockchain, *Applied Energy*, Vol. 228, pp. 1385-1398, October, 2018.

[71] Z. Li, M. Shahidehpour, X. Liu, Cyber-Secure Decentralized Energy Management for IoT-Enabled Active Distribution Networks, *Journal of Modern Power Systems and Clean Energy*, Vol. 6, No. 5, pp. 900-917, September, 2018.

[72] S. Park, H. Kim, DAG-Based Distributed Ledger for Low-Latency Smart Grid Network, *Energies*, Vol. 12, No. 18, Article No. 3570, September, 2019.

[73] C. Rottondi, G. Verticale, A Privacy-Friendly Gaming Framework in Smart Electricity and Water Grids, *IEEE Access*, Vol. 5, pp. 14221-14233, July, 2017.

[74] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids, *Sensors*, Vol. 18, No. 1, Article No. 162, January, 2018.

[75] J. Ferreira, A. Martins, Building a Community of Users for Open Market Energy, *Energies*, Vol. 11, No. 9, Article No. 2330, September, 2018.

[76] A. Pieroni, N. Scarpato, L. Di Nunzio, F. Fallucchi, M. Raso, Smarter City: Smart Energy Grid based on Blockchain Technology, *International Journal on Advanced Science, Engineering and Information Technology*, Vol. 8, No. 1, pp. 298-306, 2018.

[77] J. Gao, K. Asamoah, E. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, G. Dong, GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid, *IEEE Access*, Vol. 6, pp. 9917-9925, February, 2018.

[78] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, Y. Ma, Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities, *IEEE Communications Magazine*, Vol. 56, No. 7, pp. 82-88, July, 2018.

[79] X. Huang, C. Xu, P. Wang, H. Liu, LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem, *IEEE Access*, Vol. 6, pp. 13565-13574, March, 2018.

[80] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, Y. Chen, Adaptive

Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform, *IEEE Access*, Vol. 6, pp. 25657-25665, May, 2018.

[81] R. Jin, X. Zhang, Z. Wang, W. Sun, X. Yang, Z. Shi, Blockchain-Enabled Charging Right Trading Among EV Charging Stations, *Energies*, Vol. 12, No. 20, Article No. 3922, October, 2019.

[82] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, C. Weinhardt, Designing microgrid energy markets: A case study: The Brooklyn Microgrid, *Applied Energy*, Vol. 210, pp. 870-880, January, 2018.

[83] S. Zhao, B. Wang, Y. Li, Y. Li, Integrated Energy Transaction Mechanisms Based on Blockchain Technology, *Energies*, Vol. 11, No. 9, Article No. 2412, September, 2018.

[84] S. Aiman, S. Hassan, A. Habbal, A. Rosli, A. H. M. Shabli, Smart Electricity Billing System using Blockchain Technology, *Journal of Telecommunication, Electronic and Computer Engineering*, Vol. 10, No. 2-4, pp. 91-94, July, 2018.

[85] L. Park, S. Lee, H. Chang, A Sustainable Home Energy Prosumer-Chain Methodology with Energy Tags over the Blockchain, *Sustainability*, Vol. 10, No. 3, Article No. 658, March, 2018.

[86] J. J. Sikorski, J. Haughton, M. Kraft, Blockchain Technology in the Chemical Industry: Machine-to-Machine Electricity Market, *Applied Energy*, Vol. 195, pp. 234-246, June, 2017.

[87] N. Z. Aitzhan, D. Svetinovic, Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams, *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 5, pp. 840-852, September-October, 2018.

[88] S. Khan, R. Khan, Multiple Authorities Attribute-Based Verification Mechanism for Blockchain Mircogrid Transactions, *Energies*, Vol. 11, No. 5, Article No. 1154, May, 2018.

[89] J. Wang, Q. Wang, N. Zhou, Y. Chi, A Novel Electricity Transaction Mode of Microgrids Based on Blockchain and Continuous Double Auction, *Energies*, Vol. 10, No. 12, Article No. 1971, December, 2017.

[90] C. Esposito, A. D. Santis, G. Tortora, H. Chang, K. R. Choo, Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?, *IEEE Cloud Computing*, Vol. 5, No. 1, pp. 31-37, January-February, 2018.

[91] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. S. Tavares, V. H. C. de Albuquerque, A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform, *Cognitive Systems Research*, Vol. 52, pp. 1-11, December, 2018.

[92] Q. Xia, E. Sifah, A. Smahi, S. Amofa, X. Zhang, BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments, *Information*, Vol. 8, No. 2, Article No. 44, June, 2017.

[93] K. Mannaro, G. Baralla, A. Pinna, S. Ibba, A Blockchain Approach Applied to a Teledermatology Platform in the Sardinian Region (Italy), *Information*, Vol. 9, No. 2, Article No. 44, February, 2018.

[94] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems, *IEEE Access*, Vol. 6, pp. 11676-11686, February, 2018.

[95] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain, *Journal of Medical Systems*, Vol. 42, No. 8, Article No. 136, August, 2018.

[96] S. Rahmadika, K.-H. Rhee, Blockchain Technology for Providing an Architecture Model of Decentralized Personal Health Information, *International Journal of Engineering Business Management*, Vol. 10, pp. 1-12, January, 2018.

[97] D. Mendes, I. Rodrigues, C. Fonseca, M. Lopes, J. García-Alonso, J. Berrocal, Anonymized Distributed PHR Using Blockchain for Openness and Non-repudiation Guarantee, in: J. Mantas, Z. Sonicki, M. Crisan-Vida, K. Fister, M. Hagglund, A. Kolokathi, M. Hercigonja-Szekeres (Eds.), *Studies in Health Technology and Informatics*, Vol. 255, IOS Press, 2018, pp. 170-174.

[98] A. Zhang, X. Lin, Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain, *Journal of Medical Systems*, Vol. 42, No. 8, Article No. 140, August, 2018.

[99] P. Zhang, J. White, D. C. Schmidt, G. Lenz, S. T. Rosenbloom, FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data, *Computational and Structural Biotechnology Journal*, Vol. 16, pp. 267-278, 2018.

[100] S. Lee, C. Yang, Fingernail analysis management system using microscopy sensor and blockchain technology, *International Journal of Distributed Sensor Networks*, Vol. 14, No. 3, pp. 1-13, March, 2018.

[101] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, *Journal of medical systems*, Vol. 40, No. 10, Article No. 218, October, 2016.

[102] G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology, *Sustainable Cities and Society*, Vol. 39, pp. 283-297, May, 2018.

[103] H. Kaur, A. Alam, R. Jameel, A. Mourya, V. Chang, A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment, *Journal of Medical Systems*, Vol. 42, No. 8, Article No. 156, August, 2018.

[104] Q. Xia, E. Sifah, K. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain, *IEEE Access*, Vol. 5, pp. 14757-14767, July, 2017.

[105] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-Based Data Preservation System for Medical Data, *Journal of Medical Systems*, Vol. 42, No. 8, Article No. 141, August, 2018.

[106] M. A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous Patient Monitoring With a Patient Centric

Agent: A Block Architecture, *IEEE Access*, Vol. 6, pp. 32700-32726, June, 2018.

[107] K. Griggs, O. Ossipova, C. Kohlios, A. Baccarini, E. Howson, T. Hayajneh, Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring, *Journal of Medical Systems*, Vol. 42, No. 7, Article No. 130, July, 2018.

[108] A. Firdaus, N. Anuar, M. Razak, I. Hashem, S. Bachok, A. Sangaiah, Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management, *Journal of Medical Systems*, Vol. 42, No. 6, Article No. 112, June, 2018.

[109] T. Nugent, D. Upton, M. Cimpoesu, Improving Data Transparency in Clinical Trials Using Blockchain Smart Contracts, *F1000Research*, Vol. 5, Article No. 2541, October, 2016.

[110] M. Benchoufi, R. Porcher, P. Ravaud, Blockchain Protocols in Clinical Trials: Transparency and Traceability of Consent, *F1000Research*, Vol. 6, Article No. 66, January, 2017.

[111] J. Zhang, N. Xue, X. Huang, A Secure System For Pervasive Social Network-based Healthcare, *IEEE Access*, Vol. 4, pp. 9239-9250, December, 2016.

[112] Y. Ji, J. Zhang, J. Ma, C. Yang, X. Yao, BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 42, No. 8, Article No. 147, August, 2018.

[113] J. Fiaidhi, S. Mohammed, S. Mohammed, EDI with Blockchain as an Enabler for Extreme Automation, *IT Professional*, Vol. 20, No. 4, pp. 66-72, July-August, 2018.

[114] Z. Kennedy, D. Stephenson, J. Christ, T. Pope, B. Arey, C. Barrett, M. Warner, Enhanced Anti-Counterfeiting Measures for Additive Manufacturing: Coupling Lanthanide Nanomaterial Chemical Signatures with Blockchain Technology, *Journal of Materials Chemistry C*, Vol. 37, pp. 9570-9578, October, 2017.

[115] K. Leng, Y. Bi, L. Jing, H.-C. Fu, I. Van Nieuwenhuyse, Research on Agricultural Supply Chain System with Double Chain Architecture Based on Blockchain Technology, *Future Generation Computer Systems*, Vol. 86, pp. 641-649, September, 2018.

[116] B. Fu, Z. Shu, X. Liu, Blockchain Enhanced Emission Trading Framework in Fashion Apparel Manufacturing Industry, *Sustainability*, Vol. 10, No. 4, Article No. 1105, April, 2018.

[117] S. Kim, D. Kim, Design of An Innovative Blood Cold Chain Management System Using Blockchain Technologies, *ICIC Express Letters*, *Part B: Applications*, Vol. 9, No. 10, pp. 1067-1073, October, 2018.

[118] V. Thiruchelvam, A. Mughisha, M. Shahpasand, M. Bamiah, Blockchain-based Technology in the Coffee Supply Chain Trade: Case of Burundi Coffee, *Journal of Telecommunication, Electronic and Computer Engineering*, Vol. 10, No. 3-2, pp. 121-125, September, 2018.

[119] S. Yin, J. Bao, Y. Zhang, X. Huang, M2M Security Technology of CPS Based on Blockchains, *Symmetry*, Vol. 9, No. 9, Article No. 193, September, 2017.

[120] P. Sylim, F. Liu, A. Marcelo, P. Fontelo, Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention, *JMIR Research Protocols*, Vol. 7, No. 9, Article No. e10163, September, 2018.

[121] J.-H. Tseng, Y.-C. Liao, B. Chong, S.-w. Liao, Governance on the Drug Supply Chain via Gcoin Blockchain, *International Journal of Environmental Research and Public Health*, Vol. 15, No 6, Article No. 1055, June, 2018.

[122] D. Mao, F. Wang, Z. Hao, H. Li, Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain, *International Journal of Environmental Research and Public Health*, Vol. 15, No. 8, Article No. 1627, August, 2018.

[123] S. Figorilli, F. Antonucci, C. Costa, F. Pallottino, L. Raso, M. Castiglione, E. Pinci, D. Vecchio, G. Colle, A. R. Proto, G. Sperandio, P. Menesatti, A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain, *Sensors*, Vol. 18, No. 9, Article No. 3133, September, 2018.

[124] K. Toyoda, P. T. Mathiopoulos, I. Sasase, T. Ohtsuki, A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain, *IEEE Access*, Vol. 5, pp. 17465-17477, June, 2017.

[125] H. Wu, Z. Li, B. King, Z. B. Miled, J. Wassick, J. Tazelaar, A Distributed Ledger for Supply Chain Physical Distribution Visibility, *Information*, Vol. 8, No. 4, Article No. 137, December, 2017.

[126] A. Tan, Y. Zhao, T. Halliday, A Blockchain Model for Less Container Load Operations in China, *International Journal of Information Systems and Supply Chain Management*, Vol. 11, No. 2, pp. 39-53, April, 2018.

[127] H. Hasan, E. AlHadhrami, A. AlDhaheri, K. Salah, R. Jayaraman, Smart Contract-Based Approach for Efficient Shipment Management, *Computers & Industrial Engineering*, Vol. 136, pp. 149-159, October, 2019.

[128] J. Lee, Patch Transporter: Incentivized, Decentralized Software Patch System for WSN and IoT Environments, *Sensors*, Vol. 18, No. 2, Article No. 574, February, 2018.

[129] M. Kouhizadeh, J. Sarkis, Q. Zhu, At the Nexus of Blockchain Technology, the Circular Economy, and Product Deletion, *Applied Sciences*, Vol. 9, No. 8, Article No. 1712, April, 2019.

[130] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain Technology and Its Relationships to Sustainable Supply Chain Management, *International Journal of Production Research*, Vol. 57, No. 7, pp. 2117-2135, 2019.

[131] N. Kshetri, 1 Blockchain's Roles in Meeting Key Supply Chain Management Objectives, *International Journal of Information Management*, Vol. 39, pp. 80-89, April, 2018.

[132] C. S. Tang, L. P. Veelenturf, The Strategic Role of Logistics in the Industry 4.0 Era, *Transportation Research Part E: Logistics and Transportation Review*, Vol. 129, pp. 1-11, September, 2019.

[133] J. Astill, R. A. Dara, M. Campbell, J. M. Farber, E. D. G.

Fraser, S. Sharif, R. Y. Yada, Transparency in Food Supply Chains: A Review of Enabling Technology Solutions, *Trends in Food Science & Technology*, Vol. 91, pp. 240-247, September, 2019.

[134] M. Kouhizadeh, J. Sarkis, Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains, *Sustainability*, Vol. 10, No. 10, Article No. 3652, October, 2018.

[135] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On Blockchain and Its Integration with IoT. Challenges and Opportunities, *Future Generation Computer Systems*, Vol. 88, pp. 173-190, November, 2018.

[136] I. Eyal, E. Sirer, Majority Is Not Enough: Bitcoin Mining Is Vulnerable, *18th International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, 2014, pp. 436-454.

[137] E. Kiktenko, N. Pozhar, M. Anufriev, A. Trushechkin, R. Yunusov, Y. Kurochkin, A. Lvovsky, A. Fedorov, Quantum-secured blockchain, *Quantum Science and Technology*, Vol. 3, No. 3, Article No. 035004, July, 2018.

[138] W. Yin, Q. Wen, W. Li, H. Zhang, Z. Jin, An Anti-Quantum Transaction Authentication Approach in Blockchain, *IEEE Access*, Vol. 6, pp. 5393-5401, January, 2018.

[139] F. Ablayev, D. Bulychkov, D. Sapaev, A. Vasiliev, M. Ziatdinov, Quantum-Assisted Blockchain, *Lobachevskii Journal of Mathematics*, Vol. 39, No. 7, pp. 957-960, September, 2018.

[140] W. Jung, S. Park, Preventing DDoS Attack in Blockchain System Using Dynamic Transaction Limit Volume, *International Journal of Control and Automation*, Vol. 10, No. 12, pp. 131-138, 2017.

[141] E. Jesus, V. Chicarino, C. Albuquerque, A. Rocha, A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack, *Security and Communication Networks*, Vol. 2018, Article No. 9675050, April, 2018.

[142] Y. Kano, T. Nakajima, A Novel Approach to Solve a Mining Work Centralization Problem in Blockchain Technologies, *International Journal of Pervasive Computing and Communications*, Vol. 14, No.1, pp. 15-32, April, 2018.

[143] L. Cheng, J. Liu, C. Su, K. Liang, G. Xu, W. Wang, Polynomial-Based Modifiable Blockchain Structure for Removing Fraud Transactions, *Future Generation Computer Systems*, Vol. 99, pp. 154-163, October, 2019.

[144] B. Huang, Z. Liu, J. Chen, A. Liu, Q. Liu, Q. He, Behavior Pattern Clustering in Blockchain Networks, *Multimedia Tools and Applications*, Vol. 76, No. 19, pp. 20099-20110, October, 2017.

[145] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When Mobile Blockchain Meets Edge Computing, *IEEE Communications Magazine*, Vol. 56, No. 8, pp. 33-39, August, 2018.

[146] C. Xu, K. Wang, M. Guo, Intelligent Resource Management in Blockchain-Based Cloud Datacenters, *IEEE Cloud Computing*, Vol. 4, No. 6, pp. 50-59, November-December, 2017.

[147] J. Park, D. Lee, H. In, Saving Deployment Costs of Smart Contracts by Eliminating Gas-wasteful Patterns, *International Journal of Grid and Distributed Computing*, Vol. 10, No. 12, pp. 53-64, 2017.

[148] L. Feng, H. Zhang, Y. Chen, L. Lou, Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain, *Applied Sciences*, Vol. 8, No. 10, Article No. 1919, October, 2018.

[149] L.-N. Lundbaek, D. Beutel, M. Huth, S. Jackson, L. Kirk, R. Steiner, Proof of Kernel Work: A democratic low-energy consensus for distributed access-control protocols, *Royal Society Open Science*, Vol. 5, No. 8, Article No. 180422, August, 2018.

[150] Y. Ren, Y. Liu, S. Ji, A. Sangaiah, J. Wang, Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks, *Mobile Information Systems*, Vol. 2018, Article No. 6874158, August, 2018.

[151] Q. Nasir, I. Qasse, M. Talib, A. Nassif, Performance Analysis of Hyperledger Fabric Platforms, *Security and Communication Networks*, Vol. 2018, Article No. 3976093, September, 2018.

[152] M. Dai, S. Zhang, H. Wang, S. Jin, A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain, *IEEE Access*, Vol. 6, pp. 22970-22975, March, 2018.

[153] Y. Kim, J. Jo, Binary Blockchain: Solving the Mining Congestion Problem by Dynamically Adjusting the Mining Capacity, in: R. Lee (Eds.), *Applied Computing and Information Technology*, *Studies in Computational Intelligence*, Vol. 727, Springer, 2018, pp. 29-49.

Biographies

Tuan-Vinh Le received the M.S. degree in business administration from the Department of Business Administration, National Formosa University, Taiwan. He is currently pursuing the Ph.D. degree with the Graduate Institute of Business and Management, Chang Gung University, Taiwan. He has some publications in *IEEE Access*, *Sensors*, and *Journal of Internet Technology*. His research interests include information security, communication system security, applied cryptography, cryptographic protocol, and blockchain. As an international student, he was granted a Full Scholarship for his M.S. degree in business administration from National Formosa University, in 2014, and a Full Scholarship for his Ph.D. degree in business and management from Chang Gung University, in 2016. He was a Session Chair of *MD2020* and a Reviewer of *IEEE Access*.

Chien-Lung Hsu received the M.S. and Ph.D. degrees in information management from the National Taiwan University of Science and Technology, in 1997 and 2002, respectively. From August 2009 to May 2012, he was the Director of the Chinese Cryptology and Information Security Association (CCISA), Taiwan. From August 2012 to July 2013, he was a Visiting Scholar with the Department of Electrical Engineering and Computer Science, University of Central Florida, USA. From August 2013 to August 2016, he was the Chair of the Department of Information Management, Chang Gung University, Taiwan. He is currently a joint Professor with the Department of Information Management, Graduate Institute of Business and Management, Chang Gung University. His research interests include smart home, smart healthcare, mobile commerce, computer and communication security, information security, applied cryptography, digital right management, auto identification technology, and user centered service. He received lots of honors, awards, certificates in terms of information security for his research, and has a great number of publications in his research related fields.