Blockchain-based Systems and Applications: A Survey

Jingyu Zhang[1], Siqi Zhong[1], Tian Wang[2], Han-Chieh Chao[3], Jin Wang[1,4]

[1] Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation, School of Computer & Communication Engineering, Changsha University of Science & Technology, China
[2] College of Computer Science and Technology, Huaqiao University, China
[3] Department of Electrical Engineering, National Dong Hwa University, Taiwan
[4] School of Information Science and Engineering, Fujian University of Technology, China
zhangzhang@csust.edu.cn, zhongsiqi@stu.csust.edu.cn, cs_tianwang@163.com, hcc@mail.ndhu.edu.tw, jinwang@csust.edu.cn

Abstract

Currently, many efforts have been done towards secure data privacy protection and reliable information trace, however the conventional solutions are still vulnerable to information loss, privacy leakage and other attacks till the blockchain technology emerged. Blockchain can record historical data by establishing a collectively maintained and tamper-resistant public ledger to ensure the security and reliability of the data stored in a distributed network. It realizes a decentralized network architecture, which can bring new solutions to many fields such as information tracing and privacy protection. In recent years, blockchain technology has gradually attracted the close attention of all industries, and this paper summarizes the existing blockchain-based systems and applications. We mainly review the applications of blockchain traceability technology in various fields, the blockchain decentralized applications, and other blockchain applications in data security protection, respectively. This work may bring new opportunities and challenges for the development of various industries in the future.

Keywords: Blockchain technology, Decentralized architecture, Blockchain applications, Privacy protection

1 Introduction

Blockchain technology originated from Bitcoin [1], and the original structure is shown in Figure 1. The blockchain is essentially a distributed database over peer-to-peer networks. In a blockchain system, the transaction data will be packed into blocks by miner nodes, and all blocks are linked together via hash operations. As shown in Figure 1, a complete original block is composed of block header and block body. The block header encapsulates the metadata for identifying, and it mainly includes three groups of important metadata. The block body contains the details of each transaction and the complete Merkle tree, so that each transaction can be traced and queried. Table 1 details the data structure in each block.

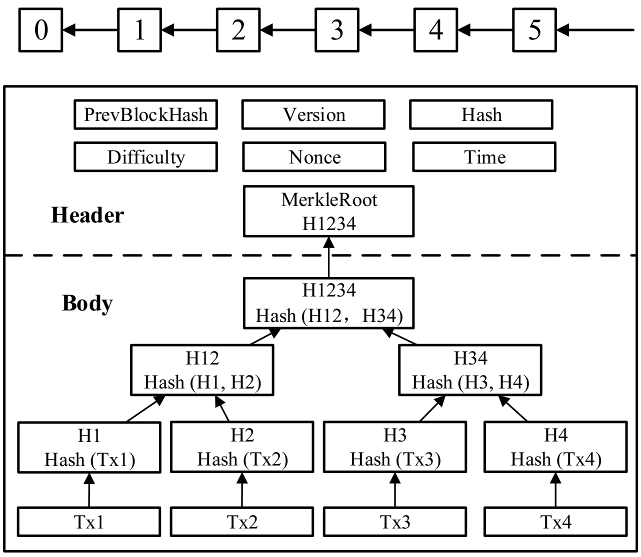


Figure 1. Blockchain logic structure and block composition

*Corresponding Author: Jin Wang; E-mail: jinwang@csust.edu.cn
DOI: 10.3966/160792642020012101001

Table 1. Block data structure

Type	Function	Item	Description
Block header	Retrieve historical information as a hash pointer.	PrevBlockHash	The hash value of the parent block by which each block can point to its previous block.
	Block identification.	Hash	The block header hash value of this block that can be used as a unique identifier for the current block.
	The relevant important data of PoW (Proof of Work).	Difficulty	Difficulty target value of PoW for this block
		Nonce	A value used for the PoW, and the process of PoW is essentially the process of finding the nonce that meet the requirements.
		Timestamp	Approximate time when miners generate the block.
	Verify the correctness of the transactions in the block.	Merkle root	Merkle root hash value for all transactions in this block. As long as only one transaction changes, the Merkle tree root value will also change.
Block body	Verify the correctness of each transaction in the block.	Merkle tree	Merkle tree is a binary tree made up of hashes for all transactions to efficiently verify the integrity of large data sets.
	Protect transactions and trade blocks.	Digital signature	Digital signature is an encryption mechanism used to verify the authenticity and integrity of numbers and data.

Blockchain stores all transactions in a peer-to-peer network [2] in a secure, verifiable, and transparent manner [3]. A complete blockchain system includes many technologies (e.g., the consensus algorithms, proof-of-work mechanisms, digital signature, timestamp technology). The blockchain system has the following characteristics: (1) Decentralization: The whole network does not rely on a centralized hardware or management organization; (2) Reliable database: All the full nodes hold a complete blockchain, and the destruction of one node does not affect the data integrity of the whole database; (3) Collective maintenance: The whole blockchain network is maintained by all the nodes, unless the malicious nodes exceed 50% of the computing power of the whole network, they will not be able to tamper with the historical data; (4) Security and credibility: Once the data is verified, it will be permanently saved in the blockchain database, and it can not be tampered with; (5) Anonymity: The nodes follow a fixed algorithm, and the parties do not need to disclose their identities.

According different application scenarios, the development of blockchain can be divided into three stages, which are called Blockchain 1.0, Blockchain 2.0 and Blockchain 3.0 respectively. Blockchain 1.0 is the era of virtual cryptocurrency represented by Bitcoin, which focuses on secure online electronic payment. Blockchain 2.0 refers to smart contracts, which combine with cryptocurrency to provide a broader application scenario for the financial business. In December 2013, Vitalik Buterin [4] developed the public Blockchain 2.0 platform, which is called Ethereum [5], which uses the smart contracts to provide the traceability and the tamper-resistance in decentralized and trusted environment [6]. Blockchain 3.0 refers to the application scenarios in various industries outside the financial industry, which can satisfy more complex business demand. At Blockchain 3.0 stage, how to use blockchain technology to tackle the pain points and difficulties in various fields has been widely concerned by researchers. This paper summarizes the existing applications and systems based on blockchain technology, we hope our work can provide some insights and help for the current and future research.

The rest of this paper is organized as follows. Section 2 introduces the combination of blockchain and traceability technology, including the applications in the fields of property management and asset delivery. In Section 3, the decentralized applications in blockchain systems are introduced. Section 4 introduces the blockchain-based applications for data security and data privacy protection. Section 5 summarizes this paper.

2 Blockchain-based Traceable Anti-counterfeiting Systems

The traditional traceable anti-counterfeiting system [7] is mainly based on QR (Quick Responce) code and RFID (Radio Frequency Identification) technology. These methods adopt centralized data storage to manage the product information, which can not track the product data reliable and lacks of the consumers' trust. Blockchain provides the new solutions for the above problems with its decentralized secure storage. Integrating the timestamp, blockchain can build the trust in the decentralized environment, verify the transactions, and make the blockchian database easy to track back and unforgeable.

2.1 Blockchain-based Supply Chain Traceable Systems

Nowadays, with the rapid development of information technology and other Internet technologies, the centralized supply chain management system is not enough to meet the requirements of consumers on product quality management. Most of the research focuses on improving the rate of RFID [8-9] and the security of RFID protocols [10-11]. However, these protocols are only applicable to various RFID applications that rely on centralized databases. The decentralized architecture of blockchain can solve data storage isolation and the lack of trust when the traditional supply chain management system involves multiple parties [12].

In order to successfully fuse RFID and blockchain technologies together, a secure method of communication is required between the RFID tagged goods and the blockchain nodes, and the communication protocol between nodes should also have robustness [13]. [14] proposed a robust ultra-lightweight mutual authentication RFID protocol that works together with a decentralized database to create a secure blockchain-based supply chain management system. Wang et al. [15] proposed a novel blockchain-based mutual authentication security protocol, which can apply to distributed RFID systems with high security demand and relatively low real-time requirement. The work in [16] provided a verifiable ownership transfer of products attached with the RFID tags using blockchain technology to address various security requirements.

Customer information analysis is critical for the companies in the increasingly fierce market competition [17]. However, the supply chain contains many different participants, which makes the information sometimes distorted step by step. Therefore, it is urgent to introduce new technologies [18-20] to realize data security in supply chain systems. Lin et al. [21] proposed a food safety traceability prototype system based on blockchain and electronic product code information service. IoT (Internet of Things) is another hot topic in current work [22-24], the management architecture of on-chain and off-chain data can alleviate the blockchain data explosion in IoT field.

Blockchain can solve the fraud problem [25] in business and the inadequate market supervision problem. The paper [26] deployed public auditable contracts in a blockchain system that increased the transparency with respect to the access and usage of data. Through this approach, the data accountability and tracking in supply chain management can be realized. In [27], a new solution to link legal documentation and blockchain technology within a traceability system was proposed. The novelty of this method is to change the normal blockchain into the two-factor blockchain, so as to improve the reliability of the whole product tracking system. In view of the difficulties caused by the complexity of supply chain interaction on organization management, [28] proposed a novel supply chain operation model based on blockchain and big data management, to improve the integrity and speed of supply chain data.

Based on the above analysis, we summarize the structures of supply chain traceability system based on blockchain in Figure 2, and we present the functions of each node in Table 2.

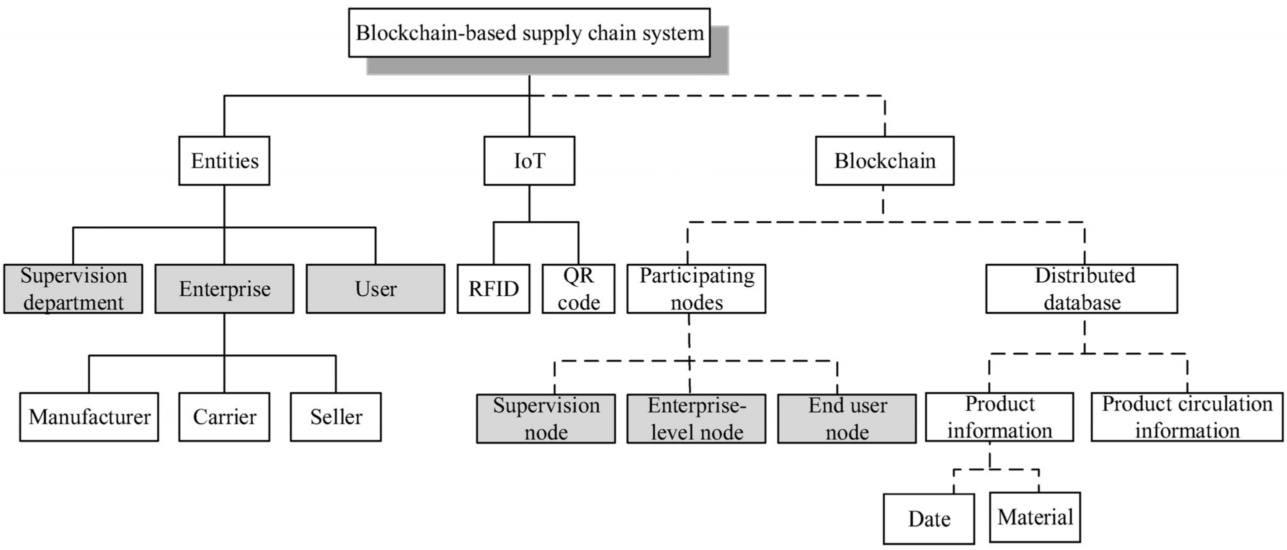


Figure 2. Blockchain-based supply chain system structure

Table 2. Functions of all nodes in blockchain-based supply chain system

Node type	Participator	Node permissions and functions					
		Write	Read	Verification	Analysis	Process supervision	Trade supervision
Enterprise node	Supplier	Yes	Yes	Yes	Yes	No	No
	Manufacturer	Yes	Yes	Yes	Yes	No	No
	Seller	Yes	Yes	Yes	Yes	No	No
	Carrier	Yes	Yes	Yes	Yes	No	No
End user node	Consumer	No	Yes	No	No	No	No
	Visitor	No	Yes	No	No	No	No
Supervisor node	Market supervision department	No	Yes	No	No	Yes	Yes
	Legal supervision department	No	Yes	No	No	Yes	Yes

2.2 Blockchain-based Intellectual Property Management Systems

With the rapid development of modern networks, malicious image tampering technologies [29-33] have emerged. At the same time, a large number of pirated books and videos have been spread. Such security loopholes cause people to question the protection of data privacy in the intellectual property industry. At present, most solutions [34] are proposed in a centralized way to protect intellectual property, which can not eliminate these phenomena fundamentally.

The intellectual property protection in the multimedia field is very weak, and researchers have done a lot of work [35] in this field. Many researchers think that the key problem is how to protect data from unauthorized access, and how to prove the authority of user data. Based on this, [36] proposed a data protection architecture and protocol based on blockchain, which defines a new effective framework. The framework allows the user to not only store data but also to query, share and audit the data as well. The hiding technique [37] provides a basic security service for digital videos. To avoid external centralized attacks, Zhao et al. [38] proposed a blockchain-based data hiding method for digital video protection, which improves the integrity authentication of confidential data and videos.

The centralized registration of Copyright Office has following disadvantages: high service cost, long processing time and easy to be tampered with registration records. Centralized cloud storage management has improved the registration systems by some methods, such as encryption protection [39] and optimization [40-41], and blockchain also did some related further work [42]. Zeng et al. [43] proposed a new digital image copyright registration architecture based on the consortium blockchain. The improvement of digital copyright protection system based on digital watermarking mainly focused on algorithms, while generation and storage of the watermark information was ignored. Based on the insight, Meng et al. [44] proposed a improved design scheme for blockchain copyright management systems based on digital watermarking and its information. Paper [45] established a blockchain record preservation method to protect the originality. In this work, they constructed the verifiable storage system using blockchain technology.

2.3 Blockchain-based Applications for Asset Delivery

In recent decades, asset delivery usually relies on the third-party trust institution to supervise and prove the transaction process. This centralized trust institution has some trust problems such as missing transaction records and forged information. Blockchain is known as a new trusted and secure platform [46-47] for recording the transfer of all asset types in the digitized world.

At present, some researchers have used blockchain technology to improve the asset delivery certification systems. [48-50] proposed new decentralized PoD solutions for digital asset certification. In order to trace and track physical items, Pop et al. [51] proposed an improved blockchain-based solution that solves the drawbacks of the centralized stock exchange architecture. Utz et al. [52] addressed the coordination of assets, equipment, and stakeholders in the energy market by introducing a blockchain-based smart contract ecosystem.

In order to provide an effective way to manage and retrieve digital asset, [53] proposed a new digital asset management platform with transaction-based access control. Tran et al. introduced model-driven engineering tools [54] which can be used to implement business processes to manage assets on the blockchain. Based on existing research, the work in [55] introduced a built-in mechanism to reduce the transaction risks caused by the irreversibility of transactions in blockchain systems.

In general, the blockchain-based solutions provide the proof for the asset delivery and transactions traded between two individual parties. The interactive relationship of each role in the blockchain-based asset delivery management system is shown in Figure 3, which also shows the implementation process of asset delivery.

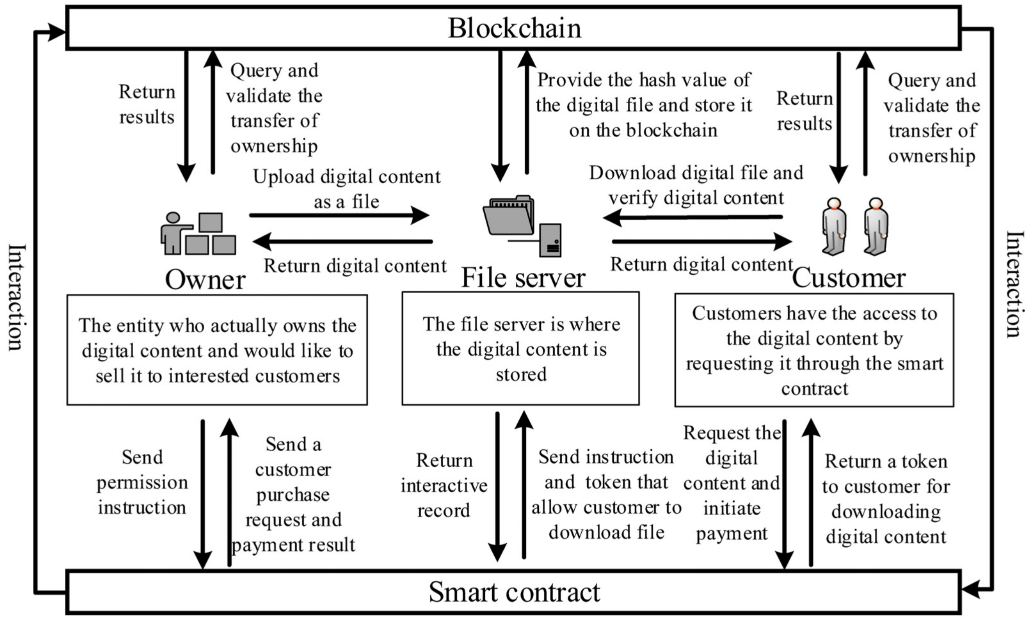


Figure 3. Implementation process of blockchain-based asset delivery

3 Decentralized Applications Based on Blockchain

With the development of blockchain technology and Blockchain 3.0, a lot of decentralized applications emerge, including decentralized social networks, decentralized trading systems and decentralized insurance services. EVS (Electronic Voting System) is the most typical application, and we mainly discuss it in this section. EVS as distributed audit layer [56] is expected to be verifiable and tamper-resistant [57]. Blockchain technology can provide transparency for such services, while preventing agent tampering with electoral electronic data.

To combine blockchain technology with electronic voting, a new reliable decentralized voting protocol [58-59] is introduced. In terms of vote confidentiality and integrity and validity verification, [60] proposed a practical platform-independent secure and verifiable voting system that can be deployed on any blockchain systme that supports an execution of a smart contract. Yu et al. [61] proved that blockchain technology, combined with modern cryptography can provide the transparency, integrity and confidentiality required from reliable online voting. In [62], Panja et al. modified the DRE-ip [63] system, and presented a novel cryptographic technique for an authenticated, end-to-end verifiable and secret ballot election. Fusco et al. [64] proposed an e-voting system [65] named Crypto-voting. This solution is based on a secret sharing approach, and needs to be implemented using the blockchain technology.

Existing voting solutions have different issues, and significant one is lack of transparency and auditability [66]. Blockchain technology brings the new solution for it. [67] presented an auditable blockchain voting system, which describes e-voting processes and components of a supervised Internet voting system that is audit and verification capable. This method is designed through utilization of blockchain technology and voter-verified paper audit trail. Multi-proxy signature [68] is a variant of proxy signature, which allows that a delegator can manage his signing rights to many proxy signers. On this basis, [69] further studid the work of [67] and resented a new design in auditable blockchain voting system, which is a end-to-end verifiable and auditable blockchain-based supervised Internet voting system.

The decentralized voting application model is shown in Figure 4. With the decentralized distributed features of blockchain, users can vote for specific candidates in an distributed environment, and each vote will be recorded on the blockchain. To sum up, the blockchain-based voting system described in the research and analysis can be depicted as follows:

(1) Voters' votes can not be tampered with;

(2) Candidates' votes can not be tampered with;

(3) Votes are authentic, reliable and can not be forged;

(4) Voting results can be queried and verified.

According to the above, blockchain can make the voting systems more transparent, fairer and more open.

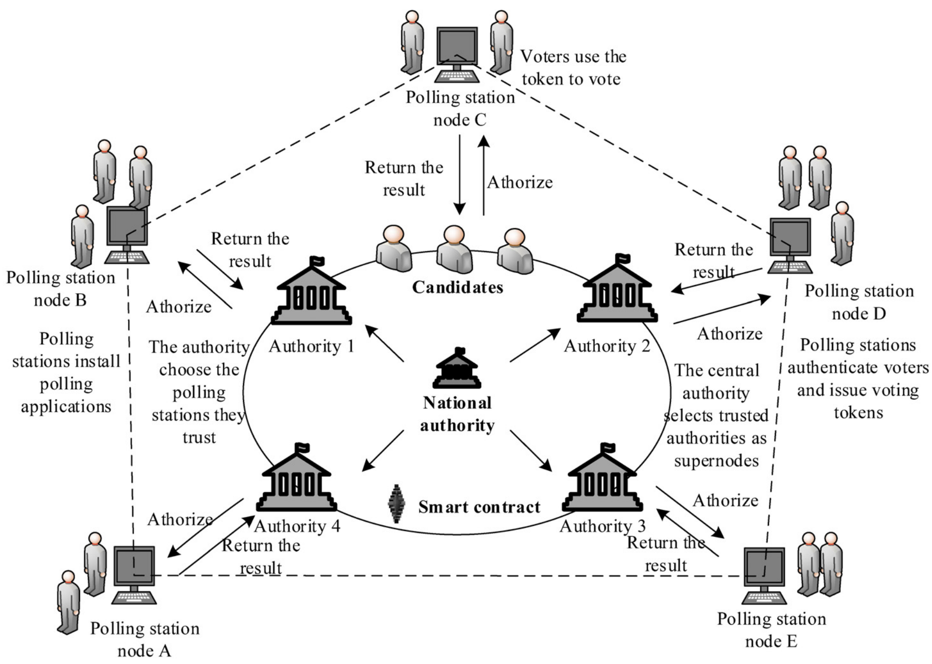


Figure 4. Blockchain-based EVS network

4 Decentralized Applications in the Data Security Field

The rise of big data era has led to the explosive growth of data scale in all walks of life [70-71]. Meanwhile, the trust has become the biggest problem of big data, which will hinder the secure data transmission. Blockchain technology provides a new solution to the problem of data security and privacy protection, which combines the features of tamper-resistance and traceability. In blockchain systems, smart contracts can automatically execute default instructions to ensure the safe storage and transmissions of data resources. This section reviews the research in finance, IoT and healthcare. At the end of this section, we will summarize relevant technologies and development prospects.

4.1 Blockchain in the Financial Industry

Data privacy protection has always been a key security issue in the financial industry. Even though many privacy protection schemes [72-73] have been proposed, traditional data storage is still centralized and can not solve the essential problem, and the emerging blockchain presents some new solutions.

At present, the use of blockchain in moblie enviroment is still limited, because the limitation of computing and energy resources. [74] developed an optimal auction based on deep learning for the edge resource allocation. In [75], Jiao et al. Presented an edge computing service to support the mobile blockchain. They [76] futher focused on the trading between the cloud/fog computing service providers and miners, and proposed an auction-based market model for efficient computing resource allocation. The inherent transparency and the lack of privacy posed a great challenge for many financial applications, In [77], the authors tackled this challenge and presented a smart contract for a verifiable sealed-bid auction on the Ethereum. Based on the typical auction security requirements, Blass et al. [78] proposed a new auction protocol running on the blockchain to ensure the bidding confidentiality of the completely malicious party. Xia et al. [79] proposed a secure payment routing protocol for economic systems based on blockchain.

Traditional WSN data [80-81] processing platforms handle the data in centralized way which is vulnerable to attacks. Blockchain provides the distributed databases. [82] proposed a blockchain-based distributed collocation storage architecture for data security processing platform of WSN with consensus protocol and asymmetric signature scheme. Digital banking as an essential service is hard to access in remote areas. Hu et al. [83] proposed a blockchain-based digital payment scheme that can deliver reliable services on the top of unreliable networks in remote regions. To tackle the problem of fast payment, [84] proposed FastPay, a solution for achieving secure fast payments in blockchain-backed edge-IoT systems. Real-time gross settlement system is the cornerstone of inter-bank payment business. [85] introduced an end-to-end inter-bank payment systems prototype based on Hyperledger Fabric enterprise blockchain platform. In the existing online payment systems, some information such as reputation could be manipulated by the malicious. In [86], Ahn et al. proposed Reptor, a model for calculation of trust and reputation with the values stored on blockchain-based payment system ledger.

Currently, blockchain-based applications mainly focus on solving the problems of data security in the financial field and the security of payment system. How to effectively supervise the financial blockchain still needs to be well studied.

4.2 Blockchain-based Applications of IoT

There are various insecure factors in the Internet that make IoT devices vulnerable to attacks. Researchers improve and optimize the IoT device network in terms of network security and algorithms [87-91], which still lack an effective means to prevent attacks and privacy leaks. Blockchain technology is expected to become a promising way to alleviate the data security problems in the IoT. Figure 5 summarizes blockchain features integrated with IoT.

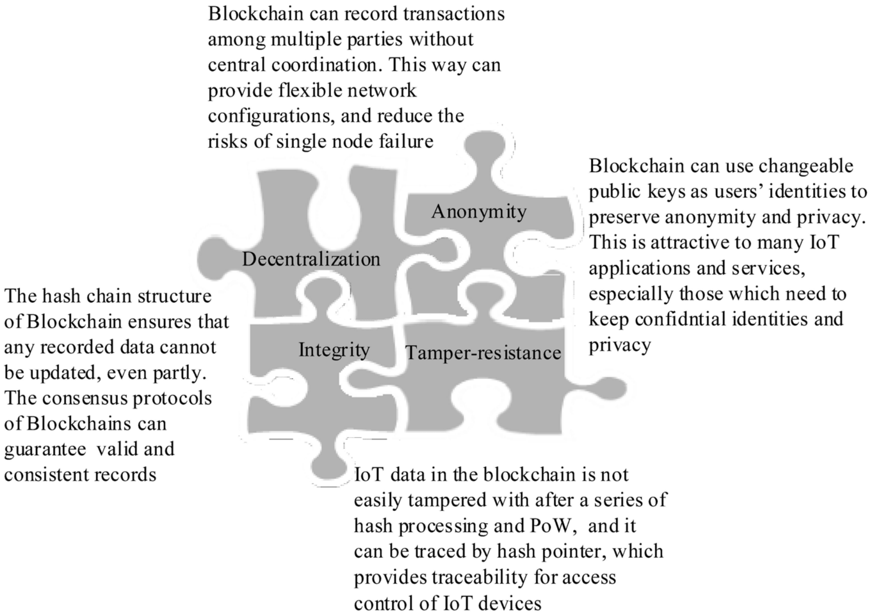


Figure 5. Blockchain features integrated with IoT

Based on the existing knowledge and privacy protection schemes [92-93], [94] proposed a design theory for a blockchain-based sensor data protection system that enables data certification. Blockchain technology can be used as access management technology [96], and Yu et al. [95] proposed an improved interference-aware and robust access control method of IoT devices. In [97], Cha et al. proposed a powerful blockchain design which securely maintains user privacy preferences for IoT devices. [98] proposed a novel attribute-based access control scheme for IoT systems. [99] adopted fingerprint identification technology for privacy control. [100] proposed a novel blockchain-based distributed key management architecture to reduce access latency. In [101], Rathee et al. used a blockchain-based mechanism to extract information from IoT devices. One of the important networks in IoT is wireless sensor network. In [102], the blockchain technology is utilized to build the first incentive mechanism of nodes as per data storage for wireless sensor networks [103-105]. [106] designed a new smart contract for multi-party power resources bidding based on blockchain technology.

Generally, IoT is a centralized system whose security and performance mainly rely on centralized servers. To solve the problem, in [107], a blockchain-based identity management and access control mechanism is designed via edge computing. IoT devices are mostly mobile devices [108], a new mechanism combing blockchain with regeneration coding is proposed [109] to improve the security and reliability of stored data for edge computing. Ramezan et al. [110] proposed a novel blockchain-based contractual routing protocol for a network of untrusted IoT devices. There still are the needs to profile the energy consumption of blockchains, protect IoTs and analyze energy-performance trade-offs. Towards the goals, [111] profiled the impact of workloads based on smart contract. As IoT devices are increasingly connected to the system [112], it is difficult to coordinate external computing resources to improve the performance of IoT, and [113] proposed a novel blockchain-based threshold IoT service system: BeeKeeper. [114] presentd a multi-layer secure IoT network model based on blockchain technology.

The purpose of using blockchain technology is to solve the problems of data privacy and data security in the IoT. Combining with blockchain technology, the traditional ecosystem of the IoT can be further improved, and the IoT devices can run with higher efficiency and security.

4.3 Medical Data Protection Based on Blockchain

With the fast development of information technology, medical institutions have used electronic information systems to manage the patient data. Medical data protection based on blockchain has great development potential. To achieve confidentiality, authentication, integrity of medical data, and support fine-grained access control, Wang et al. [115] proposed a secure electronic health record system based on attribute-based cryptosystem and blockchain technologies. In order to breaking the information isolation phenomenon of medical data, [116] designed a storage scheme to manage personal medical data based on blockchain and cloud storage. Furthermore, the authors described a useful service framework for sharing medical records. Fan et al. also proposed a blockchain-based information management system, MedBlock in [117] to handle patient information. Li et al. [118] proposed a novel blockchain-based data preservation system for medical data. [119] designed a new systems based on blockchain to provide reliable storage solution and data collection.

Ji et al. [120] investigated the location sharing based on blockchains for telecare medical information systems. Then they proposed a blockchain-based multi-level location sharing scheme, using order-preserving encryption and merkle tree. In order to handle the protected health information generated by medical IoT devices, Griggs et al. [121] created a new system where the sensors communicate with a smart device using a private blockchain based on the Ethereum. In [122], Azaria et al. proposed MedRec: a novel, decentralized record management system to handle electronic medical records based on blockchain technology. The system gives patients comprehensive, immutable log and is easy to access.

In order to facilitate the reading, Table 3 summarizes and compares the above several blockchain-based management systems in different fields.

Table 3. Comparison of different blockchain-based applications

Fields	Applications	Targets	Advantages
IoT	BeeKeeper: Blockchain-Based IoT System	To provide a secure storage and homomorphic computation.	(1) Servers can process a user's data by performing homomorphic computations on the data without learning anything from them. (2) Any node can become a leader's server if the node and the leader desire.
	Blockchain Connected Gateway	(1) To achieve secure management of privacy preferences. (2) To resolve privacy disputes.	(1) It design a robust digital signature mechanism for authentication and secure management (2) This way improve user privacy and trust in IoT applications while legacy IoT devices are still in use.
Payment	Blockchain-Based Secure Payment Routing Protocol	To build a secure and scalable routing protocol for transfer of funds between clients in a micropayment network.	It can realize a kind of low cost and expansible bidirectional micropayment transactions.
	Inter-Bank Payment System on Enterprise Blockchain Platform	To provide higher level of payment settlement service.	The system supports gross settlement, gridlock resolution, and reconciliation for inter-bank payment business.
Auction	Optimal Auction Approach in Mobile Blockchain Networks	To develope an optimal auction based on deep learning for the edge resource allocation.	It constructs a multi-layer neural network architecture based on an analytical solution of the optimal auction.
	Strain: Secure Auction for Blockchains	To meet auction security requirements such as non-retractable bids against fully-malicious adversaries.	Efficiency and low blockchain latency.
Healthcare	Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain	(1) To achieve confidentiality, authentication, integrity of medical data. (2) To support fine-grained access control.	(1) The system uses identity-based signature to implement digital signatures. (2) The system uses attribute-based encryption and identity-based encryption to encrypt medical data.
	Blockchain-Based Medical Records Secure Storage and Medical Service Framework	To provide a distributed and decentralized way to store and manage medical data.	(1) Blockchain in this system recorded index information of medical data and transaction records. (2) Large medical data are encrypted and stored in cloud storage under the chain in the framework.

Table 3. Comparison of different blockchain-based applications (continue)

Fields	Applications	Targets	Advantages
Healthcare	Blockchain-Based Medical Data Preservation System	(1) To provide a storage scheme to manage personal medical data based on blockchain and cloud storage. (2) To provide a service framework for sharing medical records. (3) To guarantee user privacy.	(1) The system ensures the data are consistent with the user local's after submission and preserve important data in perpetuity. (2) The system prevents data from being tampered with, forged or deleted.
	Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme	(1) To achieves a decentralized management. (2) To achieves unforgeability of patients' location records. (3) To realize privacy-preserving location sharing based on blockchains for telecare medical information systems.	The system builts a blockchain-based multi-level location sharing scheme by using order-preserving encryption and merkle tree.
	Healthcare Blockchain System Using Smart Contracts	To handle the protected health information generated by medical IoT devices.	The system can support real-time patient monitoring and medical interventions.

5 Conclusion

Through the combination of various computer technologies, blockchain has formed a new technology architecture, which realizes the decentralized secure storage systems. Compared with the traditional centralized models, the decentralized models of blockchain can solve the trust-lacking problems in the traditional centralized institutions, and improve the data security. Blockchain can alleviate the centralization of cloud services and cloud storage, and can also benefit various industries. This paper summarized the systems and applications based on blockchain in numerous fields. As investigated by the above studies, blockchain will contribute to improving the solutions in multiple fields such as the IoT, smart city and supply chain systems. It will also bring new opportunities and challenges for the development of various industries in the future.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61802031, 61772454, 61811530332, 61811540410). It was also supported by the open research fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education (No. JZNY201905).

References

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.

[2] J. Zou, H. Zhang, Y. Tang, L. Li, T. Liu, H. Chen, L. Qu, X. Zheng, *Blockchain Technology Guide*, China Machine Press, 2018.

[3] J. Al-Jaroodi, N. Mohamed, Blockchain in Industries: A Survey, *IEEE Access*, Vol. 7, pp. 36500-36515, March, 2019.

[4] W. Chen, Z. Zheng, E. C. Ngai, P. Zheng, Y. Zhou, Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum, *IEEE Access*, Vol. 7, pp. 37575-37586, March, 2019.

[5] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, https://github.com/ethereum/wiki/wiki/white-paper.

[6] N. Szabo, *The Idea of Smart Contracts*, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

[7] J. Ding, H. Xu, P. Li, F. Zhu, Research on Food Safety Traceability Technology Based on RFID Security Authentication and 2-Dimensional Code, *Proceedings of the 12th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIs)*, Matsue, Japan, 2018, pp. 517-526.

[8] L. Arjona, H. Landaluce, A. Perallos, E. Onieva, Timing-Aware RFID Anti-Collision Protocol to Increase the Tag Identification Rate, *IEEE Access*, Vol. 6, pp. 33529-33541, June, 2018.

[9] M. A. Bonuccelli, F. Martelli, A Very Fast Tags Polling Protocol for Single and Multiple Readers RFID Systems and Its Applications, *Ad Hoc Networks*, Vol. 71, pp. 14-30, March, 2018.

[10] Z. Shen, P. Zeng, Y. Qian, K. R. Choo, A Secure and Practical RFID Ownership Transfer Protocol Based on Chebyshev Polynomials, *IEEE Access*, Vol. 6, pp. 14560-14566, February, 2018.

[11] Y. Naija, V. Beroulle, M. Machhout, Security Enhancements of a Mutual Authentication Protocol Used in a HF Full-Fledged RFID Tag, *Journal of Electronic Testing*, Vol. 34,

No. 3, pp. 291-304, June, 2018.

[12] Q. Lu, X. Xu, Adaptable Blockchain-based Systems: A Case Study for Product Traceability, *IEEE Software*, Vol. 34, No. 6, pp. 21-27, November/December, 2017.

[13] Y. Chen, J. Wang, R. Xia, Q. Zhang, Z. Cao, K. Yang, The Visual Object Tracking Algorithm Research Based on Adaptive Combination Kernel, *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, No. 12, pp. 4855-4867, December, 2019.

[14] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, J. H. Khor, Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains, *IEEE Access*, Vol. 7, pp. 7273-7285, January, 2019.

[15] S. Wang, S. Zhu, Y. Zhang, Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems, *2018 IEEE Symposium on Computers and Communications (ISCC)*, Natal, Brazil, 2018, pp. 74-77.

[16] S. Anandhi, R. Anitha, S. Venkatasamy, RFID Based Verifiable Ownership Transfer Protocol Using Blockchain Technology, *IEEE Cyber, Physical and Social Computing (CPSCom)*, Halifax, NS, Canada, 2018, pp. 1616-1621.

[17] B. Yin, K. Gu, X. Wei, S. Zhou, Y. Liu, A Cost-Efficient Framework for Finding Prospective Customers Based on Reverse Skyline Queries, *Knowledge-based Systems*, Vol. 152, pp. 117-135, July, 2018.

[18] Y. Fu, J. Zhu, Big Production Enterprise Supply Chain Endogenous Risk Management Based on Blockchain, *IEEE Access*, Vol. 7, pp. 15310-15319, January, 2019.

[19] G. Perboli, S. Musso, M. Rosano, Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases, *IEEE Access*, Vol. 6, pp. 62018-62028, October, 2018.

[20] R. Bettín-Díaz, A. E. Rojas, C. Mejía-Moncayo, Methodological Approach to the Definition of a Blockchain System for the Food Industry Supply Chain Traceability, *International Conference on Computational Science and Its Applications (ICCSA)*, Melbourne, VIC, Australia, 2018, pp. 19-33.

[21] Q. Lin, H. Wang, X. Pei, J. Wang, Food Safety Traceability System Based on Blockchain and EPCIS, *IEEE Access*, Vol. 7, pp. 20698-20707, February, 2019.

[22] H. Liu, L. T. Yang, J. Chen, M. Ye, J. Ding, L. Kuang, Multivariate Multi-Order Markov Multi-Modal Prediction With Its Applications in Network Traffic Management, *IEEE Transactions on Network and Service Management*, Vol. 16, No. 3, pp. 828-841, September, 2019.

[23] H. Liu, L. T. Yang, J. Ding, Y. Guo, S. S. Yau, Tensor-train-based High-order Dominant Eigen Decomposition for Multimodal Prediction Services, *IEEE Transactions on Engineering Management*, PP(99), pp. 1-15, July, 2019, DOI: 10.1109/TEM. 2019.2912928.

[24] J. Ding, H. Liu, L. T. Yang, T. Yao, W. Zuo, Multi-user Multivariate Multi-order Markov Based Multi-modal User Mobility Pattern Prediction, *IEEE Internet of Things Journal*, November, 2019, DOI: 10.1109/JIOT.2019.2951134.

[25] 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, 3133, September, 2018.

[26] R. Neisse, G. Steri, I. N. Fovino, A Blockchain-based Approach for Data Accountability and Provenance Tracking, *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES)*, Reggio Calabria, Italy, 2017, pp. 1-10.

[27] A. A. Arsyad, S. Dadkhah, M. Köppen, Two-Factor Blockchain for Traceability Cacao Supply Chain, *International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, Bratislava, Slovakia, 2018, pp. 332-339.

[28] M. A. Rubio, G. M. Tarazona, L. E. Bravo, Big Data and Blockchain Basis for Operating a New Archetype of Supply Chain, *Data Mining and Big Data (DMBD)*, Shanghai, China, 2018, pp. 659-669.

[29] D. Zhang, Z. Liang, G. Yang, Q. Li, L. Li, X. Sun, A Robust Forgery Detection Algorithm for Object Removal by Exemplar-based Image Inpainting, *Multimedia Tools & Applications*, Vol. 77, No. 10, pp. 11823-11842, May, 2018.

[30] D. Zhang, T. Yin, G. Yang, M. Xia, L. Li, X. Sun, Detecting Image Seam Carving with Low Scaling Ratio Using Multi-Scale Spatial and Spectral Entropies, *Journal of Visual Communication and Image Representation*, Vol. 48, pp. 281-291, October, 2017.

[31] D. Zhang, G. Yang, F. Li, J. Wang, A. K. Sangaiah, Detecting Seam Carved Images Using Uniform Local Binary Patterns, *Multimedia Tools and Applications*, pp. 1-16, July, 2018.

[32] L. Xiang, W. Wu, X. Li, C. Yang, A Linguistic Steganography Based on Word Indexing Compression and Candidate Selection, *Multimedia Tools and Applications*, Vol. 77, No. 21, pp. 28969-28989, November, 2018.

[33] L. Xiang, X. Wang, C. Yang, P. Liu, A Novel Linguistic Steganography Based on Synonym Run-length Encoding, *IEICE Transactions on Information and Systems*, Vol. E100-D, No. 2, pp. 313-322, February, 2017.

[34] Q. Yang, F. Peng, J. Li, M. Long, Image Tamper Detection Based on Noise Estimation and Lacunarity Texture, *Multimedia Tools and Applications*, Vol. 75, No. 17, pp. 10201-10211, September, 2016.

[35] W. Tsai, L. Feng, H. Zhang, Y. You, L. Wang, Y. Zhong, Intellectual-Property Blockchain-Based Protection Model for Microfilms, *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, San Francisco, CA, USA, 2017, pp. 174-178.

[36] A. Vishwa, F. K. Hussain, A Blockchain Based Approach for Multimedia Privacy Protection and Provenance, *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, Bangalore, India, 2018, pp. 1941-1945.

[37] D. Taranovsky, Data Hiding and Digital Watermarking, in: J. Chen, W. Cranton, M. Fihn (Eds.), *Handbook of Visual Display Technology*, Springer, 2012, pp. 387-399.

[38] H. Zhao, Y. Liu, Y. Wang, X. Wang, J. Li, A Blockchain-Based Data Hiding Method for Data Protection in Digital Video, *International Conference on Smart Blockchain (SmartBlock)*, Tokyo, Japan, 2018, pp. 99-110.

[39] T.-Y. Wu, C.-M. Chen, K.-H. Wang, C. Meng, E. Wang, A Provably Secure Certificateless Public Key Encryption with Keyword Search, *Journal of the Chinese Institute of Engineers*, Vol. 42, No. 1, pp. 20-28, January, 2019.

[40] J.-S. Pan, C.-Y. Lee, A. Sghaier, M. Zeghid, J. Xie, Novel Systolization of Subquadratic Space Complexity Multipliers Based on Toeplitz Matrix-Vector Product Approach, *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 27, No. 7, pp. 1614-1622, July, 2019.

[41] Z. Meng, J.-S. Pan, K.-K. Tseng, PaDE: An Enhanced Differential Evolution Algorithm with Novel Control Parameter Adaptation Schemes for Numerical Optimization, *Knowledge-Based Systems*, Vol. 168, pp. 80-99, March, 2019.

[42] B. Bodó, D. Gervais, J. P. Quintais, Blockchain and Smart Contracts: The Missing Link in Copyright Licensing, *International Journal of Law and Information Technology*, Vol. 26, No. 4, pp. 311-336, Winter, 2018.

[43] J. Zeng, C. Zuo, F. Zhang, C. Li, L. Zheng, A Solution to Digital Image Copyright Registration Based on Consortium Blockchain, *Chinese Conference on Image and Graphics Technologies (IGTA)*, Beijing, China, 2018, pp. 228-237.

[44] Z. Meng, T. Morizumi, S. Miyata, H. Kinoshita, Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain, *IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Tokyo, Japan, 2018, pp. 359-364.

[45] A. Schönhals, T. Hepp, B. Gipp, Design Thinking Using the Blockchain: Enable Traceability of Intellectual Property in Problem-Solving Processes for Open Innovation, *CryBlock'18: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CRYBLOCK@MobiSys)*, Munich, Germany, 2018, pp. 105-110.

[46] M. Murray, An Examination of the Blockchain, the Emerging Technology that Promises to Transform Digital Tracking of Assets, *Twenty-fourth Americas Conference on Information Systems (AMCIS)*, New Orleans, LA, USA, 2018, pp. 1-1.

[47] Z. Ren, K. Cong, T. Aerts, B. Jonge, A. Morais, Z. Erkin, A Scale-Out Blockchain for Value Transfer with Spontaneous Sharding, *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, 2018, pp. 1-10.

[48] H. R. Hasan, K. Salah, Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts, *IEEE Access*, Vol. 6, pp. 65439-65448, October, 2018.

[49] H. R. Hasan, K. Salah, Blockchain-Based Solution for Proof of Delivery of Physical Assets, *2018 International Conference on Blockchain (ICBC)*, Seattle, USA, 2018, pp. 139-152.

[50] 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.

[51] C. Pop, C. Pop, A. Marcel, A. V. Vesa, T. Petrican, T. Cioara, I. Anghel, I. Salomie, Decentralizing the Stock Exchange Using Blockchain an Ethereum-based Implementation of the Bucharest Stock Exchange, *2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP)*, Cluj-Napoca, Romania, 2018, pp. 459-466.

[52] M. Utz, S. Albrecht, T. Zoerner, J. Strüker, Blockchain-Based Management of Shared Energy Assets Using a Smart Contract Ecosystem, *International Conference on Business Information Systems (BIS)*, Berlin, Germany, 2018, pp. 217-222.

[53] Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, W. C. Chu, Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control, *2018 IEEE International Conference on Services Computing (SCC)*, San Francisco, CA, USA, 2018, pp.193-200.

[54] A. B. Tran, Q. Lu, I. Weber, Lorikeet: A Model-Driven Engineering Tool for Blockchain-Based Business Process Execution and Asset Management, *16th International Conference on Business Process Management (BPM)*, Sydney, Australia, 2018, pp. 56-60.

[55] B. Notheisen, J. B. Cholewa, A. P. Shanmugam, Trading Real-World Assets on Blockchain: An Application of Trust-Free Transaction Systems in the Market for Lemons, *Business & Information Systems Engineering*, Vol. 59, No. 6, pp. 425-440, December, 2017.

[56] J. Cucurull, A. Rodríguez-Pérez, T. Finogina, J. Puiggalí, Blockchain-Based Internet Voting: Systems' Compliance with International Standards, *International Conference on Business Information Systems (BIS)*, Berlin, Germany, 2018, pp. 300-312.

[57] J. Alves, A. Pinto, On the Use of the Blockchain Technology in Electronic Voting Systems, *International Symposium on Ambient Intelligence (ISAmI)*, Toledo, Spain, 2018, pp. 323-330.

[58] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, S. Huang, A Privacy-Preserving Voting Protocol on Blockchain, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, 2018, pp. 401-408.

[59] Y. Liu, Q. Wang, An E-voting Protocol Based on Blockchain, *IACR Cryptology ePrint Archive*, Vol. 2017, pp. 1043, 2017.

[60] B. Yu, J. Liu, A. Sakzad, S. Nepal, R. Steinfeld, P. Rimba, M. H. Au, Platform-Independent Secure Blockchain-Based Voting System, *International Conference on Information Security (ISC)*, Guildford, UK, 2018, pp. 369-386.

[61] X. Yang, X. Yi, S. Nepal, F. Han, Decentralized Voting: A Self-tallying Voting System Using a Smart Contract on the Ethereum Blockchain, *International Conference on Web Information Systems Engineering (WISE)*, Dubai, United Arab Emirates, 2018, pp. 18-35.

[62] S. Panja, B. K. Roy, A Secure End-to-end Verifiable e-Voting System Using Zero Knowledge Based Blockchain, *IACR Cryptology ePrint Archive*, Vol. 2018, pp. 466, August, 2018.

[63] S. F. Shahandashti, F. Hao, DRE-ip: A Verifiable e-Voting Scheme without Tallying Authorities, *21st European Symposium on Research in Computer Security (ESORICS)*, Heraklion, Greece, 2016, pp. 223-240.

[64] F. Fusco, M. I. Lunesu, F. E. Pani, A. Pinna, Crypto-voting, A Blockchain Based e-Voting System, *10th International Conference on Knowledge Management and Information Sharing (KMIS)*, Seville, Spain, 2018, pp. 221-225.

[65] F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, G. Hjálmtýsson, Blockchain-Based E-Voting System, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, 2018, pp. 983-986.

[66] M. Pawlak, J. Guziur, A. Poniszewska-Maranda, Towards the Blockchain Technology for System Voting Process, *International Symposium on Cyberspace Safety and Security (CSS)*, Amalfi, Italy, 2018, pp. 209-223.

[67] M. Pawlak, J. Guziur, A. Poniszewska-Maranda, Voting Process with Blockchain Technology: Auditable Blockchain Voting System, *International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, Bratislava, Slovakia, 2018, pp. 233-244.

[68] K. Gu, W. Jia, C. Li, R. Chen, Identity-based Group Proxy Signature Scheme in the Standard Model, *Journal of Computer Research and Development*, Vol. 50, No. 7, pp. 1370-1386, July, 2013.

[69] M. Pawlak, A. Poniszewska-Maranda, J. Guziur, Intelligent Agents in a Blockchain-Based Electronic Voting System, *International Conference on Intelligent Data Engineering and Automated Learning (IDEAL)*, Madrid, Spain, 2018, pp. 586-593.

[70] C. Wu, Y. Chen, F. Li, Decision Model of Knowledge Transfer in Big Data Environment, *The China Communications*, Vol. 13, No. 7, pp. 100-107, July, 2016.

[71] C. Wu, E. Zapevalova, F. Li, D. Zeng, Knowledge Structure and Its Impact on Knowledge Transfer in the Big Data Environment, *Journal of Internet Technology*, Vol. 19, No. 2, pp. 581-590, March, 2018.

[72] W. Zeng, P. Chen, H. Chen, S. He, PAPG: Private Aggregation Scheme Based on Privacy-preserving Gene in Wireless Sensor Networks, *KSII Transactions on Internet and Information Systems*, Vol. 10, No. 9, pp. 4442-4466, September, 2016.

[73] J. Zhang, C. Wu, D. Yang, Y. Chen, X. Meng, L. Xu, M. Guo, HSCS: A Hybrid Shared Cache Scheduling Scheme for Multiprogrammed Workloads, *Frontiers of Computer Science*, Vol. 12, No. 6, pp. 1090-1140, December, 2018.

[74] N. C. Luong, Z. Xiong, P. Wang, D. Niyato, Optimal Auction for Edge Computing Resource Management in Mobile Blockchain Networks: A Deep Learning Approach, *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018, pp. 1-6.

[75] Y. Jiao, P. Wang, D. Niyato, Z. Xiong, Social Welfare Maximization Auction in Edge Computing Resource Allocation for Mobile Blockchain, *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018, pp. 1-6.

[76] Y. Jiao, P. Wang, D. Niyato, K. Suankaewmanee, Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 30, No. 9, pp. 1975-1989, September, 2019.

[77] S. H. Galal, A. M. Youssef, Verifiable Sealed-Bid Auction on the Ethereum Blockchain, *International Conference on Financial Cryptography and Data Security (FC)*, Nieuwpoort, Curaçao, 2018, pp. 265-278.

[78] E. Blass, F. Kerschbaum, Strain: A Secure Auction for Blockchains, *European Symposium on Research in Computer Security (ESORICS)*, Barcelona, Spain, 2018, pp. 87-110.

[79] Q. Xia, E. B. Sifah, K. Huang, R. Chen, X. Du, J. Gao, Secure Payment Routing Protocol for Economic Systems Based on Blockchain, *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, 2018, pp. 177-181.

[80] K. Karlsson, W. Jiang, S. B. Wicker, D. Adams, E. Ma, R. Renesse, H. Weatherspoon, Vegvisir: A Partition-Tolerant Blockchain for the Internet-of-Things, *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, 2018, pp. 1150-1158.

[81] Y. Chen, M. Zhou, Z. Zheng, M. Huo, Toward Practical Crowdsourcing-Based Road Anomaly Detection With Scale-Invariant Feature, *IEEE Access*, Vol. 7, pp. 67666-67678, May, 2019.

[82] L. Feng, H. Zhang, L. Lou, Y. Chen, A Blockchain-Based Collocation Storage Architecture for Data Security Process Platform of WSN, *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Nanjing, China, 2018, pp. 75-80.

[83] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne, A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain, *IEEE Access*, Vol. 7, pp. 33159-33172, March, 2019.

[84] Z. Hao, R. Ji, Q. Li, FastPay: A Secure Fast Payment Method for Edge-IoT Platforms using Blockchain, *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, Seattle, WA, USA, 2018, pp. 410-415.

[85] X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao, W. Zhao, Inter-Bank Payment System on Enterprise Blockchain Platform, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, 2018, pp. 614-621.

[86] J. Ahn, M. Park, J. Paek, Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System, *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, 2018, pp. 1431-1436.

[87] W. Li, H. Xu, H. Li, Y. Yang, P. K. Sharma, J. Wang, S. Singh, Complexity and Algorithms for Superposed Data Uploading Problem in Networks with Smart Devices, *IEEE Internet of Things Journal*, October, 2019, DOI: 10.1109/JIOT.2019.2949352.

[88] W. Li, Z. Chen, X. Gao, W. Liu, J. Wang, MultiModel Framework for Indoor Localization under Mobile Edge Computing Environment, *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp. 4844-4853, June, 2019.

[89] W. Li, H. Liu, J. Wang, L. Xiang, Y. Yang, An Improved Linear Kernel for Complementary Maximal Strip Recovery:

Simpler and Smaller, *Theoretical Computer Science*, Vol. 786, pp. 55-66, September, 2019.

[90] L. Li, X. Jiang, R. Wang, An Offline Matching Method for Large Scale Trajectories, *Journal of Internet Technology*, Vol. 18, No. 5, pp. 1185-1191, September, 2017.

[91] G. Wang, J. Fan, Y. Lv, B. Cheng, S. Kan, The Constructive Algorithm of Vertex-disjoint Paths in the Generalized Hypercube under Restricted Connectivity, *Journal of Internet Technology*, Vol. 20, No. 6, pp. 1995-2006, November, 2019.

[92] C. Yin, L. Shi, R. Sun, J. Wang, Improved Collaborative Filtering Recommendation Algorithm Based on Differential Privacy Protection, *Journal of Supercomputing*, pp. 1-14, January, 2019.

[93] S. He, W. Zeng, K. Xie, H. Yang, M. Lai, X. Su, PPNC: Privacy Preserving Scheme for Random Linear Network Coding in Smart Grid, *KSII Transactions on Internet and Information Systems*, Vol. 11, No. 3, pp. 1510-1532, March, 2017.

[94] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, F. Wortmann, Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data, *Journal of the Association for Information Systems*, Vol. 20, No. 9, pp. 1274-1309, September, 2019, DOI: 10.17705/1jais.00567.

[95] B. Yu, J. Wright, S. Nepal, L. Zhu, J. K. Liu, R. Ranjan, IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain, *IEEE Cloud Computing*, Vol. 5, No. 4, pp. 12-23, July/August, 2018.

[96] S. He, K. Xie, K. Xie, C. Xu, J. Wang, Interference-aware Multisource Transmission in Multiradio and Multichannel Wireless Network, *IEEE Systems Journal*, Vol. 13, No. 3, pp. 2507-2518, September, 2019.

[97] S. Cha, J. Chen, C. Su, K. Yeh, A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things, *IEEE Access*, Vol. 6, pp. 24639-24649, January, 2018.

[98] S. Ding, J. Cao, C. Li, K. Fan, H. Li, A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT, *IEEE Access*, Vol. 7, pp. 38431-38441, March, 2019.

[99] Y. Chen, M. Zhou, Z. Zheng, Learning Sequence-Based Fingerprint for Magnetic Indoor Positioning System, *IEEE Access*, Vol. 7, pp. 163231-163244, November, 2019.

[100] M. Ma, G. Shi, F. Li, Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario, *IEEE Access*, Vol. 7, pp. 34045-34059, March, 2019.

[101] G. Rathee, A. Sharma, R. Kumar, R. Iqbal, A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology, *Ad Hoc Networks*, Vol. 94, 101933, November, 2019.

[102] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, J. Wang, Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks, *Mobile Information Systems*, Vol. 2018, pp. 1-10, August, 2018.

[103] J.-S. Pan, L. Kong, T.-W. Sung, P.-W. Tsai, V. Snasel, Alpha-Fraction First Strategy for Hierarchical Model in Wireless Sensor Networks, *Journal of Internet Technology*, Vol. 19, No. 6, pp. 1717-1726, November, 2018.

[104] T.-T. Nguyen, J.-S. Pan, T.-K. Dao, An Improved Flower Pollination Algorithm for Optimizing Layouts of Nodes in Wireless Sensor Network, *IEEE Access*, Vol. 7, pp. 75985-75998, June, 2019.

[105] J.-S. Pan, L. Kong, T.-W. Sung, P.-W. Tsai, V. Snášel, A Clustering Scheme for Wireless Sensor Networks Based on Genetic Algorithm and Dominating Set, *Journal of Internet Technology*, Vol. 19, No. 4, pp. 1111-1118, July, 2018.

[106] Z. Xia, J. Tan, J. Wang, R. Zhu, H. Xiao, A. K. Sangaiah, Research on Fair Trading Mechanism of Surplus Power Based on Blockchain, *Journal of Universal Computer Science*, Vol. 25, No. 10, pp. 1240-1260, October, 2019.

[107] Y. Ren, F. Zhu, J. Qi, J. Wang, A. K. Sangaiah, Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things, *Applied Sciences*, Vol. 9, No. 10, 2058, May, 2019.

[108] J. Wang, Y. Gao, X. Yin, F. Li, H. Kim, An Enhanced PEGASIS Algorithm with Mobile Sink Support for Wireless Sensor Networks, *Wireless Communications and Mobile Computing*, Vol. 2018, No. 8, pp. 1-9, December, 2018.

[109] Y. Ren, Y. Leng, Y. Cheng, J. Wang, Secure Data Storage Based on Blockchain and Coding in Edge Computing, *Mathematical Biosciences and Engineering*, Vol. 16, No. 4, pp. 1874-1892, March, 2019.

[110] G. Ramezan, C. Leung, A Blockchain-Based Contractual Routing Protocol for the Internet of Things Using Smart Contracts, *Wireless Communications and Mobile Computing*, Vol. 2018, pp. 1-14, November, 2018.

[111] S. Sankaran, S. Sanju, K. Achuthan, Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things, *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, 2018, pp. 1454-1459.

[112] B. Yin, X. Wei, Communication-Efficient Data Aggregation Tree Construction for Complex Queries in IoT Applications, *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp. 3352-3363, April, 2019.

[113] L. Zhou, L. Wang, Y. Sun, P. Lv, BeeKeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation, *IEEE Access*, Vol. 6, pp. 43472-43488, June, 2018.

[114] C. Li, L.-J Zhang, A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things, *2017 IEEE International Congress on Internet of Things (ICIOT)*, Honolulu, HI, USA, 2017, pp. 33-41.

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

[116] Y. Chen, S. Ding, Z. Xu, H. Zheng, S. Yang, Blockchain-based Medical Records Secure Storage and Medical Service Framework, *Journal of Medical Systems*, Vol. 43, No. 1, Article 5, January, 2019.

[117] 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 136, August, 2018.

[118]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 141, August, 2018.

[119]J. Wang, Y. Gao, W. Liu, A. K. Sangaiah, H. Kim, An Intelligent Data Gathering Schema with Data Fusion Supported for Mobile Sink in WSNs, *International Journal of Distributed Sensor Networks*, Vol. 15, No. 3, pp. 1-9, March, 2019.

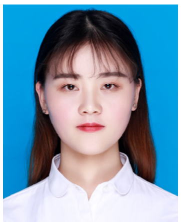
[120]Y. Ji, J. Zhang, J. Ma, C. Yang, X. Yao, BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 42, No.8, Article 147, June, 2018.

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

[122]A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: Using Blockchain for Medical Data Access and Permission Management, *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, 2016, pp. 25-30.

Biographies

Jingyu Zhang received the Ph.D. degree in Computer Science and Technology from Shanghai Jiao Tong University in 2017. He is currently an Assistant Professor at the School of Computer & Communication Engineering, Changsha University of Science and Technology, China. His research interests include blockchain, computer architecture, and mobile networks.



Siqi Zhong is currently a graduate student at the School of Computer & Communication Engineering, Changsha University of Science & Technology, Changsha, China. Her research interests include blockchain and network security.

Tian Wang received his Ph.D. degree in City University of Hong Kong in 2011. Currently, he is a professor at the College of Computer Science and Technology, Huaqiao University, China. His research interests include Internet of Things and edge computing.

Han-Chieh Chao is serving as the president of National Dong Hwa University since February 2016. He received his M.S. and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 1993 respectively. He has authored or co-authored 4 books and has published about 300 refereed professional research papers.

Jin Wang received the M.S. degree from Nanjing University of Posts and Telecommunications, China in 2005. He received Ph.D. degree from Kyung Hee University, Korea in 2010. Now, he is a professor at Changsha University of Science and Technology. His research interests mainly include wireless sensor network and network security.