Blockchain-based Systems and Applications: A Survey

Jingyu Zhang¹, Siqi Zhong¹, Tian Wang², Han-Chieh Chao³, Jin Wang¹,⁴

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](image-url)
Table 1. Block data structure

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

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 Response) 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 blockchain 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

<table>
<thead>
<tr>
<th>Node type</th>
<th>Participator</th>
<th>Write</th>
<th>Read</th>
<th>Verification</th>
<th>Analysis</th>
<th>Process supervision</th>
<th>Trade supervision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise node</td>
<td>Supplier</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Manufacturer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Seller</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Carrier</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>End user node</td>
<td>Consumer</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Visitor</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supervisor node</td>
<td>Market</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>supervision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>department</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>supervision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>department</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 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](image)

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 system 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 studied the work of [67] and presented 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 a 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 cannot be tampered with;
2. Candidates’ votes cannot be tampered with;
3. Votes are authentic, reliable and cannot 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.
Decentralized Applications in the Data Security Field

The rise of the 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 mobile environment 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] further 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.

![Blockchain features integrated with IoT](image)

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] presented 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

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


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

<table>
<thead>
<tr>
<th>Fields</th>
<th>Applications</th>
<th>Targets</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain-Based Medical Data Preservation System</td>
<td>To provide a storage scheme to manage personal medical data based on blockchain and cloud storage. (1) To provide a service framework for sharing medical records. (3) To guarantee user privacy.</td>
<td>(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.</td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td>Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme</td>
<td>(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.</td>
<td>The system builds a blockchain-based multi-level location sharing scheme by using order-preserving encryption and merkle tree.</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Blockchain System Using Smart Contracts</td>
<td>To handle the protected health information generated by medical IoT devices.</td>
<td>The system can support real-time patient monitoring and medical interventions.</td>
</tr>
</tbody>
</table>

### 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 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


S. Wang, S. Zhu, Y. Zhang, Blockchain-based Mutual


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 (DMDB), Shanghai, China, 2018, pp. 659-669.


[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.


Blockchain-based Systems and Applications: A Survey


**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, Huqiao 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.