

Received August 19, 2021, accepted September 9, 2021, date of publication September 13, 2021, date of current version September 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3112608

Application of Hyperledger in the Hospital Information Systems: A Survey

ZEQI LENG¹, ZHENJIANG TAN, AND KUNHAO WANG

College of Computer Science, Jilin Normal University, Siping 136000, China

Corresponding author: Zhenjiang Tan (tanzj@jlnu.edu.cn)

This work was supported in part by the Ministry of Education Project of China under Grant NGII20180408, and in part by Jilin Normal University Graduate Research and Innovation Project of China under Grant 201951.

ABSTRACT Hyperledger is considered to be the most mature consortium chain technology. Compared with other blockchain technologies, Hyperledger focuses on the application development of enterprise-level standards. Due to its unique permission management, fine-grained access control, pluggable consensus algorithm and higher transaction performance, Hyperledger has been increasingly used in the hospital information systems. Although there are more and more applications of Hyperledger in the field of health care, there is currently no research to comprehensively classify and compare them. This article obtained the latest 222 articles related to Hyperledger from the Web of science, Wordlib, and EBSCO databases. And this article used manual method to filter out the literates needed for this review. This article had comprehensively analyzed and compared the above literature, then summarized four research directions related to hospital information systems, including medical drug traceability, medical records, medical images and other medical fields (financial benefits, medical insurance, medical system performance and dynamic processing). Through in-depth analysis of all solutions, this article reconstructed the architecture diagrams of each solution that focus on Hyperledger, and showed the most intuitive comparison results. In addition, we summarized each solution, and analyzed their implementation form four aspects, including traceability, monitoring, security and privacy. Finally, the future opportunities and prospects were discussed. Four potential medical research directions of Hyperledger in DNA research, pathological image sharing, protein folding calculation and machine learning had been identified. Finally, this article discussed the opportunities and prospects for the future of hospital information systems, and summarized the applications of Hyperledger in four potential directions, including DNA research, pathological image sharing, protein folding calculation and machine learning.

INDEX TERMS Hyperledger, blockchain, healthcare application, hospital information system, distributed information management.

I. INTRODUCTION

The Hospital Information System (HIS) is the necessary technical support for the operation of modern hospitals. It is mainly responsible for standardized hospital management, improving the efficiency of medical work and the quality of medical services. However, as HIS has spread to medical institutions around the world, HIS has presented many technical and management challenges.

Challenges in technology: cost, safe storage and privacy protection. For example, due to the high cost of information systems [1], most organizations still use paper materials or

other incomplete information systems to manipulate medical information. Medical data is usually stored in a centralized database, and the patient's identity and detailed medical records are completely controlled by a third-party organization. This will cause individuals or institutions to tamper with and leak case materials driven by interests. In addition, most of the medical information has not been systematically and professionally anonymized, and the privacy of patients will be exposed to their vision when a third party calls this information.

Challenges in management: efficiency and sharing. For example, most of the current medical systems adopt a centralized method of processing medical data. However, with the exponential growth of medical data, this processing method

The associate editor coordinating the review of this manuscript and approving it for publication was Fabrizio Marozzo².

will lead to lower work efficiency. Patients may need to go to different medical institutions for consultation, especially when the patient moves to another region, city or country [2]. The lack of interoperability causes the patient to be re-examined in the hospital. If it involves radiological examinations, the patient will again bear the risk of radiation and unnecessary expenses.

Recent studies have shown that blockchain technology provides new ideas for the reform of HIS. Although blockchain is widely adopted by the research community, all peers in the network are treated equally and no reasonable access mechanism is provided [3]. Medical records are sensitive data, which makes users unwilling to share private information on a publicly anonymous blockchain network. In addition, most of the current blockchain systems lack the ability to meet the strict requirements of the operation and business environment. For example, scalability, complexity, and cryptocurrency market volatility have prevented general blockchain solutions from being widely accepted [4].

Therefore, the blockchain technology with permissions has attracted the attention of many researchers. Hyperledger is currently the most mature consortium chain technology. It was established in 2015, led by the Linux Foundation and co-founded by more than 30 companies. Hyperledger is one of the fastest growing open source collaboration results, which aims to promote the development of cross-industry blockchain technology [5]. Since Hyperledger focuses on the application development of enterprise-level standards, Hyperledger has many unique designs in addition to the characteristics common to other blockchain technologies. For example, Hyperledger supports the management of fine-grained permissions, so it realizes the function of conducting a variety of secure transactions in a distributed network. Each consortium chain in the Hyperledger network is only open to some members, so it has higher throughput and lower latency. Hyperledger does not need to use consensus protocols and cryptocurrencies as a reward mechanism, so it has higher performance. The chaincode in Hyperledger (equivalent to the smart contract in Ethereum) can be implemented by Go language [6], which means that developers can implement any logic implemented by Go language on top of Hyperledger [7], so Hyperledger can be widely accepted. In addition, a variety of pluggable components and a highly modular structure make Hyperledger more flexible, so it can be extended to any industry. In conclusion, the unique advantages of Hyperledger can promote the reform of HIS and solve the current challenges faced by HIS to a certain extent. Figure 1 shows the architecture of a Hyperledger-based medical information sharing system.

The main contribution of this article is:

- (1) In terms of research content: The main purpose of this article is to study the latest application of Hyperledger in the healthcare system, and demonstrate the effectiveness and feasibility of the integration of Hyperledger technology with the medical industry. This article

extracts the articles in the medical field of Hyperledger, and summarizes four main research directions, including medical traceability, medical records, pathological images and other medical fields (research on hospital revenue, medical insurance, medical system performance and dynamic processing)

- (2) In terms of comparison methods: As most of the solution architecture diagrams are constructed at a macro level, many research details cannot be reflected in these diagrams. Therefore, this article proposes a new comparison method to achieve a more intuitive comparison. Based on the Hyperledger project tested and used in the article, and the original architecture diagram of the article, this article has implemented an upgrade to each architecture diagram, which more intuitively reflects the characteristics of each program. Through in-depth analysis of the structure and design details of each solution, this paper reconstructs the architecture diagram of each solution and gives the most intuitive comparison. This new comparison method is the first attempt in the field of Hyperledger review.

The overall arrangement of this article is as follows: In the second section, this article introduces the overall architecture and key enabling technologies of Hyperledger in detail, and comprehensively analyzes the engine of Hyperledger in the medical field. In Section 3, this article comprehensively reviews the implementation of the solutions in the four research directions. In the comparison part of this article, the reconstruct architecture diagram of the article in each direction was draw and describe one by one in the main part of the article. In addition, after the text description of each research direction, this article summarizes each solution again and compares the implementation of these solutions in four features, including traceability, monitoring, security and privacy. In Section 4, this article summarize four potential research areas with high research value, including DNA data research, protein folding calculation, pathological image sharing, and machine learning-assisted therapy.

II. HYPERLEDGER OVERVIEW

A. HYPERLEDGER ARCHITECTURE

Hyperledger system is a highly modular umbrella structure. It has 9 components [8], including consensus layer, contract layer, communication layer, data storage module, encryption module, identity service module, policy service module, APIs and interoperability module. The consensus layer encapsulates a variety of consensus algorithms and consensus mechanisms, and is mainly responsible for confirming whether the transaction set that creates the block is correct. The contract layer is responsible for responding to requests sent by the application and executing business logic. The communication layer is responsible for the transmission of information of each peer to realize the sharing of accounts. The data storage module is responsible for the storage of pluggable databases. For example, in a consortium chain, each module is allowed

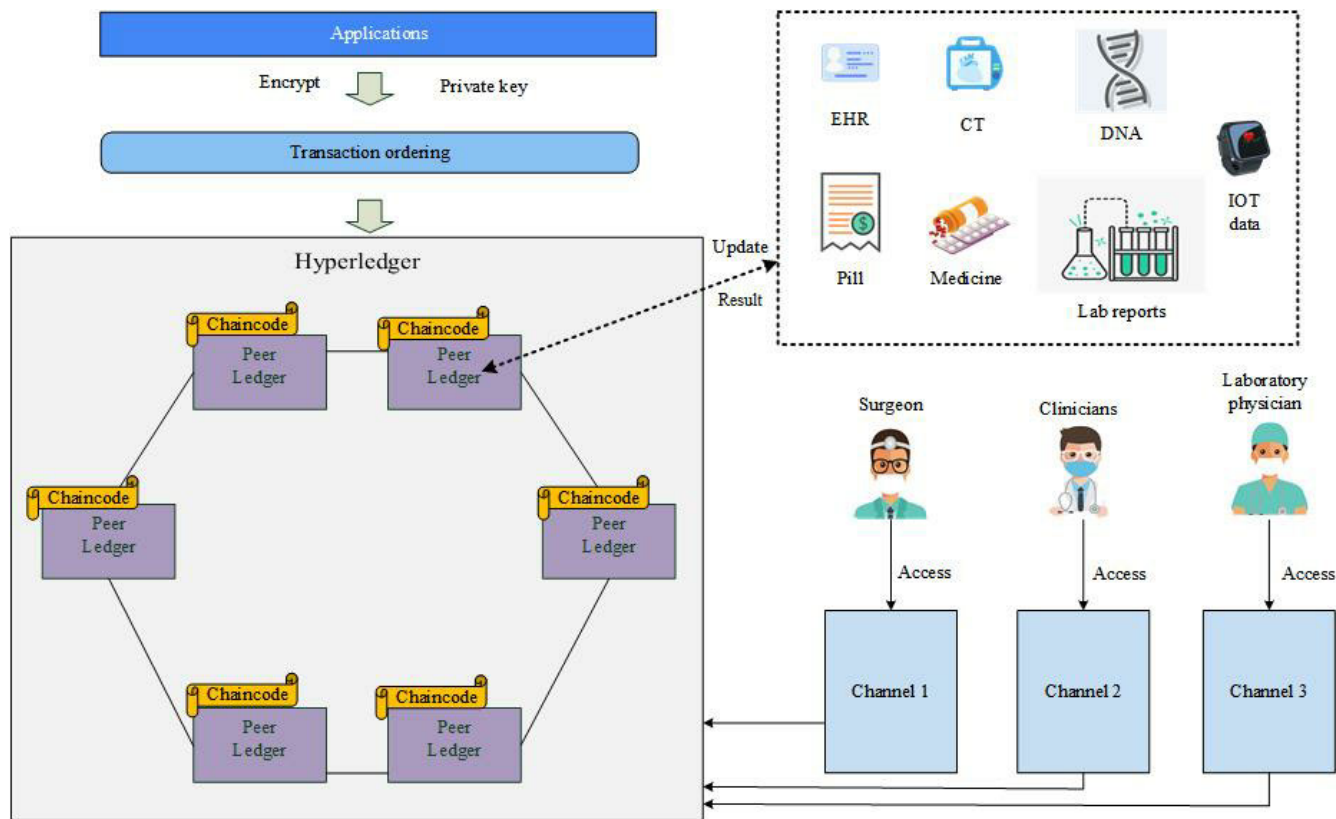


FIGURE 1. Hyperledger-based medical information sharing platform (The system encrypts the data and uploads it to the hyperledger system after sorting services. After processing multiple transactions, the system will add new blocks. Then the system will update EHR, etc. Database. surgeon, Clinician and laboratory physician share medical information with different channels through set permissions).

to use different databases and does not affect the work of other modules. The encryption module is also a pluggable component, and the module allows the exchange of multiple encryption algorithms such as proxy re-encryption, homomorphic encryption, and quantum encryption. The identity service module needs to meet high commercial standards, so only authorized members can join the distributed network for data sharing. The identity service of Hyperledger provides the management of membership, including adding, revoking, and auditing. The strategy service module is mainly responsible for managing the strategies to be implemented such as consensus policies or group policies. APIs enable clients and applications to connect to the Hyperledger system. The interoperability module is mainly responsible for information sharing, including between groups, institutions and research centers.

Hyperledger also provides 6 development collaboration tools, including ACCOUNT, ROCKETCHAT, GITHUB, WIKI, BUG REPORTING and MAILING LISTS. ACCOUNT is a free and unique community ID that helps individuals applies. ROCKETCHAT provides an online communication platform that supports multiple functions. GITHUB stores all the official codes in the Hyperledger, which helps beginners to easily obtain development codes. WIKI enables researchers to obtain real-time information

from the Hyperledger community. BUG REPORTING is a centralized place for all the latest BUG solutions. MAILING LISTS provides special communication channels for each project to ask questions about development. These development collaboration tools help developers develop systems efficiently. Since Hyperledger is a joint project, its main technology is provided by top projects that contribute to the platform. This article will introduce key project technologies in the next section.

B. KEY ENABLING TECHNOLOGY

Hyperledger currently has 18 top projects. These projects involve multiple businesses, including cross-domain identity authentication, EVM, mobile applications, professional blockchain system performance evaluation, etc. They provide the technology that Hyperledger implements in the Internet of Things, e-government, medical and artificial intelligence and other fields, and make Hyperledger suitable for any commercial application. The development of each project goes through five stages: proposal, incubation, active, promoted release and end of life. Therefore, if the research team wants to submit the created project to the official website of Hyperledger, the sponsor will first prepare the proposal materials (such as the project purpose and scope, etc.), and then the global technical committee will review and vote. After the

vote is passed, the project will be incubated, and when the project is mature, you can apply to enter the active state. If the project is no longer active and enters the maintenance phase, the life cycle is finally terminated. The applied project may execute the above stages in order, or it may go through multiple iterations. In addition, if a project is in the deprecated stage, the project will be deprecated after six months of maintenance by the community (such as Composter, which has been deprecated). This article will introduce in detail the five top-level projects that are currently active with many users.

1) FABRIC

Hyperledger Fabric is the first project submitted to the Hyperledger platform and is currently the most widely used technology. This project provides Hyperledger with consortium chain technology that focuses on fine-grained authority management.

Fabric has many unique designs that are different from other blockchains, including pluggable consensus, multi-channel, state-based endorsement strategy, and fine-grained access control. Fabric does not rely on the native cryptocurrency [9], so it has higher performance. For example, in the case of 32 v-CPU peers, its throughput can reach 3870tps, and the delay is less than 1.5s [10]. In addition, all Hyperledger programs run in docker containers. The container provides a sandbox environment that separates the application from the physical resources, and isolates the containers from each other to ensure the security of the application [11].

The Fabric network has four nodes with different roles: Endorser Peer, Committer Peer, Orderer, and CA. Endorser Peer is responsible for checking all transaction proposals, executing smart contracts, calculating the results of transactions and endorsing them. Orderer is responsible for receiving all transactions and sorting them. Committer Peer is responsible for checking the legitimacy of the transaction results after sorting and updating the local ledger in real time. The CA is responsible for issuing and revoking certificates for all nodes. Figure 2 shows the transaction processing flow of Fabric 2.0 version.

2) SAWTOOTH

Compared with other projects, Hyperledger Sawtooth provides a more flexible and energy-efficient technology for Hyperledger. Each complete node consists of four parts, including Validator, Transaction Processor, REST API and Client. Validator is the core component of each node and the fixed structure of each node. The Validator is responsible for receiving transaction requests and keeping the global state consistent with other Validators. Except for Validator, other components are pluggable, and each Validator can dynamically join the network. The Transaction Processor is responsible for processing the transaction and returning the result. The client generates the request according to the data structure specified by Transaction and Batch. REST API is a standardized network transmis-

sion data format. In addition, Sawtooth provides a POET consensus algorithm. The validator with the shortest waiting time of a specific transaction block is selected as the leader, so this consensus algorithm ensures the randomness and security of selecting the leader node (Official homepage: <https://wiki.hyperledger.org/display/sawtooth>). This makes the participant's cost low and can provide the possibility for a large number of Internet of Things users to use.

3) IROHA

Hyperledger Iroha provides functions for the development of Hyperledger on the mobile and web terminals. Iroha focuses on the needs of mobile terminals and web pages, and is a framework for a distributed ledger platform (Official homepage: <https://wiki.hyperledger.org/display/iroha>). The project supports the YAC (Yet another Consensus) consensus algorithm with high fault tolerance.

4) INDY

Hyperledger Indy provides cross-domain authentication for Hyperledger (Official homepage: <https://wiki.hyperledger.org/display/indy>). The project focuses on global digital identity management, which can solve the problems caused by isolated management. Indy realizes the interoperability between different regions, different cities or different countries for Hyperledger.

5) BESU

Hyperledger Besu provides a client that supports enterprise-level Ethereum. Besu aims to enable Hyperledger to integrate with Ethereum faster through a clean interface and modular structure (Official homepage: <https://wiki.hyperledger.org/display/besu>).

Besu has 8 modules, including EVM, consensus algorithms (POA, IBFT2.0, Clique, and POW), RocksDB key-value database, P2P network, user-oriented APIs, monitoring (allows monitoring of nodes and performance), privacy and permissions. Besu enables users to operate, maintain and monitor the Ethereum network in Hyperledger.

This article collected the development data of each top project from the beginning to 2020 (data sourced from <https://www.hyperledger.org>). And this article compared their active level through five indicators, including the year of submission, the number of contributions, the proportion of development languages, the number of codes added and the number of codes deleted. In Table 1, Fabric is still the most mature project at present, Besu is a project that has developed rapidly in recent years, and its users have surpassed Sawtooth.

This article systematically summarizes the advantages of Hyperledger in order to implement a new generation of information systems:

- (1) High efficiency: Hyperledger has more peer-to-peer types. Different nodes are assigned different functions to coordinate transaction processing, which improves the efficiency of transaction processing.

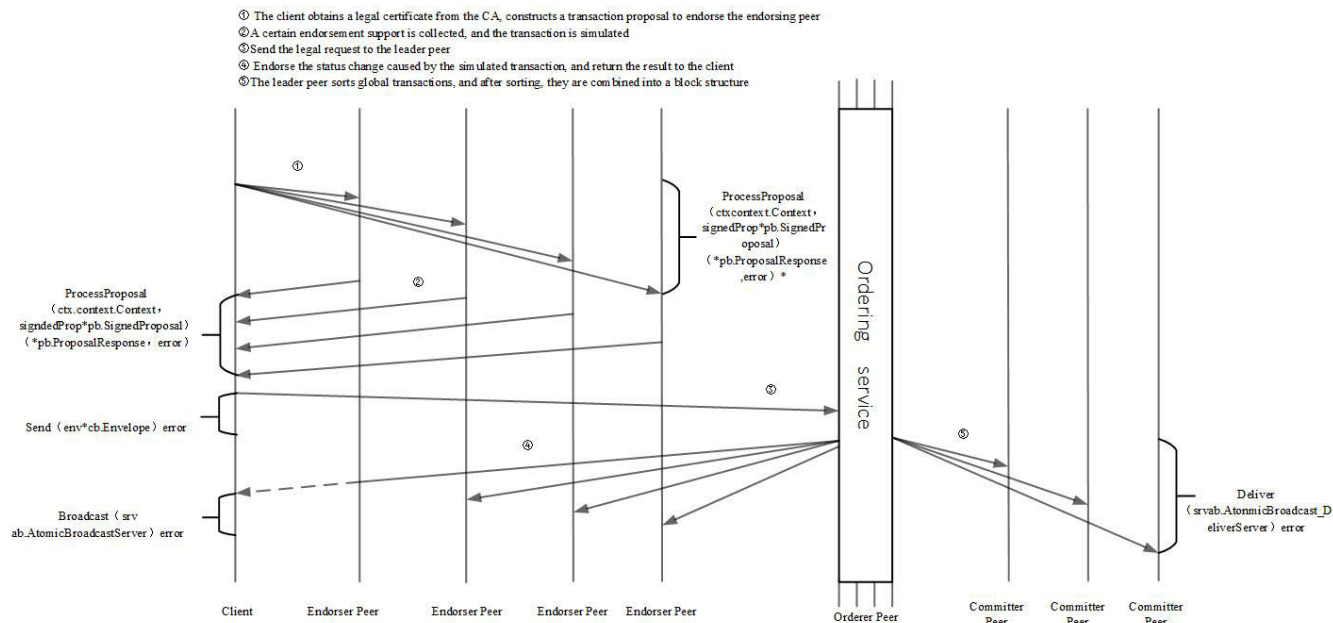


FIGURE 2. The transaction process of Fabric2.0 (the interfaces or methods that need to be passed to execute each step are shown in parentheses).

TABLE 1. Comparison of FABRIC, SAWTOOTH, IROHA, INDY, BESU(The data calculated the active data of each project from the beginning to 2020).

Top items of Hyperledger	Submitted year	Contributions	Percentage of code language	Code additions (KB)	Code deletions (KB)
FABRIC	2015	76 people submitted 4660 times.	Go 99.4%,Other 0.6%.	2037.3242	1507.2295
SAWTOOTH	2016	48 people submitted 1134 times.	Python72.3%,Rust23.8%,Other 3.9%.	85.0771	169.4922
IROHA	2016	30 people submitted 804 times.	C++93.4%,CMake 2.7%,Other 3.9%.	204.3184	62.4365
INDY	2017	49 people submitted 2318 times.	Python93.4%,Shell5.2%,Other 1.4%.	187.7695	150.9736
BESU	2019	86 people submitted 2461 times.	Java99.4%,Other0.6 %.	994.3760	653.0332

- (2) High autonomy: Patients can decide what to share and who they want to share by setting the function of the chaincode.
- (3) Humanized access control: Hyperledger allows data providers to create multiple channels according to their own needs, and medical record books of different channels are isolated from each other.
- (4) Powerful flexibility: failure of any node on the Hyperledger does not affect the operation of the overall system.
- (5) Strong privacy protection and safe storage: The data in the Hyperledger cannot be tampered with or forged.
- (6) Each user’s information will be encrypted by an encryption algorithm, which is difficult to crack.
- (7) Auditability: Every user has the authority to review the operation records on the chain.
- (8) Tracking operations: Once the data in the Hyperledger is shared, the Hyperledger can track the ins and outs of these data (including operation records) to prevent denial.

Therefore, Hyperledger provides reliable technical support for large-scale data sharing. These various unique features make Hyperledger help to encourage individuals and groups to actively share data. Below, this article elaborates on the engine of Hyperledger in the new generation of HIS.

C. APPLICATION MOTIVATION OF HYPERLEDGER IN THE NEW GENERATION OF HIS

HIS manages various types of medical information, including electronic health records, medical images, surgical records, laboratory reports, medical allergy history, etc. These data are the patient's medical history, personal data, experimental results, surgical medical records, etc. Once the information is leaked or falsified, it may endanger the life of the patient. Researchers will encounter many challenges when implementing HIS. For example, it is difficult for a large number of private clinics to provide funding for the medical information system. Individual medical practitioners rarely receive IT training. When there are technical problems with nursing data (such as accidental deletion of files by medical staff), these data will not be restored in time [12]. At present, most HIS are centralized platforms. Despite the maturity of technology development, they do not trust each other, which make it impossible for enterprises to conduct transactions with confidence [13]. In a small number of blockchain-based HIS that has been implemented, providers of medical information do not have proper control rights. Patients cannot know who accessed their medical data, when they were accessed, and what purpose they were used for.

Based on current research, this article summarizes the necessary conditions for implementing a new generation of HIS:

- (1) Integrity of medical information.
- (2) Data privacy protection and safe sharing.
- (3) The data provider has control over the data.
- (4) Real-time traceability of data operations.
- (5) Regularly review medical information to facilitate accountability.
- (6) Interoperability between different medical institutions.

As mentioned earlier, the unique advantages of Hyperledger can solve the challenges of the existing medical system and have the necessary conditions for a new generation of HIS. Hyperledger provides an unprecedented direction for HIS research and is of great significance. In the third section, this article reviews the latest research progress of Hyperledger in the medical field.

III. VARIOUS MEDICAL SYSTEMS BASED ON HYPERLEDGER

A. APPLICATION IN THE FIELD OF MEDICINES TRACEABILITY

Fake medicines are a key issue leading to unsafe quality of medicines. According to a survey of fake medicines in low- and middle-income countries, 42% of the 1,500 fake medicines reported to the agency in the past four years

were from Africa, 21% from the Americas and 21% from Europe [14]. In a survey in Southeast Asia, volunteers purchased 104 random samples in Cambodia, Laos, Myanmar, Thailand and Vietnam, and 38% were found to be fakes without active ingredients [15]. With the increase in the scale of medicines sales, the sales of fake medicines have not declined but increased.

One of the main reasons for this phenomenon is the globalization of medicines production and distribution. Medicine companies are setting up manufacturing and research facilities in remote areas around the world, which has brought unprecedented new regulations and enforcement challenges [16]. The second main reason is the contradiction between the production cost of fake medicines and the cost of identification. The cost of experimental analysis of medicines in low-income countries is high. However, the cost of fake medicines is very low. As far as biological reagents are concerned, fake medicines can range from simple saline to any diluted version of the medicine [17]. In addition, consumers cannot obtain all distribution information from medicine manufacturing to sales. Therefore, the complete record and security sharing (medicine traceability) of the entire medicine supply chain can solve the problem of medicine quality and safety to the greatest extent. As shown in Figure 3, this article focused on Hyperledger and upgraded the architecture diagram of each solution.

As shown in Figure 3(a), Sinclair *et al.* [18] implemented the four functions in the Composer trade template, including participants (manufacturers and retailers), transactions, access control, and assets. This system verifies the feasibility of Hyperledger to implement medicine traceability. As shown in Figure 3(b), Raj [19] proposed a medicine traceability model. When the circulation information of the medicine circulation reaches each node (the EPC code needs to be marked before the medicine transmission), the ownership of the medicine is transferred at the same time. After the consumer receives the medicine and confirms the bill, the quality information of the medicine will be updated to each node. As shown in Figure 3(c), Guggenberger [20] tested the sharing of medicine traceability information among three organizations (ORG1-ORG3). After each shared transaction flow is sorted by the Orderer, it is endorsed in the Hyperledger. The invoice data of each transaction is stored separately in the PDC.

As shown in Figure 3(d), Sylim [21] developed a medicine traceability system. Retailer, wholesaler, and manufacturer are respectively authorized by the FDA in the Hyperledger, and users can query the information circulating in the medicine traceability documents through WEB or APP. As shown in Figure 3(e), Jamil [22] combined smart hospitals and Hyperledgers to develop a medicine traceability ecosystem. The system builds three Hyperledger networks for the medical department, neurosurgery and cardiology. Users such as doctors connect to the smart hospital system to verify their identity with the Hyperledger network, query medicine information, and trade medicines. As shown in Figure 3(f),

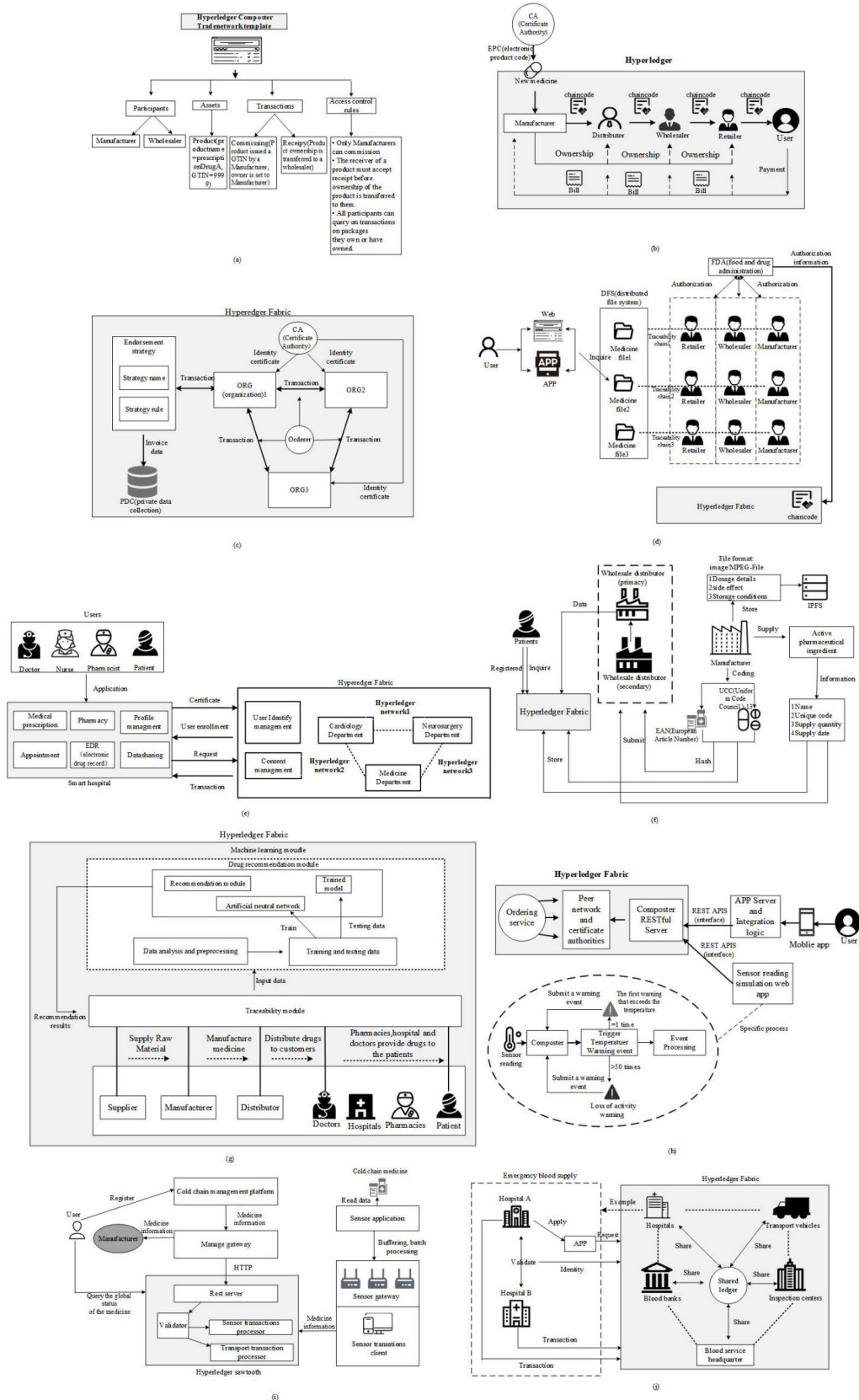


FIGURE 3. 3(a) DSCSA, 3(b) Proof of ownership/identify-based system, 3(c) Healthtec, 3(d) DFS, 3(e) Faisal Jamil et al., 3(f) Medledger, 3(g) DSCMR, 3(h) Fabiana Fournier et al., 3(i) Pharmaceutical blood cold chain system, 3(j) Seungeun Kim et al.

Uddin [23] proposed a method of separately tracing medicine information. The manufacturer in this model stores the storage conditions and other details of the medicine on the IPFS, and the hash value of the manufacturing record (by marking the EAN code or UCC-13 code) and the information such as the active ingredient of the medicine are separately uploaded to the Hyperledger. The system sends this information to the primary wholesale distributor and the secondary wholesale distributor, both of which store the complete medicine information in the Hyperledger. After the patient has registered in the Hyperledger, he can query the retrospective medicine information.

How to quickly select the best therapeutic medicine among the same medicines from multiple trusted manufacturers? As shown in Figure 3(g), Abbas [24] developed an intelligent medicine supply chain system combining Hyperledger and machine learning. In the traceability module, the system records the entire circulation information from the provider to the patient. The traceability module uploads medicine information and patient feedback data to the machine learning module. The training model in machine learning can learn and update in real time from the comments and ratings provided, and update the recommendation results accordingly.

Some research focuses on the traceability of cold chain medicines. Cold chain medicines generally have temperature restrictions. For example, the tuberculosis vaccine in Kenya must be refrigerated and can only be transported at a temperature of 2 degrees Celsius to 8 degrees Celsius [11]. The key to the traceability of cold chain medicines is to ensure that cold chain medicines are transported within the validity period. As shown in Figure 3(h), Fournier [25] proposed a solution based on Composter and Fabric. The temperature of the medicine is collected by the sensor on the container and uploaded to the Hyperledger through REST APIS. The user also connects to the REST APIS through the mobile phone APP to query the quality of medicines. The system reads the temperature of the medicine once a minute. When the temperature of the medicine exceeds the normal threshold, the system will submit a warning event to the Hyperledger (the gray exclamation mark in the figure). When the system receives 50 warnings, the system determines that the medicine is inactive (the black exclamation mark in the picture), and the user can terminate the transaction. As shown in Figure 3(i), Hulea [26] developed a system based on the Hyperledger Sawtooth framework. The information detected by the medicine sensor is batch processed and buffered through the sensor gateway and the client, and the medicine information is uploaded to Sawtooth. The sensor transaction processor and the transmission transaction processor are responsible for storing the real-time quality of the medicine and updating the global state of the medicine. The user registers the identity from the cold chain management platform, and the medicine information through the management gateway will be sent to the manufacturer in the form of a transaction. Users can check the status of cold chain medicines through Hyperledger. As shown in Figure 3(j), Kim [27] developed

a cold chain traceability platform for emergency blood. The platform establishes blood transactions between five types of entities (the dotted lines indicate the flow of transactions between each entity), including blood banks, hospitals, transport vehicles, inspection centers, and blood service headquarters. Take the hospital as an example. Hospital A makes a request to the Hyperledger through the APP. After the system verifies the identity of the hospital, the neighboring hospital (Hospital B) conducts blood transactions with Hospital A. Hyperledger will create new blocks and update the ledger. Each entity in the Hyperledger shares the ledger and provides timely blood resource information.

As shown in Table 2, this article summarized the above solutions, and sorted out the implementation of each solution in terms of traceability, monitoring, security and privacy.

B. APPLICATION IN THE FIELD OF MEDICAL RECORDS

Electronic medical records are specifically divided into three types of data: EMR (Electronic Medical Records), EHR (Electronic Health Records) and PHR (Personal Health Records). EMR is a health record owned by a specific organization, such as an individual doctor. It comes from the information compiled by a doctor during the diagnosis and treatment of patients, and belongs to internal data. Therefore, the advantage of EMR is that it helps to identify patients who need to be screened or followed up, but the record is not open to patients. EHR is similar to EMR, but has a wider range of sources. It is not only an office data but also a collection of health records of all clinicians involved in treatment. Therefore, the advantage of EHR is that it can be shared with multiple medical organizations, and the same organization can continuously monitor the health of patients. This record is completely paperless, and patients can check their health records (information comes from <https://www.continuouscare.io/blog/difference-between-emr-ehr-phr>). PHR is established by a medical service provider or patient, and includes information such as drug history, hospitalization records, health status, family medical history, and allergy history. PHR is mainly derived from clinical information, laboratory reports, and wearable medical device monitoring data from doctors. Therefore, the advantage of PHR is that patients actively participate in the management of data and decide on their own sharing permissions.

Medical records contain a large amount of detailed clinical information and provide some unique advantages for clinical research, including cost efficiency, big data scalability, and the ability to analyze data over time [28]. Its wide application provides clinicians and researchers with unprecedented opportunities for health informatics, disease risk prediction, actionable clinical advice and precision medicine [29]. This article focuses on how Hyperledger solves the shortcomings of the existing medical record management system, and reviews the latest research from two perspectives of EHR and PHR.

TABLE 2. Analyze the medicine traceability solutions based on hyperledger.

Name(author) of medicines traceability solutions	System test platform	Summary	Traceability	Monitoring	Security	Privacy
DSCSA	Hyperledger Composer	By designing participants, assets, queries, and access control rules, the feasibility of users querying drug tracking information is determined. However, only the original functionality of the composer template is implemented.	✓	✓	✓	
Proof of ownership/identity-based system	Hyperledger Fabric	The authenticity of drugs is improved through the transfer of ownership agreements designed by smart contracts. But there are risks to a highly centralized EPC.	✓	✓	✓	✓
Healthtec	Hyperledger Fabric	By improving drug replenishment and improving the efficiency of supply chain, distributed drug information tracking is achieved. However, the system is limited to three organizations, and use cases apply only to companies.	✓	✓	✓	✓
DFS	Hyperledger Fabric Hyperledger Composer Hyperledger Caliper	Recursive validation increases the accuracy of the data. But only officially known drug can be monitored and tracked.	✓	✓	✓	✓
Faisal Jamil et al.	Hyperledger Fabric Hyperledger Composer	Improved access security for drug records and EHR through a time-limited smart contract.	✓	✓	✓	✓
Medledger	Hyperledger Fabric	By storing real data separately from the data index, the possibility of third-party intervention in the chain of intervention is reduced.	✓	✓	✓	
DSCMR	Hyperledger Fabric	The adoption of smart drug recommendations through machine learning increases the credibility of medicines.	✓	✓	✓	✓
Fabiana Fournier et al.	Hyperledger Composer Hyperledger Fabric	Through a temporal logic smart contract, the monitoring of cold chain drugs is strengthened.	✓	✓	✓	
Pharmaceutical Blood Cold chain system	Hyperledger Sawtooth	By extending the custom transaction series and sensor gateways, the flexibility of cold-chain drug traceability systems is enhanced and transaction batch processing is more efficient.	✓	✓	✓	✓
Seungeun Kim et al	Hyperledger Composer	Through an emergency blood supply scheme, the blood supply time in first aid is shortened and the remaining blood stock is used effectively.	✓	✓	✓	

1) EHR AND EMR SYSTEMS BASED ON HYPERLEDGER

As shown in Figure 4, this article showed the solution of EHR and EMR.

As shown in Figure 4(a), Dubovitskaya [30] proposed a system for storing EHR separately. Users and nodes in the Hyperledger register and obtain identity certificates and keys

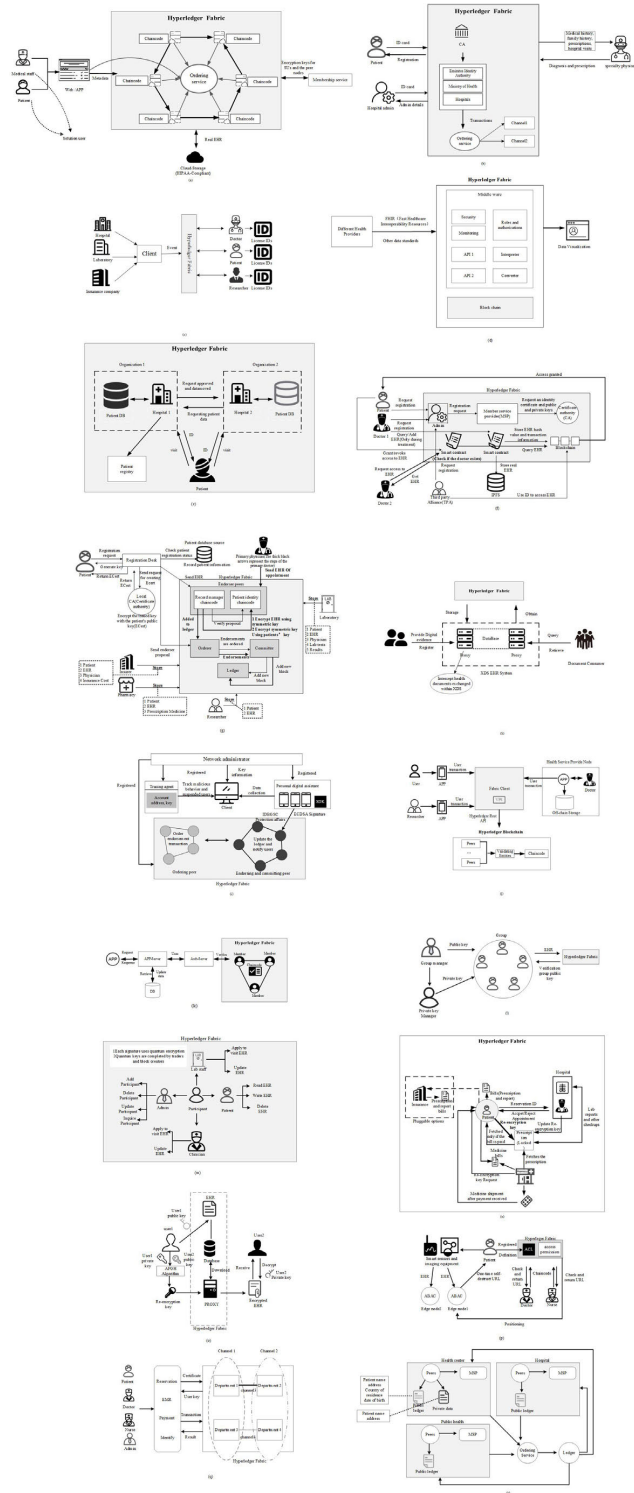


FIGURE 4. 4(a) Action-EHR, 4(b) Mblocks, 4(c) Tagrid Alshalali et al., 4(d) B4HEALTH, 4(e) Naveen Kumar S et al., 4(f) Jasleen Kaur et al., 4(g) Mueen Uddin et al., 4(h) eHealth systems, 4(i) Dara Tith et al., 4(j) MedHypchain, 4(k) ClinicAPPChain, 4(l) Tomas Mikula et al., 4(m) Healthcare record-keeping, 4(n) Blockchain and quantum blind signature hybrid scheme, 4(o) PREHEALTH, 4(p) Proxy re-encryption in permissioned blockchain, 4(q) Hybrid architecture of blockchain and edge node, 4(r) Medical blockchain for EMR Integrity.

through the CA. When a patient wants to view his EHR, the patient visits the hospital through the user interface. And

share the EHR directly through the web application, and set the access permissions (the specific permission information is in the dotted box). The generated chain code is stored in CS. When a patient wants to store their own EHR, the patient stores the metadata in the Hyperledger through mobile or APP, and stores the real data in the cloud through AWS (the storage in the cloud must be stored in accordance with the HIPAA standard provided by the AWS business partner appendix). As shown in Figure 4(b), Alamir [31] analyzed the needs of EHR sharing in the UAE and developed a shared EHR system. The system has three users, including patients, hospital management and professional physicians. The CA is assumed by the government of the Emirate of Alin and is responsible for issuing IDs to users. CA provides a user interface and sets access levels, and creates a shared chain code. The patient checks the medical history and other information through the Hyperledger client (inside the dotted box). The hospital management adds the patient’s detailed information and verifies the EHR uploaded by the patient through the Hyperledger client. Professional physicians can view medical history, family medical history and other information (in the dotted box) through the Hyperledger client. These sharing requests are sorted through the Orderer, and then the EHR is shared through two channels. As shown in Figure 4(c), Alshalali [32] developed an EHR sharing system between laboratories, hospitals and insurance companies on the Fabric template. The hospitals, laboratories, and insurance companies in the system can perform two operations through the client: 1 create a transaction and 2 calls a transaction. The client accesses the permissions in the chaincode through Hyperledger. Users with access rights store the encrypted pointer and patient ID of the EHR in the Hyperledger, and store the EHR in the off-chain database (provided by the local healthcare provider). The system takes doctors sharing EHR as an example: When doctors want to share EHR, they can access it through the client. The client creates a shared transaction and sends it to the patient client. After the patient’s first approval, the doctor will be identified and the identification will be stored. As shown in Figure 4(d), Roehrs [33] constructed an EHR sharing model based on the FHIR standard. The model divides medical data providers into three roles, including doctor’s office, hospital, and clinician. The EHR provided by the provider is divided into two types, one conforms to the FHIR standard, and the other conforms to other standards. The system stores the EHR conforming to the FHIR standard in the Hyperledger through the channel. The system automatically converts other standard EHRs through the data converter and stores them in the Hyperledger. Hyperledger uses middleware and blockchain to convert EHR into visual data. Patients can view their EHR information through the Hyperledger. As shown in Figure 4(e), Kumar [34] developed a shared EHR system. The system has three entities, including patient, organization 1 and organization 2. When the patient visits the organization, the organization will register an ID for the patient and store the EHR provided by the patient (detailed information in the

dotted box) in the organization's own DB. After the patient finishes the consultation, the DB will be updated accordingly. When organization 2 wants to share the EHR in organization 1, it first applies to organization 1, and after organization 1 obtains the patient's consent, it will share the EHR with organization 2. As shown in Figure 4(f), Kaur [35] proposed a shared model of distributed storage EHR. As shown in the figure, both patients and doctors (Doctor 1 and Doctor 2) must first request registration from the administrator, and the Hyperledger will issue identity certificates and public and private keys to the patients and doctors. After the patient has registered the identity, the entity allowed to access the EHR can be preset. The visiting doctor (Doctor 1) has the right to access EHR during the treatment, including adding and querying. The doctor in the doctor stores the updated EHR hash value and transaction information on the blockchain through the smart contract (chain code), and the hyperledger stores the real EHR in the IPFS. When doctor 2 wants to access the EHR, he needs to make a request to the system, and the system will query whether the doctor exists through the smart contract, and then the query block will return the EHR directly. When TPA accesses EHR, he needs to request access rights from the patient through Hyperledger. After the patient agrees, TPA will access the EHR through the Hyperledger query block. As shown in Figure 4(g), Uddin [36] proposed a way to integrate and manage the healthcare ecosystem. As shown in the figure, the patient registers through the Registration Desk and obtains the key. The Registration Desk retrieves the registration status of the patient from the Record patient information, and determines whether the patient is already registered or unregistered. The Registration Desk requests the local CA to create an ECert key and returns the key to the patient. The Registration Desk will perform endorsement and sorting of the EHR, and the accounting node will add a new block. The Primary physician (the steps performed by the Primary physician are the thick black lines in the figure) will submit the updated EHR during diagnosis to the Hyperledger for endorsement, and the Orderer will send the endorsement result to the accounting node to add blocks. When it comes to the operation of related patients, insurer, pharmacies, researchers, and laboratories all store updated EHR (in the dotted box) to the Hyperledger, and the general ledger of the system provides EHR sharing.

As shown in Figure 4(h), Margheri [37] proposed a proxy-based re-encryption method to share EHR. The system is integrated with the XDS EHR system. The system has three entities, including EHR source, EHR consumer and Hyperledger. Proxy retrieves EHR through chain code and obtains EHR from EHR sources. Proxy is responsible for intercepting EHR documents, digitally signing and standardizing them, and converting EHR documents into standard documents. The document is marked with a chain code and converted into a PROV document. XDS EHR system stores PROV files in Hyperledger. When the EHR consumer makes a query and retrieval request, another Proxy obtains the PROV document from the Hyperledger and shares it with the EHR consumer.

As shown in Figure 4(i), Tith [38] proposed an EHR system protected by a proxy re-encryption method. When user 1 wants to share his EHR with user 2, he uses the AFGH encryption algorithm [39], [40] to encrypt his private key and user 2's public key into a re-encryption key. And use your own public key to encrypt EHR. Hyperledger stores EHR in the on-chain DB. The agent downloads the encrypted EHR from the DB, and uses the re-encryption key to encrypt the EHR. User 2 decrypts the EHR with its own private key. There are also some studies focusing on the access control strategy in the EHR of Hyperledger.

As shown in Figure 4(j), Kumar [41] proposed a system for sharing EHR in IOT devices. The system has five entities, including NA, TA, Client, PDA and Hyperledger. NA is responsible for performing registration, identification and issuing keys for these five entities. TA is responsible for tracking malicious users and revoked users from the client. The data PDA is composed of multiple device data and Fabric SDK. The client collects data from the PDA, signs the data with the ECDSA scheme, and stores it in the Hyperledger. In the system, Hyperledger is divided into two types of nodes: Ordering peers and Endorsing and committing peers. Ordering peers uses the PBFT consensus algorithm, which is responsible for ordering transactions from clients. These transactions will generate corresponding transactions, encrypted by IDBGSC. The encrypted transaction is updated to the ledger through Endorsing and committing peers.

As shown in Figure 4(k), Munoz [42] focused on the design of mobile terminals for users and researchers and developed an EHR system. The system mainly provides services for three roles, including patients, doctors and researchers. Patients can add or delete IOT (internet of things) devices, store EHR (in the dashed box) in the Hyperledger, and can grant or revoke the user's EHR access permission. In addition, patients can access the projects their EHR is involved in. Doctors edit their own public files on Hyperledger and access EHR. Researchers can add or modify the details of existing research projects and visit EHR. The system stores the text-based diagnosis in the Hyperledger, and the media-based diagnosis in the off-chain database.

Some studies focus on the privacy protection of patients in the EHR system. As shown in Figure 4(l), Mikula [43] proposed an EHR system that focuses on identity and access. The user sends the request for storing EHR to the APP-Server through the mobile terminal, web and Standalone app. APP-Server delegates the verification work to Auth-Server, and Auth-Server will verify the user's identity through the Hyperledger. The Hyperledger determines the user's identity through the chain code and the consensus of multiple members. After the system confirms the user's identity, APP-Server will update the account book to the DB. As shown in Figure 4(m), Prasad [44] proposed a method of verifying the public key of the group to protect the private key of the patient. The system has a group administrator who is responsible for creating a master public key for group members and a private key issued to each group

member. When a group member wants to store the EHR, he only needs to sign and encrypt it with the master public key, and upload the encrypted EHR to the Hyperledger. In order to ensure that the group members are not malicious, the Hyperledger sends a request to verify the identity of the member to the group member module. After the verification is received, the Hyperledger will store the EHR. As shown in Figure 4(n), Bhavin [45] proposed a model that uses a combination of quantum encryption and Hyperledger to protect EHR. The model has four participants, including admin, lab staff, patients and clinicians. The admin is responsible for the changes of participants, and can add, delete, update and query participants in the Hyperledger. Lab staff can apply to visit the EHR and update the EHR when the patient visits. The patient has the right to read, write and delete EHR. Clinicians have the authority to apply for access to the EHR and to update the EHR for treatment. Among them, each shared transaction is encrypted using quantum encryption. The quantum key is completed by the trader and the block creator. As shown in Figure 4(o), Stamatellis [46] uses Hyperledger to construct a hybrid identity verifier. The system has three verification entities, including health centers, hospitals, and public health. In every entity there are peers, MSP and ledger. The MSP is responsible for the identity verification of all nodes in the entity. The EHR of each entity is endorsed by peers and updated to the ledger. The health center includes public ledgers (information in the dotted box) and private ledgers (information in the dotted box). When three types of EHR are updated to the system, each transaction is submitted to the Orderer service for endorsement. The endorsement result should be verified by at least two validators before being updated to the system ledger. As shown in Figure 4(p), Meena [47] developed a patient-centric EHR sharing system. The patient submits the appointment ID to the doctor, and the doctor chooses to accept or reject the appointment according to the actual situation. After the patient's visit, the patient's laboratory report and other examinations are sent to the locked prescription. At this time, the hospital will remind the patient to update the re-encryption key and generate a bill. After the patient has paid all the bills, the prescription will be decrypted. The pharmacy generates a bill for the prescription drugs and sends it to the patient, and the pharmacy sends the drug to the patient after the patient pays the drug bill. When a patient needs to make an automatic medical claim, the insurance company will reimburse it according to the specific conditions of the patient's bill in the system.

There are also some studies focusing on the access control strategy in the EHR of Hyperledger. As shown in Figure 4(q), Guo [48] designed an access control strategy for edge nodes. Patients collect EHRs through smart sensors and imaging devices, store them in Hyperledger, and define access permissions. These sensors and devices send the patient's EHR to the edge node, generate a one-time self-destruct URL through the ABAC (Attribute Based Access Control) access strategy, and send it to the Hyperledger. Hyperledger will locate edge nodes and check the accuracy of URL. When doctors and

nurses want to share EHR, they need to access through the chain code, and the system will retrieve the access permission in the ACL. Users with access permission will get the URL.

Some research focuses on the management of EMR. As shown in Figure 4(r), Hang [49] proposed the EMR sharing system. The system allows four types of users to participate: patients, doctors, nurses and management. Users interact with Hyperledger through the APP, including registration, verification and transactions. The Hyperledger includes four hospital departments. To ensure the safety of EMR between hospital departments, each two departments need to pass through different channels (channels 1, 2, 3, 4) when sharing EMR. The user sends a sharing request to the Hyperledger through the APP, and the Hyperledger will share the EMR with the user through a specific channel.

As shown in Table 3, this article summarized the above solutions and compared the implementation of each solution in four aspects, including traceability, monitoring, security, and privacy.

2) PHR SYSTEMS BASED ON HYPERLEDGER

As shown in Figure 5, this article shows the comparison of PHR solutions by reconstructing the architecture diagram.

As shown in Figure 5(a), Im [50] proposed a PHR sharing system based on the GDPR Act. The system realizes the sharing of medical records between three entities, including hospitals, clinical research centers and patients (peer 3). The hospital includes a medical team (peer 1) and an accounting team (peer 2), and the clinical research center includes people engaged in experiments and research (peer 4). The same ledger pattern in the figure shows the ledger that can be shared between different peers, and the same chaincode pattern shows that different peers can share the ledger through the same smart contract. The system has established two channels: peer 1 shares the ledger with peer 3 through Channel 1, and peer 4 shares the ledger with peer 3 through Channel 2. Peers joining the channel can send sharing requests to other peers. These requests are first sorted by the Orderer, and then the system processes these sharing events. As shown in Figure 5(b), Choi [51] proposed a shared PHR system (the system creates two blockchains in the Hyperledger, including a private write set blockchain and a blockchain). The user first performs the de-identification process (to ensure user privacy) through the chain code, and stores the de-identification process and results in a private DB. The private DB stores the de-identification process and results in the private writing set blockchain by verifying the user's signature and de-endorsing policy. And store the hash value of the above information in the public state DB. After the above steps, the user visits the hospital through the chain code. The hospital transmits the PHR through the chain code, and stores the PHR and transaction results in the public state DB. The public state DB stores the hash value and PHR of the transaction in the blockchain after the two operations of signature verification and endorsement strategy. After users provide PHR, they can obtain rewards from healthcare companies through the

TABLE 3. Analyze the EHR and EMR solutions based on hyperledger.

Name of EHR solutions	System test platform	Summary	Traceability	Monitoring	Security	Privacy
Action-EHR	Hyperledger Fabric	By storing only metadata on the chain, the way the actual data is stored on the cloud reduces turnaround times for data sharing and reduces storage pressure.	✓	✓	✓	✓
Mblocks	Hyperledger Fabric Hyperledger Composer	Through the composer online platform, the development time of EHR sharing system is greatly reduced.		✓	✓	✓
Tagrid Alshalali et al.	Hyperledger Fabric	Verify the effectiveness of the Fabric network for patient privacy and data storage.	✓	✓	✓	
B4HEALTH	Hyperledger Fabric	By testing and comparing the Hyperledger and Ethereum to develop the EHR system at the same time, it is proved that the Hyperledger has better performance.	✓	✓	✓	✓
Naveen Kumar S et al.	Hyperledger Fabric	Through multiple sets of tests, it is determined that the Hyperledger-based EHR system has strong shared reliability.		✓	✓	✓
Jasleen Kaur et al.	Hyperledger Fabric Hyperledger Caliper	By storing the hash value of the EHR in the Hyperledger and storing the EHR in the IPFS, the storage pressure on the chain is greatly reduced.			✓	
Mueen Uddin et al.	Hyperledger Fabric	Through the realization of interoperability between six entities, including patients, doctors, laboratories, insurance companies, pharmacies and researchers. This method improves the applicability of EHR sharing.				
eHealth systems	Hyperledger Fabric	Speed integration with existing EHR systems with a PLOV proxy strategy.	✓	✓	✓	✓
Dara Tith et al	Hyperledger Fabric	The sensitive data of patients is well protected by a proxy re-encryption EHR scheme	✓	✓	✓	✓
MedHypchain	Hyperledger Fabric	Encrypting each transaction through a group signature greatly improves the confidentiality of EHR.	✓	✓	✓	✓
ClinicAPPChain	Hyperledger Fabric	The development cost of EHR systems is reduced through a lightweight distributed network.	✓	✓	✓	✓
Tomas Mikula et al.	Hyperledger Fabric	Through the test of an EHR use case, it is determined that the Hyperledger has good performance in identity and access management.		✓	✓	✓
Healthcare Record-Keeping	Hyperledger Fabric	The feature document is validated with a group public key, so members do not have to expose the personal public key when sharing the EHR securely.	✓	✓	✓	✓
Name(author) of EHR solutions	System test platform	Summary	Traceability	Monitoring	Security	Privacy
Blockchain and quantum blind signature hybrid scheme	Hyperledger Fabric Hyperledger Caliper	Using quantum blind signatures to create blocks and proposing a role-based access control reduces access latency and improves the privacy of transactions. However, the programme is close to centralization.	✓	✓	✓	✓
PREHEALTH	Hyperledger Fabric	Access to private data separates from public accounts, effectively reducing query overhead.	✓	✓	✓	✓
Proxy Re-encryption in permissioned Blockchain	Hyperledger Fabric	A medical structure centered on patient privacy has been designed to improve the privacy of patients in India.	✓	✓	✓	✓
Hybrid architecture of blockchain and edge node	Hyperledger Fabric Hyperledger Composer	EHR's secure access is enhanced through an access control combined with edge nodes and asymmetric encryption.		✓	✓	✓
Medical Blockchain for EMR Integrity	Hyperledger Fabric	By deploying and testing the EMR system, the feasibility of Hyperledger management in medical records was determined.	✓	✓	✓	✓

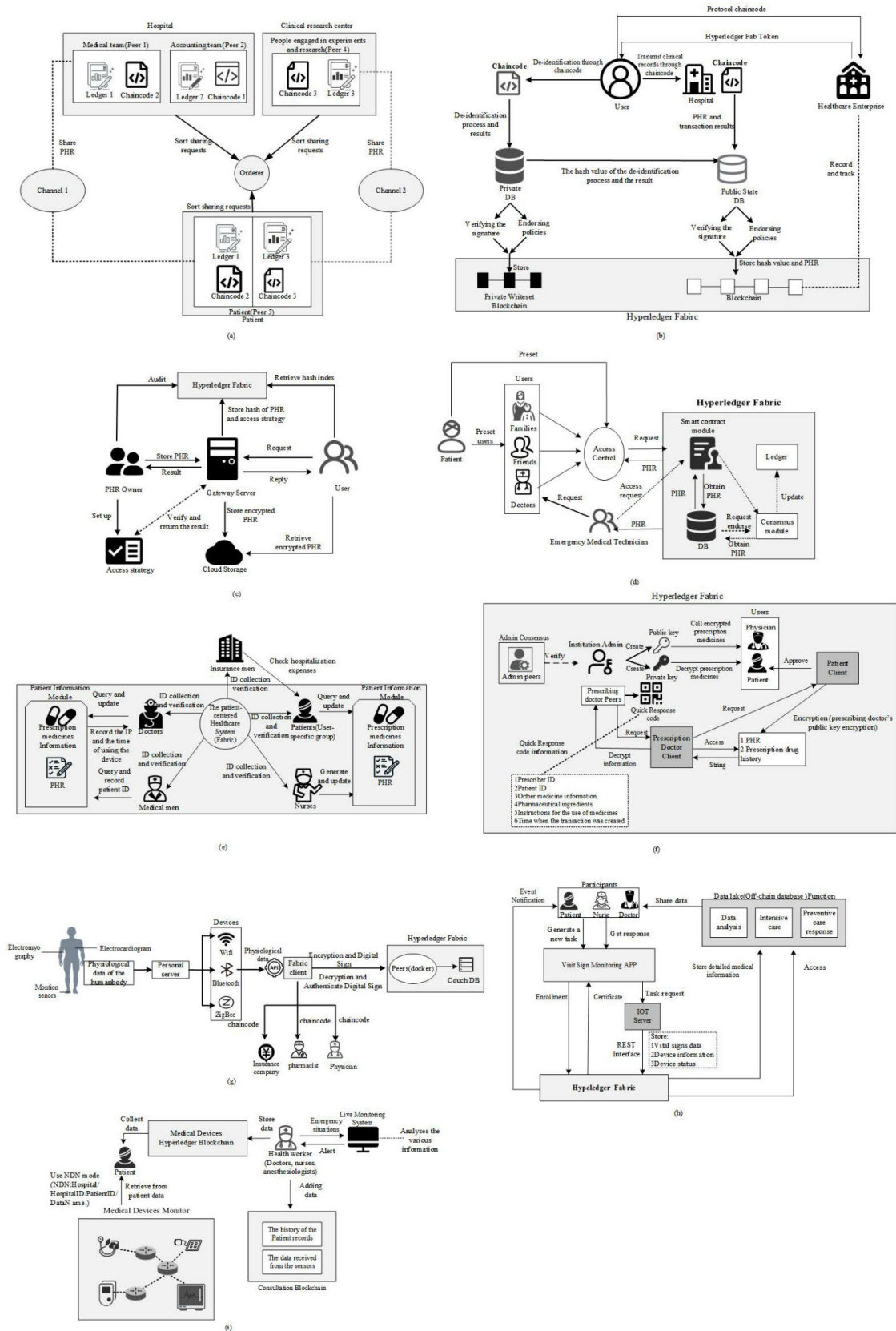


FIGURE 5. 5(a) Consortium blockchain in healthcare, 5(b) Healthcare data management and sharing platform, 5(c) Secret data sharing model for PHRs, 5(d) EACMS, 5(e) Patient-centered Healthcare system, 5(f) DMMS, 5(g) ATEAR, 5(h) Healthcare LOT blockchain platform.

signed chain code (the system distributes rewards through Fab Token). As shown in Figure 5(c), Thwin and Vasupongayya [52] proposed a system for storing PHR separately. The PHR owner requests the gateway service to store the PHR and sets the access policy. The gateway stores the hash value and access strategy of the PHR in the Hyperledger, and stores the encrypted PHR in the cloud storage. When a user sends a sharing request to the gateway, the gateway verifies the authority through the access policy and returns the result. Users who can pass the access policy retrieve the hash index from the Hyperledger, and retrieve the PHR in the cloud through the hash index. Patients can audit access records through the Hyperledger.

When a patient is being rescued, usually the patient is unconscious and cannot provide the doctor with a personal key sharing PHR in time. Therefore, as shown in Figure 5(d), Rajput [53] proposed a system for sharing PHR during first aid. In an emergency, the patient can preset the patients (including family, friends, and doctors) who are allowed to access the PHR. These users access the smart contract module in the Hyperledger through access control. The smart contract module obtains the PHR from the DB and returns it to the user. When emergency medical technicians need to share PHR, they can request the above-mentioned operations or use Hyperledger. The emergency medical technician first applies for a sharing request through the smart contract, and then endorses it through the endorsement module, and finally returns the PHR to the emergency medical technician. At this time, Hyperledger will update the access record to the ledger.

Prescription drugs refer to drugs that must be prepared, purchased, and used only with a prescription provided by a practicing physician. Some studies focus on the sharing of personal prescription drug records. As shown in Figure 5(e), Duong-Trung [54] developed a system for sharing the history of prescription drugs (Considering the overall effect of the architecture diagram, two patient information modules are designed, and the two patient information modules are indistinguishable). There are five types of participants in the system, including doctors, insurance men, medical men, patients and nurses. Each role needs to be collected and verified by ID to operate on prescription drug information and PHR through Hyperledger. Doctors can query and update information, and the information module will return the relevant record IP and the time of using the device to the doctors. The medical men have the authority to query and record the patient ID. The insurance men can check the patient's hospitalization expenses through the Hyperledger. Patients have the right to inquire and update. Nurses have the authority to generate and update. As shown in Figure 5(f), Li [55] proposed a management model for personal prescription drug history. The hospital in this model has three main entities, including endorsement administrators, institutional administrators and prescribing doctors. After the endorsement manager endorses, confirm the institutional manager of the hospital. Institutional management is responsible for creating public

and private keys for clinicians and patients. The public key is used to call and encrypt prescription drugs, and the private key is used to decrypt prescription drugs. Each prescriber uploads his prescription drug information to the Hyperledger (the specific information is in the dotted box), and generates a QR code for easy access by the patient. When the prescribing doctor wants to share the patient's prescription drug history, the prescribing doctor client first sends a request to the patient client. After the patient's approval, the patient client uses the prescribing doctor's public key to convert the encrypted information into a string, and returns it to the prescribing doctor's client. The prescriber uses his private key to decrypt the information.

Some research focuses on the monitoring of portable medical devices for personal use. As shown in Figure 5(g), Shahbazi [56] proposed a system for sharing data from wearable medical devices. The system monitors three types of data, including electromyography, monitoring sensors and electrocardiogram. These human physiological data are collected by personal servers and then by Wi-Fi, Bluetooth and Zigbee devices. These portable devices connect to the Hyperledger client through an API interface, and encrypt and digitally sign the data. The encrypted data is uploaded to the Hyperledger (the solution is run by Docker), and the encrypted data is finally stored in Couch DB. The system allows insurance companies, pharmacists and clinicians to access these shared data through chain codes. As shown in Figure 5(h), Jamil [57] proposed a vital signs monitoring system. The system showed three participants, including patients, nurses and doctors. Participants can perform two operations through the monitoring APP: create a new task and get the response of the task. Participants need to perform registration and verification operations with Hyperledger before using the monitoring system. After registration, patients will store their medical data (in the dashed box) in the Hyperledger. Hyperledger stores detailed medical data in an off-chain database, which is used for data analysis, intensive care and preventive health care. When doctors and nurses send task requests (monitoring requests) to IOT, the IOT service connects to the Hyperledger through the REST interface. Hyperledger will access the data lake and share the data with medical staff. As shown in Figure 5(i), Attia [58] proposed a system for multiple chains to jointly monitor medical equipment information. The system has four networks, including Medical Devices Hyperledger Blockchain, Medical Devices Monitor, Consultation Blockchain, and Live Monitoring System. The Medical Devices Hyperledger Blockchain is responsible for collecting IOT data from medical devices carried by patients and storing data on healthcare workers. Medical Devices Monitor uses NDN mode to retrieve patient data and monitor the patient's status. When the patient is in an emergency, the Live Monitoring system will issue a warning to health workers. The system can analyze the monitored data. Health workers add PHR and IOT data to the Consultation Blockchain.

As shown in Table 4, this article summarized the above solutions and compared the implementation of each solution

TABLE 4. Analyze the PHR solutions based on hyperledger.

Name of PHR solutions	System test platform	Summary	Traceability	Monitoring	Security	Privacy
Consortium blockchain in healthcare	Hyperledger Fabric Hyperledger Composer	Through chain code, patients are given shared control rights, which greatly improves the privacy of PHR.	✓		✓	✓
Healthcare data Management and Sharing Platform	Hyperledger fabric	By storing data in a private database, the hash value is stored in a public database. Ensure the integrity and privacy of the PHR. But the processing speed of this program is slow.	✓		✓	✓
Secret data sharing model for PHRs	Hyperledger Fabric	Only the data owner can decrypt the PHR stored on the cloud, and the private key is re-encrypted and encrypted by the proxy, which enhances the security of the PHR.	✓	✓	✓	✓
EACMS	Hyperledger Fabric	Through a pre-set access contract, the sharing of PHR in emergency situations is realized, and the medical efficiency of emergency personnel is improved.	✓	✓	✓	✓
Patient-centered Healthcare system	Hyperledger Fabric	Through five types of access control contracts, the protection of sensitive patient data has been strengthened.	✓	✓	✓	✓
DMMS	Hyperledger Fabric	Increase the level of security and privacy through Fabric, enabling faster and more complete query of personal drug history.	✓	✓	✓	✓
ATEAR	Hyperledger Fabric	Through the ATEAR routing protocol, the optimal multi-hop path is selected when the node temperature is too high. Avoid frequent division of WBAN and improve the adaptability of WBAN.	✓	✓	✓	✓
Healthcare LOT blockchain platform	Hyperledger Fabric	Support resource-constrained medical IoT devices through a lightweight distributed network, and only execute data transactions from sensors on the Hyperledger. Improved the usability of the blockchain system.	✓	✓	✓	✓
Healthcare Monitoring	Hyperledger Fabric	Through the shared ledger of 4 distributed networks of medical equipment, medical equipment chain, monitoring chain and consulting chain, better monitor the vital signs of patients.	✓	✓	✓	✓

in four aspects, including traceability, monitoring, security, and privacy.

C. APPLICATION IN THE FIELD OF MEDICAL IMAGES

Medical image is an important diagnostic data, which has a wide range of applications, including medical engineering, medical physics, and biomedical informatics. For example, medical images are an important source of anatomical and functional information in biomedical research [59]. The development of medical image models can integrate clinical and imaging data [60], and pixel-based medical imaging models can also process EHR context data and pixel data capabilities [61]. However, a large number of medical images are managed in an “island” style, which leads to the need for

repeated examinations when patients go to different hospitals. In a survey in the United States, 15% of people report that they must carry radiological examinations or other test results, and 5% of patients need to repeat the examination or procedure because they cannot obtain the previous results [62].

Sharing medical images can solve these problems well. For example, sharing medical images not only saves patients from unnecessary repetitive expenses, but also provides clinicians with more cases and improves the knowledge base of medical image diagnosis [63]. Community hospitals or clinics also have the opportunity to obtain diagnosed cases and related image research from large hospitals. Therefore, this article summarizes the key reasons for the urgent need for sharing in medical imaging systems:

- (1) Some medical imaging equipment is very expensive, and few hospitals have these equipment. And one equipment failure will affect the operation of the entire hospital [64].
- (2) The cycle of updating medical imaging devices is very long (usually about 3-7 years), and requires a lot of legal approvals and sufficient reasons.
- (3) The scanning of imaging equipment (such as CT) is defined in the scanning configuration file in the PC controlled by the host. Therefore, these images are vulnerable to various attacks. The impact of this attack can even control the entire CT operation, putting the patient at a very high risk [64].
- (4) Repetitive medical imaging examinations will increase unnecessary radiation or other risks for patients.

The sharing technology of medical images also faces some major challenges: some medical imaging applications require a large bandwidth to be used as a real-time video streaming of medical images. These medical images include real-time video streams of ultrasound imaging, angiography, and endoscopy. Therefore, many types of medical images are difficult to compress effectively [65]. Medical image sharing requires the transmission of physical copies (such as CDs or DVDs). During the image import process at the receiving site, the digital assets are transcribed to an optical medium that is usually read only once. This method has obvious inefficiency and waste [66]. The emergence of Hyperledger technology has brought opportunities to solve the above problems. Therefore, this article reviews related research on Hyperledger's solution to the problem of medical image sharing. In Figure 6, this article provided an intuitive comparison of these solutions.

As shown in Figure 6(a), Seo [67] developed a medical image sharing system based on Hyperledger. The system first preprocesses the image and extracts the Region of Interest (ROI), and uploads the image to the anonymous module for processing. The anonymous module sends the SQL K value of the data owner to the private blockchain, and the private blockchain returns the anonymous table to the data owner. The private blockchain stores the original tables and images in PACS. The system sends the anonymized image to the voting module, and the experts will vote to decide whether to share the image. As shown in Figure 6(b), Cho [68] implemented voting-based prediction of the bone age of Korean adolescents. The system extracts the region of interest from the bone image and sends it to the image processing module (including feature maps, basic learners and classifiers). The image is processed and uploaded to the TW3 prediction system. The TW3 system creates a new block to store the bone images of these teenagers. The nodes in Hyperledger share these images. The Korean Growth Medicine will vote on the images of each bone and determine the reference image for the bone age standards of Korean adolescents. The reference image is stored separately in the reference database.

D. APPLICATION IN THE OTHER FIELDS OF MEDICAL

There are still a small number of Hyperledger applications in other medical fields, including hospital financial income, automatic insurance claims, and improvements in system performance and dynamic processing. This article summarizes these studies into this chapter for unified analysis and comparison. In Figure 7, this article gave the most intuitive comparison of all the solutions.

1) FINANCIAL INCOME OF THE HOSPITAL

As shown in Figure 7(a), Upadhyaya *et al.* [69] proposed a shared system based on three German hospitals. A global channel (i.e. shared channel) is created by a tertiary hospital, and Hospital A and Hospital B join the channel by submitting X.509 or RSA certificates. The two hospitals share medical data under agreed smart contracts. When Hospital A has new medical information to share, Hospital A makes a verification request to Hospital B. Hospital B returns validation results. Hospital A submits the completed validation and medical information to Orderer sorting in the form of transactions, and finally the system updates the global ledger. This solution can change the internal resource allocation of hospitals, enabling them to generate 63% of their revenue.

2) AUTOMATIC CLAIMS FOR MEDICAL INSURANCE

As shown in Figure 7(b), Xinchu *et al.* [70] have developed an automated claims system based on Hyperledger. The patient submits his or her medical records (specific information in a dotted box) to the medical provider, which returns the patient with a health insurance bill. Patients can check the status of insurance claims through bills. The insurers sign smart contract 2 with the patient (the specific information is in the dotted box), and the medical provider signs the automatic claim smart contract 1 with the insurers. When a patient needs a medical claim, contracts 1 and 2 are automatically executed to complete the claim. When an insurance claim transaction is successful, each entity submits the completed transaction to the Hyperledger through a different system or client for endorsement and updating the ledger.

3) MEDICAL SYSTEM PERFORMANCE AND DYNAMIC PROCESSING

In terms of system performance: Agbo *et al.* [71] described the differences in the structure, security and performance of Bitcoin, Ethereum and Hyperledger, and determined that Hyperledger is the best of the three technologies for developing medical systems. In order to enhance the efficiency of verifying keys, as shown in Figure 7(c), Tian *et al.* [72] proposed a key sharing model. Patients pre-select the object of the shared key from the user base (pictured are lawyers and pharmacists). The patient generates a QR code for the public key and the selected results and sends it to the attending physician. The attending physician sends medical advice to the Hyperledger by sharing the key. Pharmacists send drug information and expenses to the Hyperledger by sharing keys.

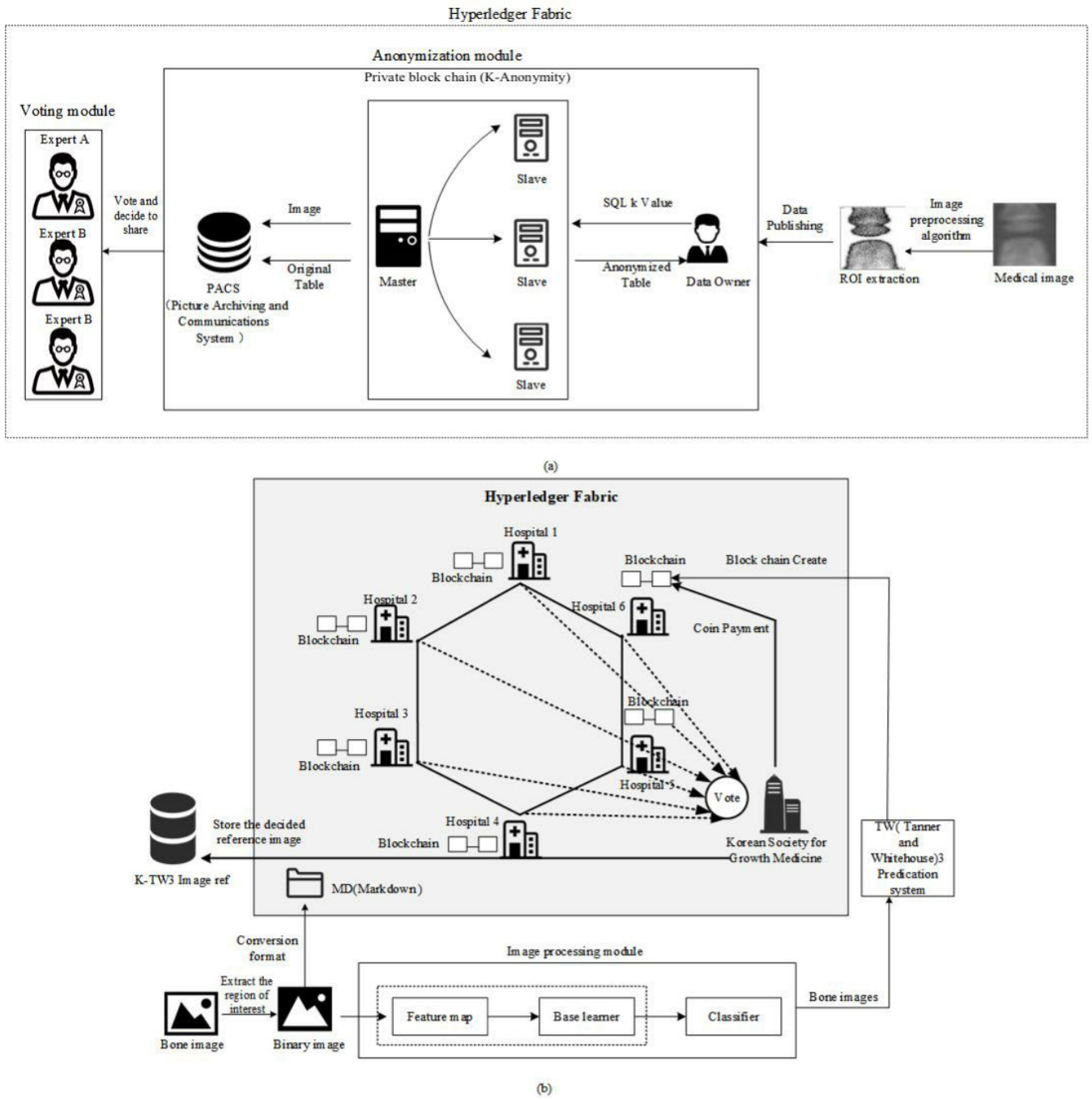


FIGURE 6. 6(a) PACS, 6(b) Bone-age prediction system.

The lawyer sends the diagnostic certificate to the Hyperledger by sharing the key.

In the dynamic processing of medical systems: Bell-CLaPadula (BLP) model is a classic method to achieve effective access control and multi-level security (MLS). But this method lacks dynamics. As shown in Figure 7(d), Kumar et al. [73] upgraded the Bell-CLaPadula (BLP) model. The model divides the roles in the system into four types through smart contracts, including supervisors, managers,

technicians, and employees. Each of the four roles has different permissions. Supervisors can comment and read access control of data. Managers can update, delete, and read data. Technicians are limited to reading data access. Ordinary employees are limited to reading data access. The model uses a variety of roles for dynamic digital medical data processing and access.

The dynamic management of patient consent in clinical trials (CTs) will directly affect the efficiency of analyzing

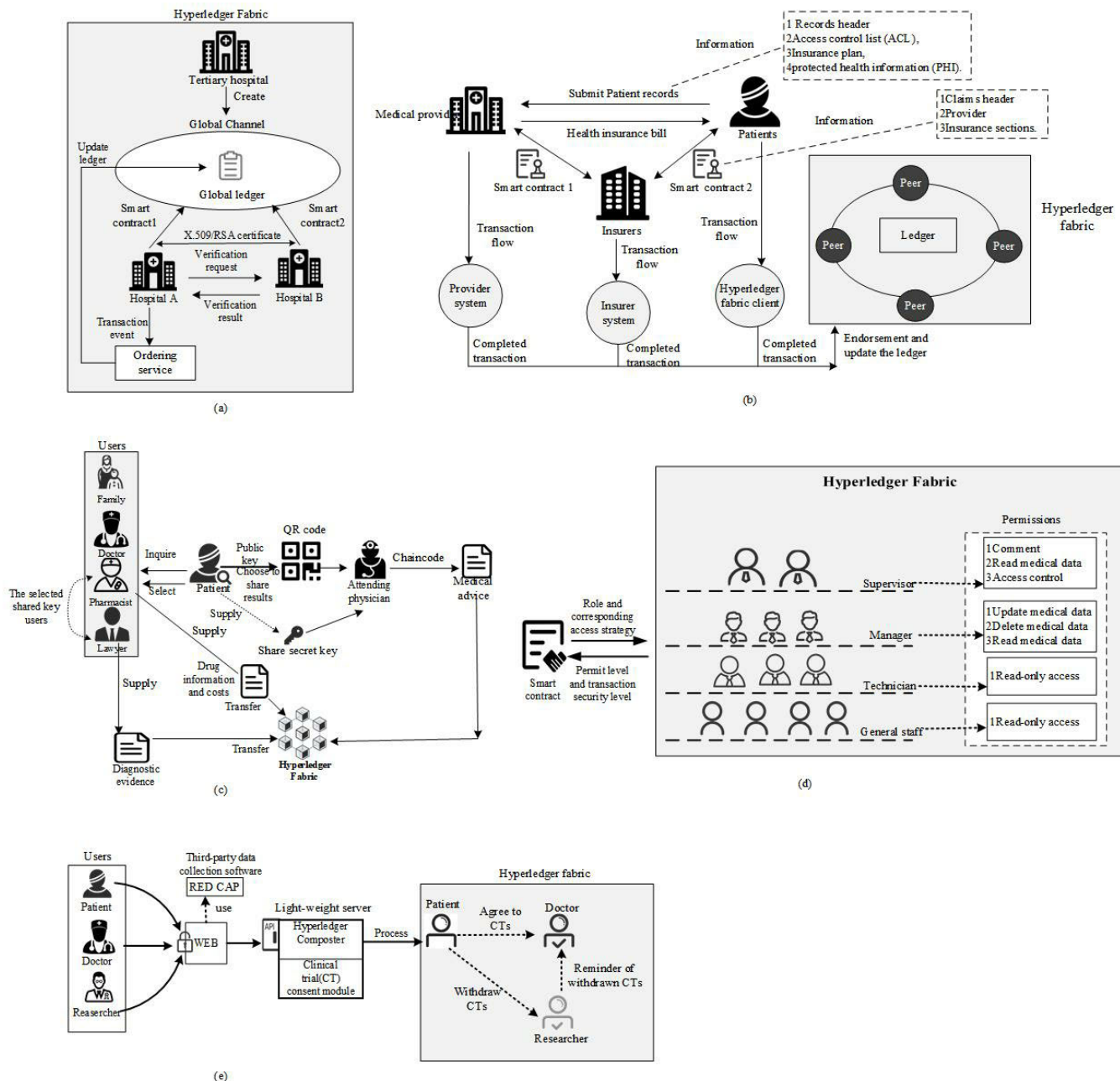


FIGURE 7. 7(a) Optimal healthcare system, 7(b) Health insurance claim system, 7(c) Cornelius C. Agbo et al., 7(d) Haibo Tian et al., 7(e) EBLP, 7(f) SCoDES.

new drugs and (biological) medical devices. As shown in Figure 7(e), Albanese *et al.* [74] proposed a module for dynamically processing CTs. There are three roles in the model, including patients, doctors, and researchers. These three roles connect to a lightweight service through WEB (and possibly RED CAP, third-party data collection software). The service includes Composter and CT trial modules. The user uses these two modules for the dynamic processing of CT consent forms. If the patient withdraws the CT with one of them; the other receives timely cancellation information.

In Table 5, this article summarized the above solutions and compared the implementation of each solution in

four aspects, including traceability, monitoring, security and privacy.

IV. FUTURE TRENDS AND PROSPECTS

A. SHARING OF DNA DATA

DNA data can help biologists and medical workers advance research. Such as molecular cloning, breeding, discovery of pathogenic genes, comparative and evolutionary studies [75]. But each person has about 3 billion base pairs [76], and personal genetic data requires a lot of storage space. How to safely store and share genetic data with authority is an important new business of HIS. Liu *et al.* [75] pointed out that

TABLE 5. Analyze the other medical fields solutions based on hyperledger.

Name(author) of solutions	System test platform	Summary	Traceability	Monitoring	Security	Privacy
Optimal healthcare system	Hyperledger Fabric	Through multiple chain codes, the internal process of the hospital was changed, and 63% of the financial income was obtained, and the effectiveness of the scheme was verified through the balanced scorecard.	✓		✓	
Health insurance claim system	Hyperledger Fabric	By separating the Hyperledger structure from the original insurance system, the compatibility and scalability of the new system are improved.	✓	✓	✓	✓
Cornelius C. Agbo <i>et al.</i>	NULL	Explained in detail the comparison of Bitcoin, Ethereum and Hyperledger in terms of structure and security. Determined the feasibility of Hyperledger in the field of healthcare.	NULL	NULL	NULL	NULL
Haibo Tian <i>et al.</i>	Hyperledger Fabric	The SIFF method is used to share the key for the first time, which improves the security of the shared key.	✓	✓	✓	✓
EBLP	Hyperledger Fabric	Through 4 different roles of access control contracts, the Bell-Lapadula model is enhanced, and the scalability problem of the blockchain network is alleviated.	✓	✓	✓	✓
SCoDES	Hyperledger Fabric	Deal with the dynamic changes of the clinical trial consent form through a three-tier distributed structure.	✓	✓	✓	✓

companies such as BGI are trying to establish cloud services to store genetic data. Compared with cloud services, Hyperledger can provide reliable sharing services and distributed storage of DNA data, alleviating this storage pressure.

B. PROTEIN FOLDING CALCULATION

Protein chains have a large number of folded states that are difficult to understand. The problem of protein folding is how the amino acid sequence of a protein determines its three-dimensional atomic structure [77]. Efficiently predicting the natural structure of a protein based on the sequence of amino acids will help drug development and DNA sequencing. Stanford University previously relied on very expensive supercomputers to simulate the protein folding process. However, the calculation of the protein folding process requires a lot of cost and is limited to a single protein structure. Hyperledger can effectively provide distributed computing for protein folding prediction, and a huge distributed network will bring high-speed computing power.

C. MEDICAL IMAGE SHARING

How to promote the safe sharing of medical images is a major challenge. AMA magazine pointed out that compared with internal organs, especially skin disease images, facial images, and cancer images. These images make it possible to distinguish the identity of the patient only by the human eye. Therefore, these medical images should be vigilant and sensitive [78]. In addition, the sharing of medical images must not only ensure the privacy of patients, but also respect cul-

tural and religious views. As mentioned earlier, Hyperledger supports multiple encryption algorithms and can encrypt different types of images. And each provider of medical images autonomously controls the sharing authority. For example, patients of different religions can achieve religious sharing through different Hyperledger communities.

D. MACHINE LEARNING ASSISTED THERAPY

Machine learning technology makes the analysis and diagnosis of medical data more intelligent. Bradley J. Erickson *et al.* believe that the algorithm system of machine learning is used to identify important image features, which can effectively assist medical diagnosis [79]. In addition, machine learning can help automatically interpret and report CTPA (Computed Tomography Pulmonary Angiogram) inspections. This method immediately triages emergency cases to doctors, thereby shortening the time for diagnosis and treatment [80]. But the model of the data set faces the risk of being inferred and being hacked. The combination of Hyperledger and machine learning will more effectively promote the development of smart hospitals, including forecasting, model security, and self-service inspections.

V. CONCLUSION

The application of Hyperledger in the HIS field is an important technology to promote the reform of hospital information systems and improve the security of medical information storage and sharing.

This work took the Hyperledger solution in the HIS field as the object and proposed a new way of comparison and analysis. In the method, this work extracted the core content and research details of each article, and upgraded and reconstructed the original architecture. Readers can intuitively observe the differences between Hyperledger solutions of the same type, especially how Hyperledger technology solves HIS problems, including interoperability, secure storage, real-time sharing and other issues. This work proved the feasibility and potential of Hyperledger in realizing a new generation of HIS.

In the future, we will upgrade this comparison method to make all reconstructions more readable and understandable.

REFERENCES

- [1] E. Ammenwerth, S. Gräber, G. Herrmann, B. T. rkleand, and J. K. and nig, "Evaluation of health information systems—Problems and challenges," *Int. J. Med. Informat.*, vol. 71, pp. 125–135, Sep. 2003.
- [2] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. Manuel, R. S. Tavares, V. Hugo, and C. Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognit. Syst. Res.*, vol. 52, pp. 1–11, Dec. 2018.
- [3] N. Andola, Raghav, M. Gogoi, S. Venkatesan, and S. Verma, "Vulnerabilities on hyperledger fabric," *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101050, doi: [10.1016/j.pmcj.2019.101050](https://doi.org/10.1016/j.pmcj.2019.101050).
- [4] K. Lampropoulos, G. Georgakakos, and S. Ioannidis, "Using blockchains to enable big data analysis of private information," in *Proc. IEEE 24th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Limassol, Cyprus, Sep. 2019, pp. 1–6.
- [5] S. Aggarwal and N. Kumar, "Hyperledger: An industrial approach to blockchain," in *Hyperledger*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 2–21.
- [6] W. Kennedy, B. Ketelsen, S. Martin and Erik, *Go in Action*. Shelter Island, NY, USA: Manning, 2016. [Online]. Available: https://www.worldcat.org/title/go-in-action/oclc/953022048&referer=brief_results
- [7] H. Zhang, X. Chen, X. Lan, H. Jin, and Q. and Cao, "BTCAS: A blockchain-based thoroughly cross-domain authentication scheme," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102538, doi: [10.1016/j.jisa.2020.102538](https://doi.org/10.1016/j.jisa.2020.102538).
- [8] T. Blummer, M. Sean, C. Cachin, *An introduction to Hyperledger*. Linux Found, 2018. [Online]. Available: https://www.Hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf
- [9] E. Androulaki, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Porto, Portugal, Apr. 2018, pp. 1–15.
- [10] H. A. Khattak, K. Tehreem, A. Almogren, Z. Ameer, I. U. Din, and M. Adnan, "Dynamic pricing in industrial Internet of Things: Blockchain application for energy management in smart cities," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102615, doi: [10.1016/j.jisa.2020.102615](https://doi.org/10.1016/j.jisa.2020.102615).
- [11] H. Liu, D. Han, and D. Li, "Fabric-IoT: A blockchain-based access control system in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020.
- [12] K. A. Wager, F. W. Lee, and J. P. Glaser, *Health Care Information Systems: A Practical Approach for Health Care Management*. San Francisco, CA, USA: Wiley, 2017. [Online]. Available: https://books.google.com/books?id=nfH6DQAAQBAJ&printsec=copyright&hl=zh-CN&source=gbs_pub_inf_r#v=onepage&q&f=false
- [13] A. Alkhodre, T. Syed, S. Jan, Y. Alsaawy, S. Khusro, and M. Khan, "A Blockchain-based value added tax (VAT) system: Saudi Arabia as a use-case," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 708–716, 2019.
- [14] B. Casassus, "Health agency reveals scourge of fake drugs in developing world," *Nature*, vol. 4, p. 10, Nov. 2017, doi: [10.1038/nature.2017.23051](https://doi.org/10.1038/nature.2017.23051).
- [15] P. Newton, S. Proux, M. Green, F. Smithuis, J. Rozendaal, S. Prakongpan, K. Chotivanich, M. Mayxay, S. Looareesuwan, J. Farrar, F. Nosten, and N. J. White, "Fake artesunate in southeast Asia," *Lancet*, vol. 357, no. 9272, pp. 1948–1950, Jun. 2001.
- [16] M. Shepherd, "Beef up international cooperation on counterfeits," *Nature Med.*, vol. 16, p. 366, Apr. 2010, doi: [10.1038/nm0410-366](https://doi.org/10.1038/nm0410-366).
- [17] C. Sheridan, "Bad medicine," *Nature Biotechnol.*, vol. 25, no. 7, pp. 707–709, Jul. 2007, doi: [10.1038/nbt0707-707](https://doi.org/10.1038/nbt0707-707).
- [18] D. Sinclair, H. Shahriar, and C. Zhang, "Security requirement prototyping with hyperledger composer for drug supply chain: A blockchain application," in *Proc. 3rd Int. Conf. Cryptogr., Secur. Privacy*, 2019, pp. 158–163.
- [19] R. Raj, N. Rai, and S. Agarwal, "Anti counterfeiting in pharmaceutical supply chain by establishing proof of ownership," in *Proc. IEEE Region 10 Conf. (TENCON)*, Kochi, India, Oct. 2019, pp. 1572–1577, doi: [10.1109/TENCON.2019.8929271](https://doi.org/10.1109/TENCON.2019.8929271).
- [20] T. Guggenberger, A. Schweizer, and N. Urbach, "Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1074–1085, Nov. 2020, doi: [10.1109/TEM.2020.2978628](https://doi.org/10.1109/TEM.2020.2978628).
- [21] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention," *JMIR Res. Protocols*, vol. 7, no. 9, Sep. 2018, Art. no. e10163, doi: [10.2196/10163](https://doi.org/10.2196/10163).
- [22] F. Jamil, L. Hang, K. Kim, and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electronics*, vol. 8, p. 505, Apr. 2019.
- [23] M. Uddin, "Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *Int. J. Pharmaceutics*, vol. 597, Mar. 2021, Art. no. 120235, doi: [10.1016/j.ijpharm.2021.120235](https://doi.org/10.1016/j.ijpharm.2021.120235).
- [24] K. Abbas, M. Afaq, T. A. Khan, and W.-C. Song, "A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry," *Electronics*, vol. 9, no. 5, p. 852, May 2020.
- [25] F. Fournier and I. Skarbovsky, "Enriching smart contracts with temporal aspects," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, 2019, pp. 126–141.
- [26] M. Hulea, O. Rosu, R. Miron, and A. Astilean, "Pharmaceutical cold chain management: Platform based on a distributed ledger," in *Proc. IEEE Int. Conf. Autom., Qual. Test., Robot. (AQTR)*, Cluj-Napoca, Romania, May 2018, pp. 1–6, doi: [10.1109/AQTR.2018.8402709](https://doi.org/10.1109/AQTR.2018.8402709).
- [27] S. Kim, J. Kim, and D. Kim, "Implementation of a blood cold chain system using blockchain technology," *Appl. Sci.*, vol. 10, no. 9, p. 3330, May 2020.
- [28] J. Zhao, Q. Feng, P. Wu, R. A. Lupu, R. A. Wilke, Q. S. Wells, J. C. Denny, and W.-Q. Wei, "Learning from longitudinal data in electronic health record and genetic data to improve cardiovascular event prediction," *Sci. Rep.*, vol. 9, no. 1, Jan. 2019, Art. no. 717.
- [29] Y. Li, P. Nair, X. H. Lu, Z. Wen, Y. Wang, A. A. K. Dehaghi, Y. Miao, W. Liu, T. Ordog, J. M. Biernacka, E. Ryu, J. E. Olson, M. A. Frye, A. Liu, L. Guo, A. Marelli, Y. Ahuja, J. Davila-Velderrain, and M. Kellis, "Inferring multimodal latent topics from electronic health records," *Nature Commun.*, vol. 11, no. 1, pp. 1–17, May 2020.
- [30] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idrani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, Aug. 2020, Art. no. e13598, doi: [10.2196/13598](https://doi.org/10.2196/13598).
- [31] O. Alamir, R. Raman, A. F. Alhashimi, F. A. Almoaber, and A. H. Alreimeithi, "M-Blocks (Medical Blocks): A blockchain based approach for patient record management using IBM Hyperledger," in *Proc. 6th HCT Inf. Technol. Trends (ITT)*, Ras Al Khaimah, United Arab Emirates, 2019, pp. 24–31, doi: [10.1109/ITT48889.2019.9075088](https://doi.org/10.1109/ITT48889.2019.9075088).
- [32] T. Alshalali, K. M'Bale, and D. Josyula, "Security and privacy of electronic health records sharing using hyperledger fabric," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Las Vegas, NV, USA, Dec. 2018, pp. 760–763, doi: [10.1109/CSCI46756.2018.00152](https://doi.org/10.1109/CSCI46756.2018.00152).
- [33] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Informat.*, vol. 71, pp. 70–81, Jul. 2017.
- [34] N. Kumar S. and M. Dakshayini, "Secure sharing of health data using hyperledger fabric based on blockchain technology," in *Proc. Int. Conf. Mainstreaming Block Chain Implement. (ICOMBI)*, Bengaluru, India, Feb. 2020, pp. 1–5, doi: [10.23919/ICOMBI48604.2020.9203442](https://doi.org/10.23919/ICOMBI48604.2020.9203442).
- [35] J. Kaur, R. Rani, and N. Kalra, "Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records," *Concurrency Comput. Pract. Exper.*, vol. 2021, May 20, Art. no. e6369, doi: [10.1002/cpe.6369](https://doi.org/10.1002/cpe.6369).

- [36] M. Uddin, M. S. Memon, I. Memon, I. Ali, J. Memon, M. Abdelhaq, and R. Alsaqour, "Hyperledger fabric blockchain: Secure and efficient solution for electronic health records," *Comput., Mater. Continua*, vol. 68, no. 2, pp. 2377–2397, 2021, doi: [10.32604/cmc.2021.015354](https://doi.org/10.32604/cmc.2021.015354).
- [37] A. Margheri, M. Masi, A. Miladi, V. Sassone, and J. Rosenzweig, "Decentralised provenance for healthcare data," *Int. J. Med. Informat.*, vol. 141, Sep. 2020, Art. no. 104197, doi: [10.1016/j.ijmedinf.2020.104197](https://doi.org/10.1016/j.ijmedinf.2020.104197).
- [38] D. Tith, J.-S. Lee, H. Suzuki, W. Wijesundara, N. Taira, T. Obi, and N. Ohya, "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthcare Informat. Res.*, vol. 26, pp. 3–12, Jan. 2020.
- [39] V. Thangam and K. Chandrasekaran, "Elliptic curve based proxy re-encryption," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies (ICTCS)*, Udaipur, India, Mar. 2016, pp. 1–6.
- [40] S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient unidirectional proxy re-encryption," in *Progress in Cryptology*, vol. 6055, D. Bernstein and T. Lange, Eds. Berlin, Germany: Springer, 2010, pp. 316–332.
- [41] M. Kumar and S. Chand, "MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic," *J. Netw. Comput. Appl.*, vol. 179, Apr. 2021, Art. no. 102975, doi: [10.1016/j.jnca.2021.102975](https://doi.org/10.1016/j.jnca.2021.102975).
- [42] D. Munoz, D. A. Constantinescu, R. Asenjo, and L. Fuentes, "Clinicap-chain: A low-cost blockchain hyperledger solution for healthcare," in *Blockchain and Applications (Advances in Intelligent Systems and Computing)*, vol. 1010, J. Prieto, A. Das, S. Ferretti, A. Pinto, and J. Corchado, Eds. Cham, Switzerland: Springer, Jun. 2019, pp. 36–44.
- [43] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, Prague, Czech Republic, Aug. 2018, pp. 699–706, doi: [10.1109/DSD.2018.00008](https://doi.org/10.1109/DSD.2018.00008).
- [44] B. Prasad and S. Ramachandram, "Decentralized privacy-preserving framework for health care record-keeping over hyperledger fabric," in *Inventive Communication and Computational Technologies (Lecture Notes in Networks and Systems)*, vol. 145, G. Ranganathan, J. Chen, and F. Rocha, Eds. Singapore: Springer, 2021, pp. 463–475, doi: [10.1007/978-981-15-7345-3_39](https://doi.org/10.1007/978-981-15-7345-3_39).
- [45] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, "Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications," *J. Inf. Secur. Appl.*, vol. 56, Feb. 2021, Art. no. 102673, doi: [10.1016/j.jisa.2020.102673](https://doi.org/10.1016/j.jisa.2020.102673).
- [46] C. Stamatellis, P. Papadopoulos, N. Pitropakis, S. Katsikas, and W. J. and Buchanan, "A privacy-preserving healthcare framework using hyperledger fabric," *Sensors*, vol. 20, p. 6587, Nov. 2020.
- [47] D. K. Meena, R. Dwivedi, and S. Shukla, "Preserving Patient's privacy using proxy re-encryption in permissioned blockchain," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur. (IOTSMS)*, Granada, Spain, Oct. 2019, pp. 450–457, doi: [10.1109/IOTSMS48152.2019.8939226](https://doi.org/10.1109/IOTSMS48152.2019.8939226).
- [48] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *Proc. IEEE Int. Conf. Blockchain*, Atlanta, GA, USA, Jul. 2019, pp. 44–51, doi: [10.1109/Blockchain.2019.00015](https://doi.org/10.1109/Blockchain.2019.00015).
- [49] Hang, Choi, and Kim, "A novel EMR integrity management based on a medical blockchain platform in hospital," *Electronics*, vol. 8, no. 4, p. 467, Apr. 2019, doi: [10.3390/electronics8040467](https://doi.org/10.3390/electronics8040467).
- [50] H. Im, K.-H. Kim, and J.-H. Kim, "Privacy and ledger size analysis for healthcare blockchain," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Barcelona, Spain, Jan. 2020, pp. 825–829, doi: [10.1109/ICOIN48656.2020.9016624](https://doi.org/10.1109/ICOIN48656.2020.9016624).
- [51] Y.-J. Choi and K. Kim, "Secure healthcare data management and sharing platform based on hyperledger fabric," *J. Internet Comput. Services*, vol. 21, no. 1, pp. 95–102, Feb. 2020.
- [52] T. T. Thwin and S. Vasupongayya, "Blockchain based secret-data sharing model for personal health record system," in *Proc. 5th Int. Conf. Adv. Inform., Concept Theory Appl. (ICAICTA)*, Krabi, Thailand, Aug. 2018, pp. 196–201, doi: [10.1109/ICAICTA.2018.8541296](https://doi.org/10.1109/ICAICTA.2018.8541296).
- [53] A. R. Rajput, Q. Li, M. T. Ahvanooy, and I. Masood, "EACMS: Emergency access control management system for personal health record based on blockchain," *IEEE Access*, vol. 7, pp. 84304–84317, 2019, doi: [10.1109/ACCESS.2019.2917976](https://doi.org/10.1109/ACCESS.2019.2917976).
- [54] N. Duong-Trung, H. X. Son, H. T. Le, and T. T. Phan, "On components of a patient-centered healthcare system using smart contract," in *Proc. 4th Int. Conf. Cryptogr., Secur. Privacy*, Nanjing, China, Jan. 2020, pp. 31–35.
- [55] P. Li, S. D. Nelson, B. A. Malin, and Y. Chen, "DMMs: A decentralized blockchain ledger for the management of medication histories," *Blockchain Healthcare Today*, p. 2, Oct. 2019.
- [56] Z. Shahbazi and Y.-C. Byun, "Towards a secure thermal-energy aware routing protocol in wireless body area network based on blockchain technology," *Sensors*, vol. 20, no. 12, p. 3604, Jun. 2020.
- [57] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, p. 2195, Apr. 2020, doi: [10.3390/s20082195](https://doi.org/10.3390/s20082195).
- [58] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application," in *Proc. 10th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Canary Islands, Spain, Jun. 2019, pp. 1–5, doi: [10.1109/NTMS.2019.8763849](https://doi.org/10.1109/NTMS.2019.8763849).
- [59] S. Boucherkha and M. Benmohamed, "A multi-tier architecture to safely share digital medical images," in *Proc. Int. Conf. Dependability Comput. Syst.*, Szklarska Poreba, Poland, May 2006, pp. 319–326, doi: [10.1109/DEPCOS-RELCOMEX.2006.3](https://doi.org/10.1109/DEPCOS-RELCOMEX.2006.3).
- [60] S.-C. Huang, A. Pareek, R. Zamanian, I. Banerjee, and M. P. Lungren, "Multimodal fusion with deep neural networks for leveraging CT imaging and electronic health record: A case-study in pulmonary embolism detection," *Sci. Rep.*, vol. 10, no. 1, Dec. 2020, Art. no. 22147, doi: [10.1038/s41598-020-78888-w](https://doi.org/10.1038/s41598-020-78888-w).
- [61] S.-C. Huang, A. Pareek, S. Seyyedi, I. Banerjee, and M. P. Lungren, "Fusion of medical imaging and electronic health records using deep learning: A systematic review and implementation guidelines," *NPJ Digit. Med.*, vol. 3, no. 1, pp. 1–9, Oct. 2020, doi: [10.1038/s41746-020-00341-z](https://doi.org/10.1038/s41746-020-00341-z).
- [62] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informat. J.*, vol. 25, pp. 1398–1411, Dec. 2019.
- [63] I. Blanquer, V. Hernandez, and F. Mas, "A peer-to-peer environment to share medical images and diagnoses providing context-based searching," in *Proc. 13th Euromicro Conf. Parallel, Distrib. Netw.-Based Process.*, Lugano, Switzerland, 2005, pp. 42–48, doi: [10.1109/EMPDP.2005.7](https://doi.org/10.1109/EMPDP.2005.7).
- [64] T. Mahler, N. Nissim, E. Shalom, I. Goldenberg, G. Hassman, A. Makori, I. Kochav, Y. Elovici, and Y. Shahar, "Know your enemy: Characteristics of cyber-attacks on medical imaging devices," in *Proc. Radiol. Soc. North Amer. (RSNA)*, Jan. 2017, pp. 1–6.
- [65] H. P. Hiriyannaiah and M. Z. J. Shahid, "Dynamic adjustment of image compression for high resolution live medical image sharing," U.S. Patent 14 291 567, Dec. 4, 2014.
- [66] L. Li, C. Chang, J. Bai, H.-D. Le, and C.-C. Chen, "Hamming code strategy for medical image sharing," *Appl. Syst. Innov.*, vol. 3, p. 8, Jan. 2020.
- [67] J. Seo and Y. Cho, "Medical image sharing system using hyperledger fabric blockchain," in *Proc. 22nd Int. Conf. Adv. Commun. Technol. (ICACT)*, Phoenix Park, South Korea, Feb. 2020, pp. 62–64, doi: [10.23919/ICACT48636.2020.9061384](https://doi.org/10.23919/ICACT48636.2020.9061384).
- [68] Y.-B. Cho, "Blockchain based bone-age predication system for sharing medical images," *J. Digit. Contents Soc.*, vol. 20, no. 11, pp. 2177–2182, Nov. 2019.
- [69] P. Upadhyaya, S. Kumar Upadhyay, B. Subedi, B. Subedi, and A. Gaire, "Revolutionizing healthcare systems of a developing country using blockchain," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCC)*, Madurai, India, Dec. 2018, pp. 1–6, doi: [10.1109/ICCC.2018.8782417](https://doi.org/10.1109/ICCC.2018.8782417).
- [70] X. He, S. Alqahtani, and R. Gamble, "Toward privacy-assured health insurance claims," in *Proc. IEEE Int. Conf. Internet Things*, Halifax, NS, Canada, Jul. 2018, pp. 1634–1641, doi: [10.1109/Cybermatics_2018.2018.00273](https://doi.org/10.1109/Cybermatics_2018.2018.00273).
- [71] C. C. Agbo and Q. H. Mahmoud, "Comparison of blockchain frameworks for healthcare applications," *Internet Technol. Lett.*, vol. 2, no. 5, p. e122, Sep. 2019, doi: [10.1002/itl2.122](https://doi.org/10.1002/itl2.122).
- [72] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain with privacy," *J. Med. Syst.*, vol. 43, no. 2, Jan. 2019, doi: [10.1007/s10916-018-1144-x](https://doi.org/10.1007/s10916-018-1144-x).
- [73] R. Kumar and R. Tripathi, "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model," *J. Ambient Intell. Hum. Comput.*, vol. 12, no. 2, pp. 2321–2338, Jul. 2020.
- [74] G. Albanese, J.-P. Calbimonte, M. Schumacher, and D. Calvaresi, "Dynamic consent management for clinical trials via private blockchain technology," *J. Ambient Intell. Hum. Comput.*, vol. 7, pp. 1–18, Feb. 2020.
- [75] L. Liu, Y. Li, S. Li, N. Hu, Y. He, R. Pong, D. Lin, L. Lu, and M. Law, "Comparison of next-generation sequencing systems," *J. Biomed. Biotechnol.*, vol. 2012, pp. 1–11, Jul. 2012, doi: [10.1155/2012/251364](https://doi.org/10.1155/2012/251364).
- [76] M. O. Yahaya, "Review of techniques for gene sequencing, annotation and comparative genomics," *Int. J. Appl.*, vol. 1, pp. 25–28, Jan. 2012.

- [77] K. A. Dill, S. B. Ozkan, M. S. Shell, and T. R. Weikl, "The protein folding problem," *Annu. Rev. Biophys.*, vol. 37, pp. 289–316, Jun. 2008.
- [78] G. M. Crane and J. M. Gardner, "Pathology image-sharing on social media: Recommendations for protecting privacy while motivating education," *AMA J.*, vol. 18, no. 8, pp. 817–825, Aug. 2016.
- [79] B. Erickson, P. Korfiatis, Z. Akkus, and T. Kline, "Machine learning for medical imaging," *RadioGraphics*, vol. 37, no. 2, pp. 505–515, 2017.
- [80] N. Iqbal, F. Jamil, S. Ahmad, and D. Kim, "A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services," *IEEE Access*, vol. 9, pp. 8069–8098, 2021, doi: 10.1109/ACCESS.2021.3049325.



ZHENJIANG TAN received the Ph.D. degree from Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Science. He is currently a Doctoral Supervisor with Jilin Normal University. His research interest includes cyberspace security.



ZEQI LENG is currently pursuing the M.S. degree with Jilin Normal University. Her main research interests include information security and blockchain.



KUNHAO WANG received the Ph.D. degree from Jilin University, China, in 2014. He is currently a Teacher with Jilin Normal University. He is also an Associate Professor. He has published three articles in SCI international journals. His research interests include bioinformation and blockchain.

...