The Application and Implementation of Blockchain Techniques in the Medical Industry

Zihao Jing[a]
Beihang University, Beijing 100191, China

Keywords: Blockchain Technology, Ethereum Smart Contracts, Electronic Medical Records, Electronic Vaccine Passports.

Abstract: To explore the new application ideas that blockchain technology brings to the medical field, this paper analyzes the emergence and development of blockchain technology, paying attention to the gradual maturity of this technology and its application in digital currency, digital identity verification, finance, trade and other scenarios, has received extensive attention. In the medical field, although blockchain technology entered the medical field relatively late, fortunately, blockchain technology may gradually replace HIE, APCD and other medical and health organizations. In the future, it is no longer necessary to run an organization to verify the identity of users. Credibility and veracity of information. Using blockchain technology not only saves costs by eliminating these intermediaries, but also improves data security. This paper will analyze the system design of electronic health records in detail. In particular, the consensus, immutability, and security of data systems will be deeply explored. According to the structural design and research analysis of the vaccine passport, a decentralized electronic vaccine passport application was created, using integrated frameworks and software such as vue and nginx, and combined with the Ethereum public chain to create a multi-terminal instance application platform, which is more vivid. The architectural approach of the system is clearly demonstrated. These results are instructive to guide the application and expansion of blockchain technology in various aspects of the medical field.

1 INTRODUCTION

Since 2008, the blockchain technology represented by Bitcoin has gradually developed into a hot topic in the computer and software industry, making the Internet usher in the era of web 3.0. Decentralization is the core competitiveness of blockchain technology. At the same time, cryptography and timestamp technology are used to encrypt data, and realize decentralized transactions and mutual recognition contracts in a non-trusted system between nodes. It cleverly solves the practical problems of high cost, limited data security, and insufficient stability of trust in centralized organizations and institutions. It has also promoted the rapid development and popularization of blockchain technology. Blockchain technology originated from a Bitcoin-related article published by Satoshi Nakamoto on the cryptography mailing group in 2008 (Yuan, 2016). As a result, the concept of Bitcoin appeared, and blockchain technology entered people's field of vision. Due to the complexity of blockchain technology itself and the rapid development of blockchain applications, there is no specific definition that is uniformly recognized by the industry. It is generally believed that a distributed database system that is decentralized, open, autonomous within the system, and cannot be tampered with is the blockchain.

Table 1: Blockchain Development Stage

Blockchain Phase	Represent	Characterization	Definition
Blockchain 1.0	Bitcoin	Digital currency-focused, no apps	Programmable Money
Blockchain 2.0	Ethereum	Technology has been dramatically developed	Programmable Finance
Blockchain 3.0	EOS	Well-established and mature application	Programmable Society

[a] https://orcid.org/0000-0001-8272-654X

Jing, Z.
The Application and Implementation of Blockchain Techniques in the Medical Industry.
DOI: 10.5220/0012036800003620
In *Proceedings of the 4th International Conference on Economic Management and Model Engineering (ICEMME 2022)*, pages 555-561
ISBN: 978-989-758-636-1

As shown in Table 1, after the origin of the technology, the blockchain has gone through three stages of development, namely the blockchain 1.0, 2.0, and 3.0 sets (Wang, 2021). Blockchain 1.0 is the early stage of accumulation of blockchain technology. Technology has just started to develop. It is mainly devoted to the application of digital currency such as Bitcoin and explores some expansion applications based on digital currency business models. The main feature of Blockchain 2.0 is the emergence of smart contracts. This programmable contract led to the launch of Ethereum, essentially a digital token. Developers can more easily customize their desired applications. The blockchain 3.0 is the stage when many blockchain applications are mature and applied to production and life. Applications using blockchain technology have gradually developed into large-scale commercial applications and penetrated public service fields, e.g., medical care, education.

With the continuous development of blockchain technology, in 2016, there were nearly 800 blockchain-related enterprises worldwide, and the industry scale reached 450 million US dollars (Siyal, 2019). According to a survey report by CIC Consulting in 2021 (Siyal, 2019), blockchain technology is mainly used in the medical field for electronic health cases, DNA wallets, bitcoin payments, and drug anti-counterfeiting. At the same time, due to the continuous improvement of the medical level, data plays an increasingly important role in medical information such as patient identity, past medical history, medical payment records and so on. However, medical data is also a person's privacy. If leaked, attacked, or abused, it will lead to unpredictable consequences. Blockchain technology can play a role here, preventing information leakage while performing information authentication, and guaranteeing the standardized and orderly use of medical information.

For example, electronic medical records based on blockchain technology can realize the access of third-party data users to patient data information under the premise of data security (Siyal, 2019). Besides, they use searchable encryption technology to search nodes on the blockchain, relying on key a certain index of words. Re-encryption technology is also used for secure access to patient data by third-party data users, and the use of asymmetric encryption also ensures the security of patient data and the usability of data users.

This paper is devoted to exploring the cutting-edge application of blockchain technology in the medical field, aiming at the general deficiencies and defects of current ordinary electronic medical records, such as high operating costs, insufficient decentralization, insufficient recognition, and promotion, and proposes efficient improvements. Electronic vaccine passports are a specific application of blockchain technology in the medical field. The current vaccination certification is regionally recognized. That is, consensus can be formed in a small area, but it isn’t easy to popularize and apply in a larger area. Such vaccination records require the existence of a maintenance and operation authority to issue, operate and maintain the vaccination record system. It may bring problems such as high operating costs and poor data security. For traditional electronic vaccination records, this article will give a detailed design scheme for vaccine passports based on blockchain technology. Starting from the needs of practical problems, gradually explore decentralized applications based on blockchain 3.0, give the overall design and architecture of the technology, and strive to create a consensus vaccine passport system.

2 DESCRIPTION OF BLOCKCHAIN AND SMART CONTRACT

2.1 The Motivation of the Paper

The leading technologies applied in this electronic vaccine passport are blockchain and smart contract technologies. The following will introduce some basic concepts and construction principles in the blockchain. Blockchain technology uses distributed nodes to store data and cryptographic encryption technology without requiring an entity authority to realize a decentralized and trustworthy system. Based on proof of work, proof of stake, and DPoS algorithm to form the theoretical basis of consensus. A sketch of the block structure shows in Fig. 1.

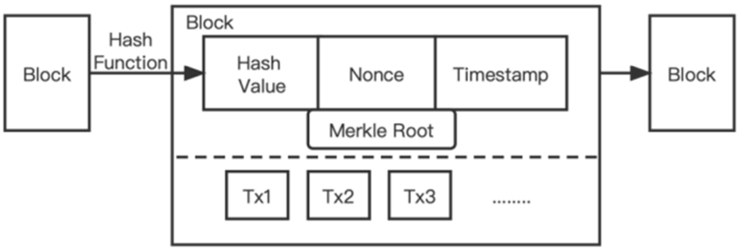

Figure 1: The structure of blocks.

As the name suggests, the main data of the blockchain is in a chain-like structure. A complete block contains a block header and a body, where the block header contains the hash value, random number, timestamp, and Merkle root of the previous block through the hash function. The focus of blockchain is on the use of hashing technology. By continuously taking the hash value of each block, it ensures that the existing blocks are immutable. The body part of the block contains each transaction in the block, and these transactions are formed into a Merkle tree, and the root node of the tree records in the block header. One needs to take the hash value of each block and record it in the next block. In the next block, the hash value and other data are used as parameters, and then the hash value is taken and stored in the third adjacent block. Such a mechanism guarantee that the data in the blockchain cannot be tampered with. If the data in a block in the chain is changed, the hash value calculated from this to be written to the following block will change, thus causing the data in the next block to change triggering a chain effect. After the hash value changes, tampering will be discovered.

Blockchain 2.0 provides users with a programmable system interface, which significantly expands the scope of blockchain applications and dramatically enhances flexibility. The emergence of Ethereum and smart contracts has enabled the realization of distributed applications with more powerful functions and richer application scenarios based on smart contracts. Szabo once proposed that a smart contract is a transaction agreement that can execute contract terms through data calculation (Niu, 2022). A smart contract is a computer protocol that provides personalized writing and deployment (seen in Fig. 2). It is not only widely used in financial business but also distributed computing systems and the Internet of Things.

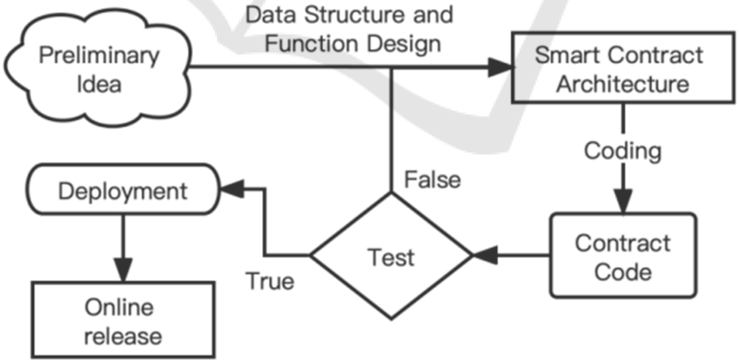

Figure 2: The generation process of smart contracts.

The specific implementation of smart contracts is to convert abstractions such as markets, assets, and behaviors into digital features by abstractly modeling the target object. Then abstractly model the actual logic of the target object, and use a language compatible with smart contracts such as solidity to write script programs. Afterward, the contract is released and deployed on the blockchain, making it a consensus and shared resource of the entire network. Calling the data and functions in the contract needs to be triggered by external events, the code inside the contract is automatically generated and executed. Then the state and data of the objects in the block are changed to control the target object on the chain.

2.2 Critical Technologies of Smart Contracts

The essence of the smart contract is also the idea of using the blockchain to ensure the security of the data by calculating the hash value (Szabo, 1997). Ethereum is a relatively mature platform for smart contracts. It integrates and improves based on a scripting language, cryptocurrencies and related protocols, enabling developers to flexibly design and develop consensus-based, fully functional personalized distributed applications. A typical data structure of the contracts illustrated in Fig. 3.

The operating environment of Ethereum is realized by the Ethereum Virtual Machine EVM, which can provide a Turing-complete scripting language. This mechanism, with accounts as the operation object and the rich interface provision enable anyone to use any tool to create distributed applications with specific functions.

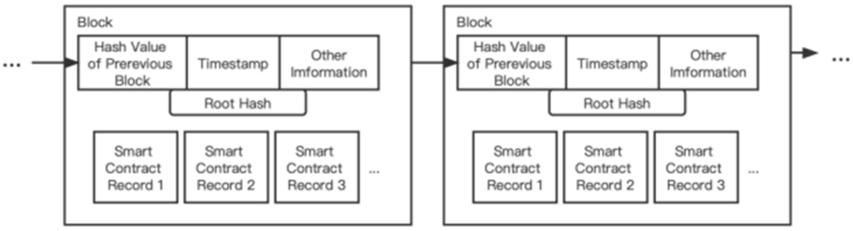

Figure 3. The data structure of smart contracts on the chain.

3 THE APPLICATION OF BLOCKCHAIN IN THE MEDICAL FIELD

The preservation of personal medical-related data is crucial, and it is also the most direct application of blockchain in the medical field. In the traditional medical record recording system, the patient's medical record is recorded in the system of each hospital he sees, which will cause the patient to not be able to master his own medical record information and to have his own accurate medical history. In order to solve the confusion about the medical records of the patients when they seek medical treatment, the use of blockchain technology to save the medical records of the patients can make the owner of the data for patients themselves, which is convenient for the patients to manage and plan their medical health, which has great advantages.

3.1 The Ideological Structure of Electronic Health Medical Records

Presently, the electronic medical record based on blockchain has had preliminary application and established a relatively mature architecture of patient private chain, hospital private chain, and public social chain (Tang, 2021). After the patient visits the hospital, the hospital has the right to write the patient's medical records into the patient's private chain. Through the records in the private chain, patients can have a comprehensive understanding of their medical conditions and medical conditions, and then can view their personal electronic medical records at any time.

Owing to the characteristics of the blockchain technology itself, the written data will not be tampered with and will be stored stably for a long time, with higher authenticity and reliability. This makes medical records more robust evidence, which can play a catalytic or decisive role in resolving medical disputes. Besides, the patient private chain application should have the accuracy of file management. To solve this problem, a unique medical identity identifier of the patient, e.g., a medical identity ID, can be bound by using the patient's identity certificate. Meanwhile, some personal information of the patient should be recorded in the private chain, such as photo, name, gender, bound ID, and other information that can identify the patient. If a hospital needs to access a patient's medical record information, it must be authorized by the patient. Therefore, the patient's personal medical information is in the hands of the patient, and the hospital can view the relevant information only after the patient's authorization. At the same time, after the medical treatment is completed, the patient can close the approval of the hospital to protect the personal information from being abused.

As for hospital private chain, in some medical scenarios, it is necessary for the hospital to store some medical information. These are of great value to improving hospital medical technology or investment in scientific research. Therefore, it is necessary to consider the rational use of medical record data on the premise of maximizing the protection of patients' personal information. Personal private information, including the patient's name, contact information, work situation, etc., will not be written on the blockchain, while necessary information (e.g., medical process, medication, and illness) will be recorded. When it is essential to view the patient's personal information (e.g., crucial medical research results, medical treatment of similar conditions the patient's authorization can be requested to obtain all the information.

In social public chain, medical records may not only need to be circulated between patients and hospitals, but other third-party institutions or government departments also need to access patients' medical records in specific scenarios, such as insurance company claims, government visa issuance, and social medical industry development and scheduling guidance. Therefore, it is necessary to establish a public medical information chain. A public chain system with rich information can improve patients' understanding of medical procedures and medicines while also allowing the medical industry to improve its understanding of the needs of patient groups so that relevant strategies can be adjusted to respond to changes in medical trends.

3.2 Electronic Medical Record Query

The electronic medical record query based on blockchain technology has the advantages of high data security, convenient query, elevated platform portability, and low cost (Xu, 2021). When blockchain technology is used in medical records, the way data is stored will change significantly. Traditional data storage is often local to a single or clustered server, database, or client, and it will be challenging to maintain its security once it receives a network attack or virus intrusion and data tampering occurs. Applying the three-layer blockchain technology discussed earlier can ensure the access rights of personalized customized information while ensuring that the data is not tampered with.

Queries using blockchain technology will be more efficient and convenient (Tang, 2021). Data access does not require the support of a third-party organization, which cannot only reduce cost overhead but also apply to a wider range of terminal applications. The platform and framework of the client do not affect the query and use of data, so that it can be widely used in applications of various platforms. One can send requests to the Ethereum JSON-RPC API via the HTTP protocol to interact with the Ethereum platform.

4 EXAMPLE OF ELECTRONIC VACCINE PASSPORT

To deeply explore the application of blockchain in the medical field, this paper explores and designs the overall architecture of a vaccine passport. Vaccine passport is a potentially massive application of blockchain in the medical field. This section will introduce a feasible design architecture of vaccine passports to show the details of the application of blockchain in vaccine passport in detail, to highlight the promotion and application value of blockchain in the medical field.

4.1 Reason of Design

Vaccination records are currently regulated differently in different regions, which is inconvenient for people traveling across regions (Xue, 2017). A consensus vaccination record book needs to be created. Blockchain has consensus-building mechanisms that use hashes to ensure that the data that has been recorded is not altered, which can ensure that vaccination records that have been written are tamper-proof. Hence, the consensus is formed. To implement the idea, a Dapp was created in which users bind an Ethereum account to the app and bind it with their real passport to ensure that the record of the current account is theirs. The user uses the app account to ask the hospital to add the vaccination record for them when they get vaccinated, and displays the relevant interface of the record information in the app when they need to show the vaccination record.

4.2 DApp Design

The central architecture of the application consists of four modules, which are the Ethereum blockchain, smart contracts, cross-platform application modules, and vaccine passport databases. This system has three main users, patients, administrators, and hospitals. There are different client portals for each user with different functions and permissions. Effectively ensure data security and software stability.

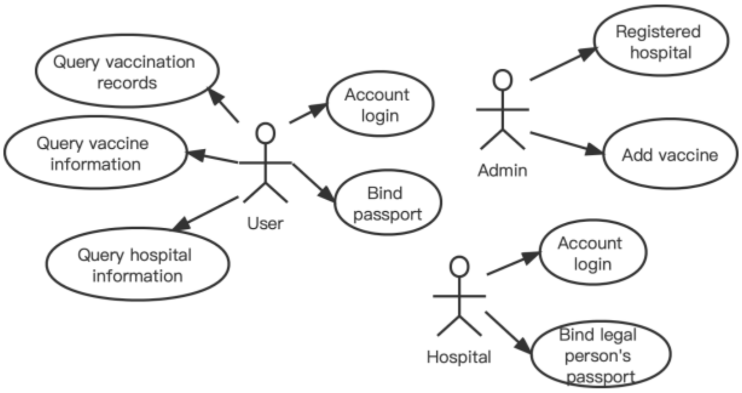
Query vaccination records
Query vaccine information
Query hospital information
User
Account login
Bind passport
Admin
Registered hospital
Add vaccine
Hospital
Account login
Bind legal person's passport

Figure 4: Functional use case diagram.

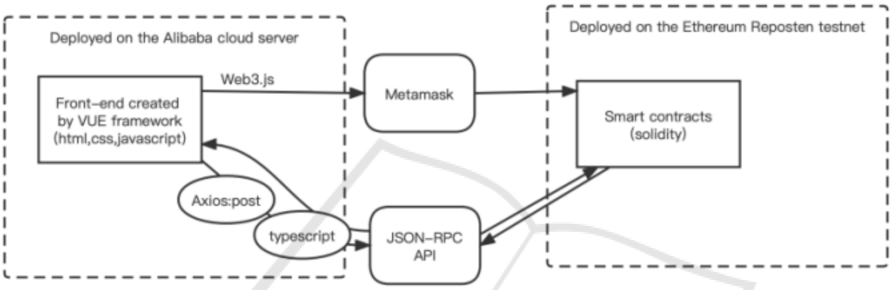
Deployed on the Alibaba cloud server
Web3.js
Front-end created by VUE framework (html,css,javascript)
Axios:post
typescript
Metamask
JSON-RPC API
Deployed on the Ethereum Reposten testnet
Smart contracts (solidity)

Figure 5: Vaccine Passport Technology Stack.

Fig. 4 shows the main working principle of the system, which is a complete application from client to server, with full design and function implementation. The system can use the front-end framework vue3 to create the client, use solidity to create smart contracts, use javascript and typescript to create interactive programs, use Metamask App as a relay to publish transactions, and use Axios to send requests to JSON-RPC API to contact with Ethereum such as sending requests uses interface eth_call to interact with the contract (as exhibited in Fig. 5). The front-end part of the application has been deployed to the relevant cloud server so that one can access and use the application through the URL. The contract part can be deployed to Ethereum's main network using the remix IDE when passes the software tests. The system will likely be favored by WHO and other health organizations as for simplicity and ease of use and high reliability. Once the vaccine information is recorded, it cannot be modified. It will be widely promoted and used to solve the problem of vaccination records in various regions the issue of being recognized by each other.

5 LIMITATIONS & FUTURE WORKS OF BLOCKCHAIN IN MEDICAL

The rapid development of blockchain technology is evident to all. The wave of Web3.0 blockchain technology has gradually become the focus of research and discussion. The application of blockchain in the medical field has attracted wide attention (Zhang, 2019). The electronic medical records and electronic vaccine passports in this article are the preliminary exploration of blockchain technology in the medical field, which can effectively meet the requirements of privacy protection, build data sharing, have consensus, and be widely used in time and region data system (Wang, 2019). However, there is still a long way to go to realize the medical big data system with the whole society and even the whole world, and realize the ultimate goal of smart medical care. In the process of implementation and design, there will still be various problems and challenges. With the further development and iteration of blockchain technology, these problems will be gradually solved. It is hoped that this article can provide help and inspiration for the application of blockchain technology in the medical field in the future.

6 CONCLUSION

In summary, the rapid development of blockchain technology has promoted the application of blockchain technology in all walks of life. With the surging wave of blockchain technology, its application value in the medical system has gradually emerged. It has enormous potential application value in electronic medical records, vaccine passports, DNA wallets, and anti-counterfeiting medicine bottles. The immutable and sharable nature of blockchain determines its potential promotion properties for reaching consensus. The implementation mechanism of smart contracts can also ensure that the ownership of data is straightforward and precise while ensuring the efficient, convenient, and low-cost characteristics of data query. Private chain, multi-layer blockchain structure combined with a public chain to ensure data security and stability. The application of blockchain technology in the medical field will contribute to the construction of a smart medical system, and play an effective role in promoting active health care, epidemic control, medical record recording, and medical data sharing.

REFERENCES

Niu, S., Chen, L., Li, W., et al.: Electronic medical record data sharing scheme based on blockchain. Acta Automatica Sinica, 48(8): 2028−2038 (2022).

Szabo, N.: Formalizing and securing relationships on public networks. First monday (1997).

Siyal, A. A., Junejo, A. Z., Zawish, M., et al.: Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3 (2019).

Tang, Y.: Application of blockchain technology in electronic medical record. Chinese Medical Records 6,1-2+22 (2021).

Wang, J., Wu, Q., Cao, H.: Review of typical applications of blockchain in China. Science, Technology and Economy, 5, 1-6 (2019).

Wang, H., Xu, Q., Zhou, A., et al.: The Development of Blockchain and Its Application in Agriculture. Journal of Agri-cultural Big Data, 03(03):76-86 (2021).

Xu, D., Feng, D., Yan, X., Yu, G.: Autonomous management of electronic medical records based on blockchain. Chinese Journal of Digital Medicine 7,18-23 (2021).

Xue, T., Fu, Q., Wang, C., Wang, X..: A medical data sharing model via blockchain. Acta Automatica Sinica, 43(9): 1555−1562 (2017).

Yuan, Y., Wang, F. Y.: Blockchain: the state of the art and future trends. Acta Automatica Sinica, 42(4), 481-494 (2016).

Zhang, C., Li, Q., Chen, Z., Li, Z., Zhang, Z.: Medical Chain: an alliance blockchain system for healthcare. Acta Automatica Sinica, 2019, 45(8): 1495−1510(2019),