Design and Conception of Will Notarization System Based on Ethereum

Fanglei Liu[1,*,†] and Jianxiang Zhao[2,†]

[1]School of Artificial Intelligence and Big Data, Henan University of Technology, Zhengzhou, China

[2]School of Management and Economy, Chinese University of Hong Kong, Shenzhen, China

*Corresponding author: fanglei_liu@stu.haut.edu.cn

†These authors contribute equally.

Abstract. It is crucial to use blockchain to notarization system. Although a notarized will has the highest legal effect, the notarization process is cumbersome, the notary agency has heavy responsibilities and high costs, which has become a drawback of notarized wills, and which makes many people give up notarized wills. This research will design a will notarization system based on blockchain technology to solve the problem of difficult will notarization. Through demand analysis and scenario analysis, this paper builds the overall architecture of the will notarization system based on blockchain technology and the Ethereum platform. The architecture consists of three parts: the client used by the user, the server provided by the notary office, and the blockchain module. Based on the Truffle framework provided by Ethereum, it will involve multiple links such as HTML front-end development, JavaScript development, solidity smart contract development, Ethereum interface call, network construction, etc., to design the entire system deployment and operation process.

Keywords: Blockchain; Notarization of Wills; Ethereum; Smart Contract.

1. Introduction

With the development of society, people's legal awareness is improved. In order to avoid disputes over property and other issues for children after death, resulting in discord in the family, more and more people pay attention to making a will. A will is a legal act that is created within the scope of the law before one's life, and the personal disposal of his estate or other affairs in the manner prescribed by the law and takes effect when the testator dies [1-3]. According to statistics from relevant departments, more than 60% of wills are deemed invalid by the court in inheritance disputes. The main reason for this is that the testator does not understand the form of the will and the relevant legal requirements, which ultimately leads to the ineffectiveness of the law and the will of the testator cannot be realized.

Wills are generally divided into notarized wills, self-written wills, written wills, and oral wills. Among them, a notarized will is a will established by notarization. It is a form of will with strong evidence and is adopted by the legislation of most countries. *China's Inheritance Law* lists notarized wills as the first of the five forms. In the "Inheritance Law", Article 17, paragraph 1, stipulates: "Notarized wills shall be handled by the testator through a notary office". To handle a notarized will, the testator must personally go to the notary office to dictate or write the will. The notary should seriously examine the authenticity and legality of the will, and after confirming its validity, the notary will issue a " Notarial Will". The notarized will shall be signed by the notary and the testator and affixed with the official seal of the notary office, and made in duplicate, which shall be kept by the notary office and the testator respectively. Changes and revocations of notarized wills are also subject to a notary public. When several wills with conflicting contents in the same inheritance coexist, the notarized will shall prevail [4]. The testator must make the corresponding preparations according to the type of will he made and its corresponding effective conditions, so that the will he made has legal effect. Therefore, a notarized will is a form of will with a strict method, true content, and strong evidence.

For a notarized will, two notaries generally write the will in front of the notary public, sign and seal the will, and indicate the date, date, and date. The will can also be recorded on behalf of a notary

public, and after it is organized into a written will, it is read to the testator. After the testator confirms that it is correct, the two notaries who have the record and the testator sign, indicate the location and date [5].

Notarization of wills is of great significance to ensure the authenticity, legality, and validity of wills, to protect the legitimate rights and interests of testators and heirs, and to maintain normal civil circulation. After the notarized will takes effect, in order to obtain the inheritance right of the inheritance, the heir who has not obtained the inheritance right will often apply for the revocation of the notarized will for various reasons such as the testator's capacity, the illegal content of the will, and the illegal notarization procedure, so as to achieve the purpose of inheriting the inheritance. And the risk of the notary agency increases because of this. Article six of the "*Notarization Law of the People's Republic of China*" stipulates that a notary institution is a certification institution that independently assumes civil liability in accordance with the law. Article twenty-four of the *Detailed Rules for Notarization of Wills* stipulates that if the notary public is at fault, the notary office shall bear the compensation. If the notary will be revoked according to the law, the notary office may face huge amounts of compensation, and the notary office may face huge amounts of compensation. Credibility will also have a negative impact. This requires notaries to fully understand the testator's behavioral capacity, property status, family information, etc. when handling the will notarization, and to strictly follow the procedures for notarization of the will, so as to make the notarized will impeccable and ensure the realization of the true will of the testator, protect the legitimate rights and interests of the heirs, and prevent the practice risks of the notary institutions themselves. At present, the cost of notarization of wills is relatively high, and corresponding costs are required for handling, storage, and determination of validity; flexibility is low, and the formulation, revocation and modification procedures of notarization of wills are also more complicated.

From the above, we can see that although notarization of wills has the highest legal effect, the process of notarization of wills is cumbersome, the notary agency has heavy responsibilities and high costs, which has become the drawback of notarized wills, and many people will give up notarization of wills. The research will design a will notarization system based on blockchain technology to solve the problem of difficult will notarization.

Blockchain is a lot of blocks of data, and the blocks are linked by hash values to form a chain. Blockchain is an innovative application model of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm, and other computer technologies in the Internet era [6]. Most reliable transactions on the Internet need to rely on trusted third parties, that is, a credit-based model. Blockchain technology is based on cryptography. Any two parties who reach an agreement can directly conduct transactions without the intervention of a trusted third party. It can realize a globally synchronized distributed ledger. The ledger records all transactions and has the characteristics of high transparency, non- tampering, and traceability, which effectively improves the security of transactions.

Blockchain is jointly managed by computer clusters distributed around the world and is a trustless, decentralized distributed database running in a non-secure environment. It provides a highly reliable and secure way to verify transactions and was originally used in cryptocurrencies such as Bitcoin. Although various cryptocurrencies are still the most active in the current blockchain application field, however, more and more governments, organizations, experts, and scholars are working to expand blockchain technology from the financial field to other Application scenarios, such as network security, insurance, Internet, medical and health data, and energy applications. Due to its characteristics of decentralization, trustworthiness, and tamper resistance, blockchain technology satisfies people's requirements for the authenticity of evidence and is very suitable for application in the field of wills and notaries that have extremely high requirements for authenticity of data. Notarize information related to will documents using blockchain as a trusted data source.

With the increasing maturity of blockchain applications, the *Regulations of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts*, which has been implemented in China since September 2018, states that electronic Data that can prove its authenticity

through electronic signatures, trusted timestamps, hash value verification, blockchain, and other evidence collection, fixation, and tamper -proof technical means, or notarized by electronic evidence collection and storage platforms. The court should confirm it. This is the first legal confirmation of blockchain and other notarization methods in China in judicial form, marking an important breakthrough in the application of electronic notarization technology at the judicial level, which has aroused great concern from all walks of life. The great attention also provides legal protection for the application of blockchain in the field of wills [7].

2. Analysis Based on Blockchain

2.1 Demand Analysis

The traditional system background is supported by a centralized or distributed database. It is necessary to establish Http and other connections to realize read-write interaction with the database. All data are stored in some fixed databases. However, in this mode, Various faults often occur, such as data leakage caused by attacks, deadlock problems caused by unreasonable data table design, and data integrity problems. User identity information is usually the data with the highest level of security in the database. If there is leakage, it will lead to heavy losses. Therefore, this paper considers putting the will notarization on the blockchain with a higher level of security, so as to realize the full network and full nods of the information. The distributed storage of nodes can ensure the security and integrity of the entire network data even if some nodes are attacked.

The system designed in this paper is to meet the needs of notarization and maintenance of wills, and the bottom layer of the system relies on blockchain technology. This paper will realize the basic functions of registration, login, logout, and modification based on the Truffle framework; coupled with the particularity of blockchain technology, the block record query, and wallet function modules are designed and implemented; considering that the general system has users For the function of authority management, based on user authority, this article designs a notarization module for registered users' will information that is only open to administrators. The overall use case diagram of the system is shown in Figure 1.

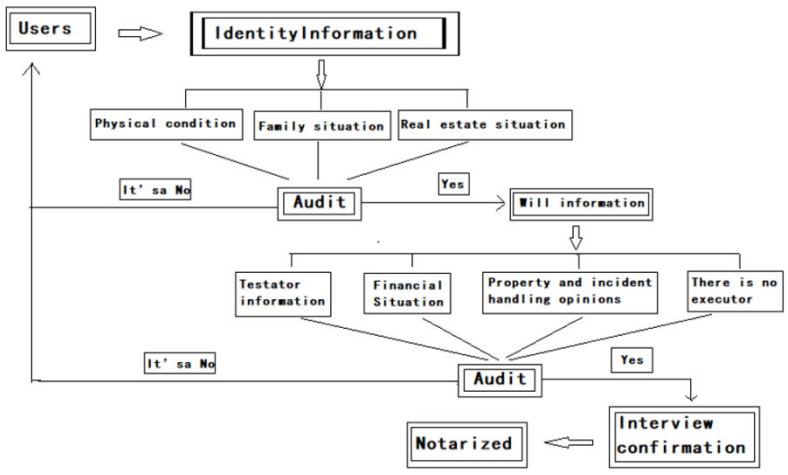

Fig 1. Use Case Diagram of probate notarization system

2.2 Analysis of Applicable Scenarios

Blockchain has the characteristics of security, transparency, traceability, and full backup. Based on these characteristics, we analyze that the will notarization system designed in this paper will be suitable for the following scenarios :

(1) Systems with high-security level requirements: Since the birth of Bitcoin in 2009, the blockchain has not experienced large-scale security incidents. Its security is based on cryptographic

mechanisms such as digital signatures to ensure the integrity of the transmitted information. Sexuality and unforgeability, and cannot be tampered with.

(2) A system with regulatory requirements: the blockchain itself has the characteristics of transparency, traceability, and non-tampering, [8] so it is convenient for institutions with certain authority to supervise the transaction data in the blockchain, so as to save supervision costs.

(3) In demanding systems, blockchain-based systems are decentralized, without a central server, and each node has a complete database backup. Even if one of the nodes is attacked, it will not affect the data of other nodes in the entire blockchain, the integrity of the entire network data is still guaranteed [9].

3. The Overall Design of the Will Notarization System

3.1 The Overall Structure of the Will Notarization System

This paper mainly consists of three parts: the client used by the user, the server provided by the notary office, and the blockchain module. The blockchain module includes a consortium chain composed of multiple notaries and a private IPFS cluster.

3.1.1 Ethereum System Architecture

Ethereum is a smart contract development platform, which provides the basic conditions necessary for contract development, including contract programming language, smart contract script, Ethereum virtual machine (EVM), IPFS file system, Whisper communication system, S Warm information management system, as well as a graphical client and command line interface based on multiple languages, with the help of the Ethereum platform, the development of the decentralized application DApp (Decentralized Application) can be easily carried out.

According to the services and usage processes provided by Ethereum, Ethereum can be roughly divided into three layers as shown in Figure 2.

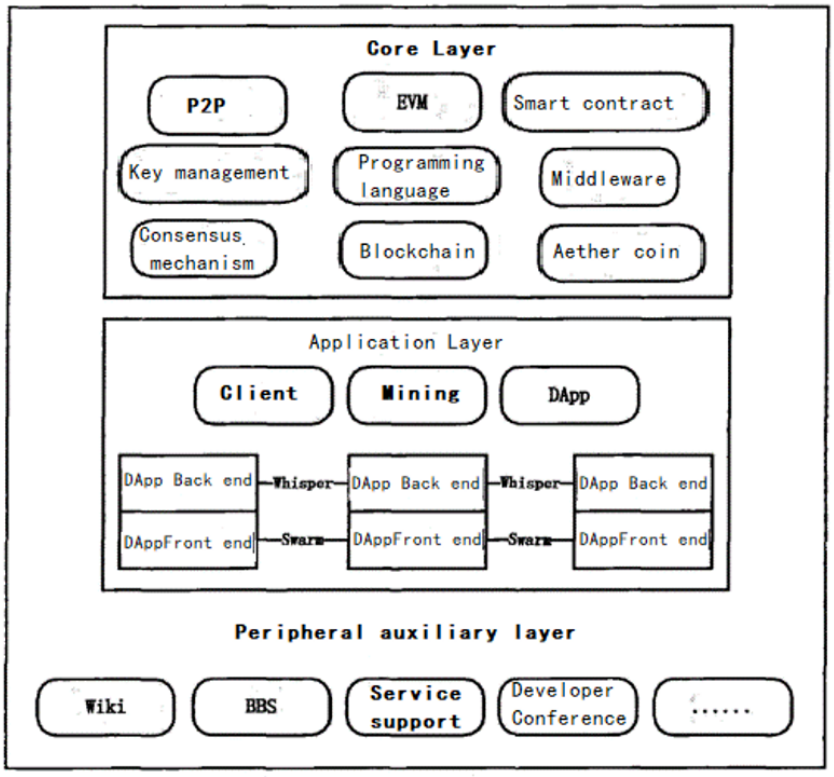

Fig 2. The architecture of Ethereum

(1) Core layer: The core part of Ethereum, including the P2P network, smart contract, EVM , programming language, key management, other middleware, etc .;

(2) Application layer: mainly refers to the applications that can be run based on the Ethereum platform, including other applications such as mining Ethereum, the client with a graphical interface, and DApp;

(3) Peripheral auxiliary layer. Other areas that support the Ethereum platform, include BBS, Wiki, reward mechanism, service support, a blockchain developer conference, etc.

3.1.2 Smart Contracts

Ethereum is the sum of block structure and smart contracts. Due to the existence of smart contracts, the programmability of the blockchain on the Ethereum platform is realized. Any business logic can be realized by writing smart contracts so that it can be implemented on the Ethereum platform.

The term Smart Contract can be traced back to at least 1995, and was proposed by Nick Szabo, a prolific cross-disciplinary legal scholar, who gave the Smart Contract this term in an article on his website. Such a definition [10] called a smart contract is a set of commitments defined in digital form, including agreements on which contract participants can execute these commitments ." Before the advent of blockchain technology, smart contracts have always lacked a suitable operating environment, and therefore not reasonably applied [11-13]. The emergence of blockchain has brought smart contracts back into the public version. Based on blockchain technology, smart contracts have been applied to more practices. At this time, smart contracts are programmable, but they are not just a string of codes. Or a program, itself a role in the blockchain, with its own account address. A smart contract can send and receive messages and values. It is not only a carrier but also a credible intermediary. It has the authority to manage assets and executes corresponding regulations according to the contract content. Figure 3 shows the Ethereum smart contract. As can be seen from the figure, smart contracts run on replicable and shareable ledgers, and provide functions for information processing, sending and receiving messages, and value management.

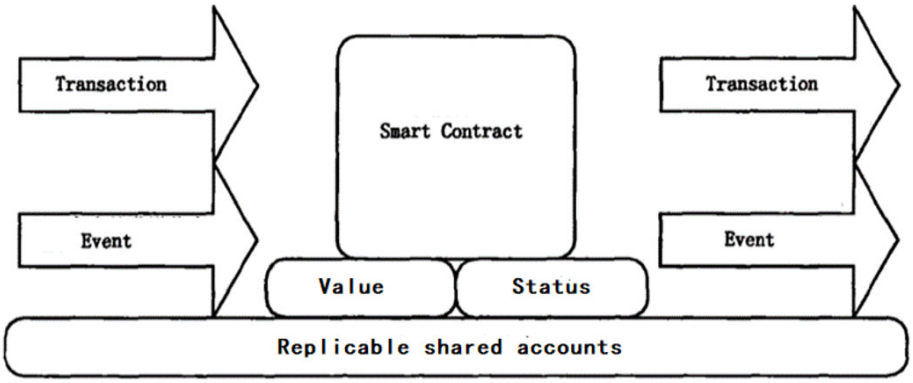

Fig 3. Intelligent contract model

3.1.3 Decentralized Applications

In Ethereum, applications based on smart contracts are called decentralized applications (DApp, Decentralized Application). The core of DApp is smart contracts, and Developers add a user-friendly interface to smart contracts and add other interaction mechanisms to form a DApp. The development of DApp includes Solidity smart contract, HTML interface, js code, and web3 runtime library. Since DApp is a blockchain-based decentralized application, it cannot run on a traditional centralized server but must run on a node of a blockchain network. All transactions initiated by nodes in the entire network will read data on the blockchain network and conduct transactions with smart contracts through the blockchain network, rather than traditional transactions with centralized databases. Besides, all nodes in the chain have a pair of public key and private key represented by Hash value, the public key represents the address of each node, the private key is the password, and all data on the network is stored locally on each node, and the entire network is consistent.

3.2 The architecture of the Will Notary System

The will notarization system designed and implemented in this paper will be developed and implemented on the Ethereum platform. Therefore, based on the above technical analysis, combined with the architecture design of Ethereum, a system architecture diagram suitable for the will notarization system in this paper is planned, as shown in Figure 4.

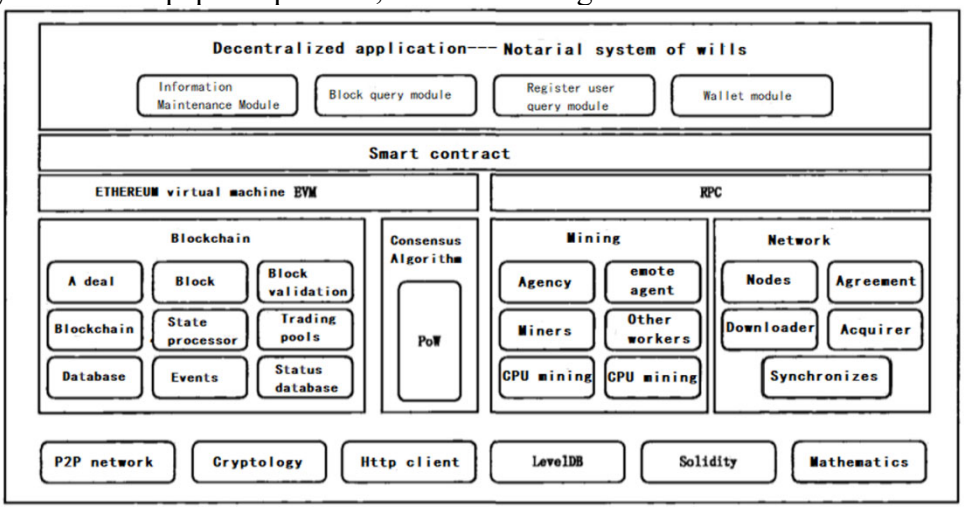

Fig 4. Will notarization system architecture

The will notarization system designed in this paper is usually used among some specific users, not all nodes on Ethereum, so in order to improve efficiency, this paper will choose a private chain. The entire private blockchain system is composed of multiple homogeneous nodes, each node is a complete data node, and each node has a complete backup of the entire blockchain data. The construction of the private chain network in this paper is mainly divided into two steps. The first step is the private chain configuration of a single node to ensure that a single node can normally access the private chain network. The second step is the construction of a multi-node cluster in the private chain. Figure 5 describes the process of building a private chain network.

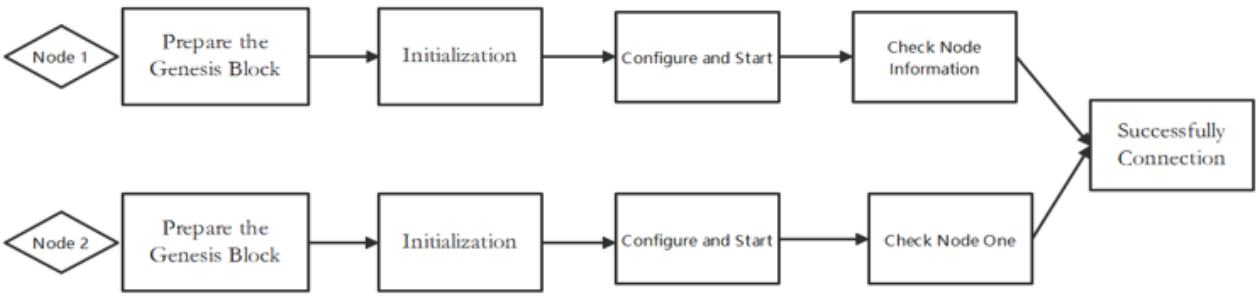

Fig 5. Private Network Construction Process

Private blockchain systems do not need to compete with each other to generate new blocks like public blockchains but conduct consensus voting when new blocks are generated, which avoids a lot of wasted computing power and improves the overall blockchain. The operating efficiency of each block is stored after reaching an agreement.

3.3 Business Functions

The business functions of the will notarization system designed and implemented in this paper mainly include 6 functional modules, including 2 query functions and 4 non-query functions. All non-query functions need to interact with smart contracts. The login function needs to be established on the premise of being registered, and all other functions need to be established on the premise of being logged in. The business processing logic between each function and each function itself is shown in Figure 6.

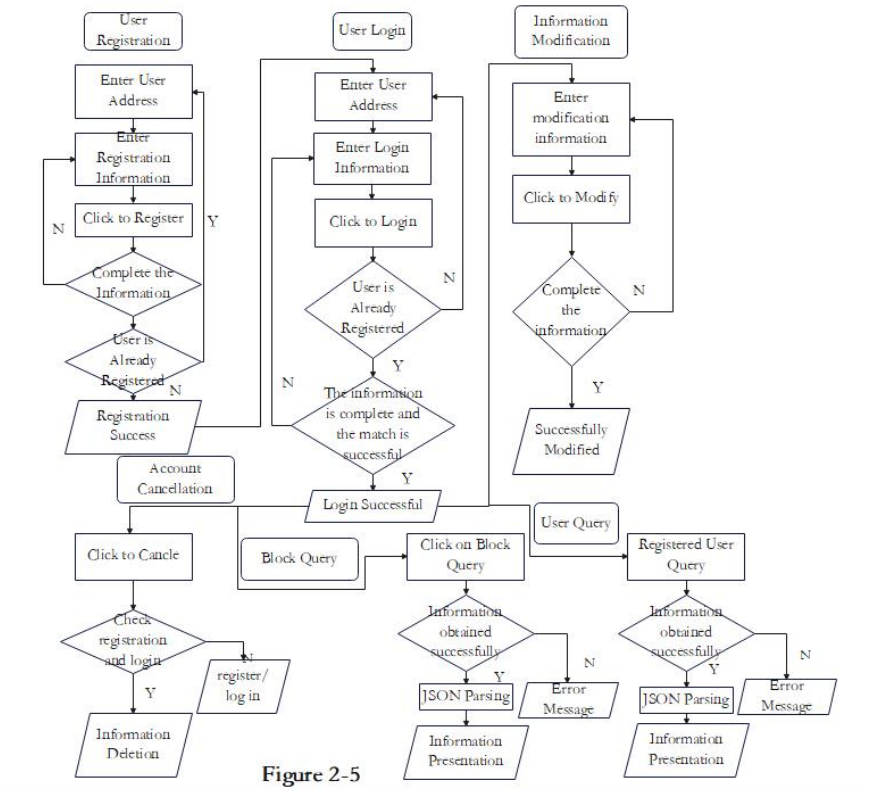

Fig 6. Structure of Construction Process

4. Analysis and Design of Will Notarization System

4.1 System Flow Analysis and Design

The design and implementation of the system in this paper will be based on the Truffle framework provided by Ethereum, which will involve HTML front - end development, JavaScript development , Solidity smart contract development, Ethereum interface calling , network construction, and other links. Figure 7 shows the entire system deployment and operation process, and each process will be explained in detail below.

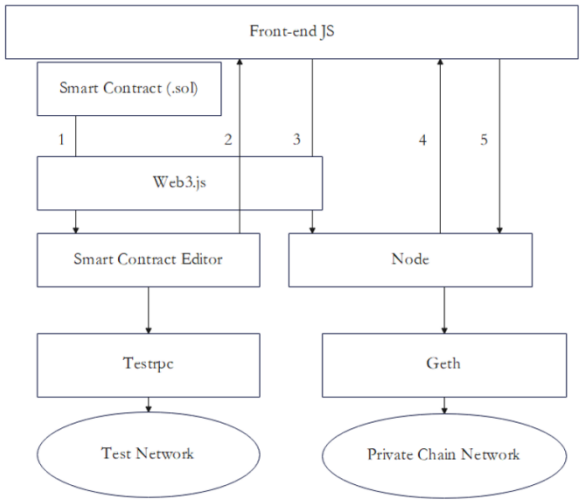

Fig 7. System development and operation process

(1) Use solidity language to write smart contracts (contract files end with .sol), through web3. The interface provided by js is sent to the smart contract compiler to obtain the binary code.

(2) Feedback the binary content of the contract to the front end of the system.

(3) Deploy the compiled smart contract to the network, and obtain the Hash address and ABI (ABI is the binary representation of the contract interface) of the smart contract in the blockchain. Here, for the convenience of development, it will be deployed to the test through testrpc. network.

(4) After the contract is deployed to the blockchain network, the contract address Address and ABI are fed back to the front end.

(5) The front end invokes the smart contract through Address+ABI+nonce to complete the operation of interacting with the contract, where the nonce is the number of transactions, which will be automatically incremented by 1 after each interaction to prevent repeated transactions.

4.2 S Analysis and Design of Will Information Maintenance Module

The so-called will information maintenance refers to the maintenance of other will information including user address, user name, password, user role, etc. The above information will use mapping to form a one-to-one mapping from address to will information to record relevant information. This module implements the basic functions of the entire system. All operations interact with the bottom layer of the blockchain and will generate the corresponding hash value, which is recorded in the blockchain in the form of transactions. The functions implemented by this module include user registration, user login, will information modification, and account cancellation. The specific process is shown in Figure 8.

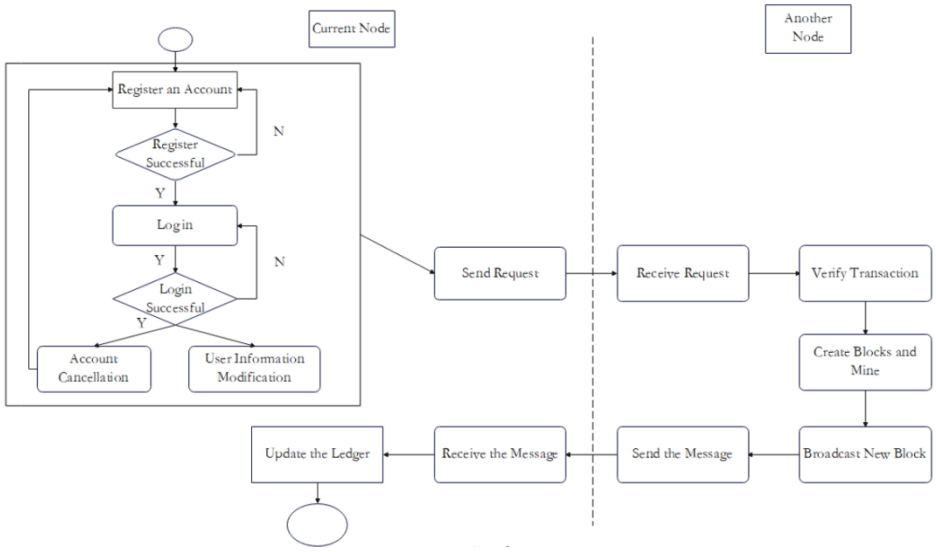

Fig 8. Will Information Maintenance Process

The home page of the system is the login and system information interface. If the current address is registered, you can log in directly. Otherwise, click Register to perform the registration operation. Fill in the fields of username, user address, user role, and password as required, and click Register. If you fill in all the information or do not fill in as required, the smart contract will notify the front end that the registration cannot be done after receiving the registration request. After the registration is successful, you can log in. If the login information is incorrect, you cannot log in normally. After successful login, you will enter the main page of the system, where you can perform account cancellation and user information modification operations. If all the above operations are successful, it will interact with the smart contract, generate a transaction, be verified by the blockchain node, add it to the new block, and continue to mine (because it is based on the PoW mechanism), and then broadcast a new block to all nodes. All block information is updated to ensure the unification of the entire network ledger.

5. Conclusion

This paper proposes and designs a will notarization system based on blockchain technology, aiming at the shortcomings of existing wills that often do not have legal effect, high costs for notarization and wills, cumbersome procedures, tampering and destruction of wills, and difficulties in inspection and verification.

The system comprehensively utilizes blockchain, cryptography, and other technologies combined with the traditional MVC construction platform, providing users with a convenient and safe way to ensure the authenticity and validity of will documents. The specific work of this paper is summarized as follows.

(1) Build an Ethereum development environment, and use the Truffle framework to implement a blockchain-based will notarization system, including user registration, user login, identity information modification, account cancellation, block information query, and registered users The functions of permission query, balance query, transfer and bill query make the whole system does not need to rely on a centralized server, all information will be stored on each node in a distributed form, and all the operations of about interaction are recorded in the block in the form of transaction number, which is convenient for traceability and review.

(2) Build a private chain environment, build a private chain cluster, deploy the developed will notary system to the private chain environment, make the decentralized system run in the designated private chain, and complete each node in the chain communication. By configuring the same genesis block, each node ensures that only specific users can join the private chain and use the system.

(3) Test the usability and security of the decentralized system. In terms of usability tests, not only test the normal operation of the system but also test and verify the function of the system in terms of block records, to ensure that the system can be changed from the traditional one. The centralized database mode is converted into a blockchain-based decentralized mode without affecting its performance. In terms of security testing, by deleting the block data backed up on any node, the security of the entire blockchain network for data backup is tested.

With the increasing maturity of blockchain technology, this paper starts with the shortcomings of the existing will notarization and combines blockchain technology to carry out a preliminary design and conception of will notarization. However, due to time constraints, the design of the system is still There are deficiencies and has room for continuous improvement, and further research and implementation are needed in the future. At the same time, it is necessary to carry out synchronous programming, testing, and verification to find out deficiencies and make changes to make the system more convenient, efficient, and safe.

References

[1] Vitalik Buterin. Ethereum White Paper: A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM. https://ethereum.org/en/whitepaper/. 2013.11

[2] Gavin Wood. ethereum: a secure decentralised generalised transaction ledger berlin version 7251f10. 2022.07

[3] The legal nature and legal effect of printed wills. People's Court News. 2014-10/30

[4] Zou Yu. Dictionary of Law: China University of Political Science and Law Press, December 1991

[5] Detailed Rules for Notarization of Wills , Ministry of Justice Order No. 57 2000-07-01

[6] Zhou Ping , Du Yu , Li Bin , et al . White paper on the development of blockchain technology and application in China . China Blockchain Technology and Industry Development Forum

[7] Provisions of the Supreme People 's Court on Several Issues concerning the Trial of Cases by Internet Courts . Supreme People's Court Network 2018-09-07

[8] Xie Hui , Wang Jian . Research on blockchain technology and its application [J] . Information Network Security , 201 (9) : 192-195 _

[9] Gao Hang, Yu Xuemai , Wang Maolu. Blockchain and New Economy : Digital Currency 2.0 Era [M] . Electronic Industry Press, 2016.

[10] Chen Heqing. Design and implementation of IM IX transmission system based on blockchain D. Nanjing University. 2016.

[11] Zhu Jianming , Fu Y006Fnggui . Supply chain dynamic multi-center collaborative notary based on blockchain [J] . Journal of Network and Information Security , 2016 , 01: 2 7-33 .

[12] Yuan Yong , Wang Feiyue . The current situation and prospect of blockchain technology development [J]. Acta Automata . 2 016, 04:481-494

[13] Zheng Ge. Blockchain and the future rule of law [J]. Eastern Law, 2018 (03) : 75-86