

Received 20 June 2022, accepted 7 July 2022, date of publication 14 July 2022, date of current version 19 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3190963

RESEARCH ARTICLE

Blockchain-Enabled Social Security Services Using Smart Contracts

SONG TANG^{1,2,3}, ZHIQIANG WANG^{1,2,3}, JIA DONG^{1,2}, AND YANDONG MA^{1,2}

¹Institute of Applied Mathematics, Hebei Academy of Sciences, Shijiazhuang 050081, China

²Hebei Authentication Technology Engineering Research Center, Shijiazhuang 050081, China

³Julu Institute of Applied Technology, Xingtai 055250, China

Corresponding author: Zhiqiang Wang (tangsnq@live.cn)

This work was supported in part by the Hebei Provincial Central Leading Local Science and Technology Development Fund Project 216Z0305G.

ABSTRACT With the development of the times, the existing social security system can no longer meet people's needs in terms of providing transparent, distributed sharing, tamper-proof, traceable, consensus trust and trustworthy services. Furthermore, they are centralized and subject to a single point of control and failure. In this context, we propose a consortium blockchain-based solution to establish and improve social security informatization to meet the above challenges. In this article, we present specific business situations for three important social security services. Namely, apply for social insurance, apply for social assistance and social benefits online. Our proposed solution also provides a multi-party trust and data sharing mechanism, and also demonstrates the integration of blockchain and Interplanetary File System (IPFS) storage systems to facilitate the security of approval documents, photos and videos related to the processing of social security services Accessibility and traceability. It also introduces the implementation and testing details of the algorithm in the smart contract, and expounds how to apply it in the automatic approval of social security business to reduce the workload of existing manual review. Finally, by comparing with the existing system, it is discussed that our solution has great advantages in promoting the online processing of social security business, and the safe access and traceability of approval documents, photos and videos.


INDEX TERMS Alliance blockchain, social security services, smart contracts, IPFS.

I. INTRODUCTION

Social security takes the government as the main body, and through the redistribution of national income, provides material assistance to citizens when their life is difficult due to various reasons, so as to ensure the basic life of the system. The essence is the pursuit of fairness. Due to the different national conditions and historical conditions of different countries, the specific content of the social security system is not consistent in different countries and different historical periods. China has a vast territory and is a world-famous country with a large population. Social security services cover four parts: social insurance, social relief, social welfare, and minimum living guarantee. As an important functional department in China [1], social security service institutions belong to the

field of people's livelihood, and have always been valued by the government and are also the most concerned issue of the people [2]. The influence of point failure, the quality of service directly affects the vital interests of the people and the harmony and stability of the country [3]. The main purpose of the new public service theory is to take citizens as the center and realize the needs and common interests of the people [4]. Social security service plays an important role in public management [5], which is the best practice of the new public service theory [6].

At present, the social security service business data is widely distributed, the types of participating institutions are diverse, and the business data interaction network is complex. There is no close connection and information sharing channels between various departments. When handling daily business, it is often necessary to repeatedly register personal information. It causes inconvenience at work and reduces

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

the work efficiency of the social security department. When people handle business, they often need to go to many departments to verify information and handle business one by one. Since each department is independent and has no intersection, it is inevitable that there will be some loopholes. If there is a shared platform between departments, it can be avoided to the greatest extent. Such inconveniences and loopholes arise. In addition, various departments of social security and various insurances are handled separately, resulting in insufficient transparency of business approvals, low efficiency of public services, and risks such as false claims of unemployment benefits and inconsistencies in the participation status of various insurances [7]. In this case, it is particularly important to establish and improve the social security informatization system. In order to achieve business collaboration among various government departments, this paper proposes a solution based on consortium blockchain to overcome the above challenges. Based on the new public service theory [8], explore and promote the application model of smart contracts based on blockchain technology to empower social security services, and under the premise of ensuring information security and building a credible system, promote cross-departmental and cross-border information Hierarchical sharing.

II. RELATED WORKS

A. CURRENT SITUATION OF SOCIAL SECURITY INFORMATION SYSTEM CONSTRUCTION

With the advancement of the informatization of social security services, provincial and prefecture-level social security departments have established data centers, and important breakthroughs have been made in business applications, data resources, public services, and security assurance capacity building. It is developing at the stage of diversification and large-scale application [9]. For the current social security service work, there are still problems such as a wide variety of businesses, intensive service process links, and continuous expansion of information sharing and cooperation scope [10]. There are also problems such as low integration of social security business data and information, limited statistical investigation, insufficient disclosure of statistical data and information, and the huge potential of data for service decision-making, service management, and serving the society has not been developed [11]. Business integration and data security sharing between departments have become urgent needs. At present, social security services do not share data with most institutions [12], and most of them are sensitive information involving personal privacy, requiring clerks to provide certificates and procedures from other regions and departments, which brings great inconvenience to clerks, or the social security service agency will conduct an investigation with other regions and departments by sending a letter, but the cycle is often long [13], and once the data is leaked, it will not only lead to the disclosure of personal privacy, but also may lead to the data being leaked. Criminals use it to cause irreparable losses.

Taking the field of social security as an example, F. Delgado *et al.* studied the international e-government data exchange method [14], using linked data to achieve interoperability to ensure interoperability between social security institutions from different countries, but the system is centralized and lacks an introduction to how to ensure the security of authority authentication. Zheng Yan *et al.* proposed a new decentralized system using blockchain technology to establish a trust evaluation under social networks [15], but there is a lack of research on how to solve data sharing in heterogeneous networks. Gu Jingjing studied the realization of e-government data sharing based on blockchain [7], and proposed that blockchain technology can realize multi-party trust and data sharing mechanism between various government departments, but there is a lack of research on social security government services. Xu Jin [13] proposed to use the decentralization of blockchain technology, non-tampering of records, data encryption, block transparency and openness, machine trust, smart contracts and other characteristics to solve the current social security in Dalian City. Inadequate data sharing among institutions, and low efficiency of business handling. However, no research has been done on how to use the smart contracts and algorithms in the blockchain to realize specific businesses in social security.

To sum up, it can be found that the current social security service information system, the data standards of various business systems are not unified [16], when using traditional means to share data, there are problems such as inconsistent interfaces and cumbersome authority authentication mechanisms, which ultimately lead to incomplete data sharing. implement [17]. In addition, in the process of realizing the informatization of traditional social security government services, manual review is required in the background. The lack of timely approval in the background and the authenticity verification of the proof materials are two major difficulties. However, the application of blockchain and smart contracts can reduce the burden of manual review. According to the pre-set smart contract rules, the business applications on the Internet are reviewed in a timely manner.

Therefore, this paper will choose to use blockchain technology to introduce social security services, give full play to the multi-centralization, distributed sharing, tamper-proof, traceability, consensus trust and other characteristics of blockchain technology, and build a unified and shared social security service data platform. It is of great practical significance to promote the construction of “smart social security services” and explore a new service model of “blockchain + social security services”.

B. BLOCKCHAIN TECHNOLOGY

A blockchain is a distributed storage ledger with a distributed consensus protocol. Blockchain technology uses cryptography and distributed consensus algorithms to achieve trust transfer and security assurance [18]. The main features of blockchain can be summarized as follows.

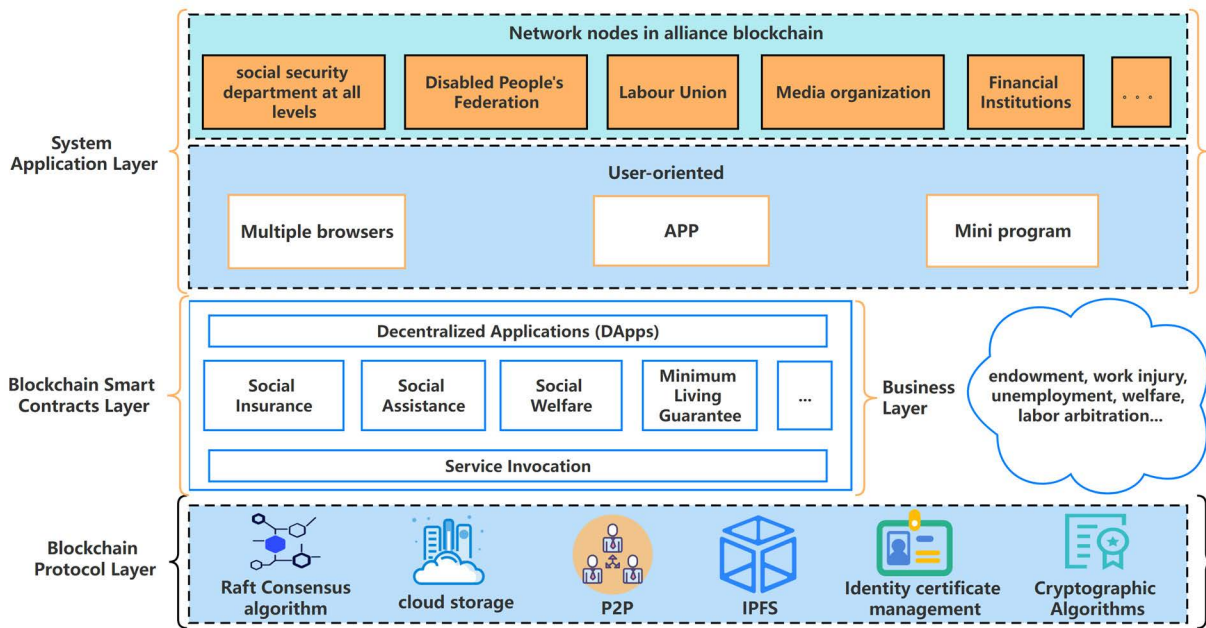


FIGURE 1. Social security service system architecture diagram.

1) DISTRIBUTED DATABASE

Transactions are recorded by multiple nodes, and each node records a complete transaction record. Therefore, each node can participate in monitoring the legitimacy of transactions and verifying the validity of transactions [19].

2) DECENTRALIZED P2P NETWORK

The blockchain network conforms to the peer-to-peer (P2P) P2P network architecture. Decentralization implies that every node in the network is equal and employs P2P communication to avoid a single individual gaining exclusive rights to censor transactions and occupy data resources [20]. The concept of decentralizing the transaction authentication process means that all participating nodes jointly verify the transaction, and the transaction will only be completed when all or a majority of the nodes approve the transaction.

3) SMART CONTRACT

Smart contracts were proposed by Nick Szabo in 1997 [21]. A smart contract is a program code that can be automatically executed in a decentralized blockchain network. It is published, stored, controlled and managed through each node of the blockchain network [22]. Three elements of smart contracts: autonomy, self-sufficiency, and decentralization. Autonomy means that the contract runs automatically once started without any intervention from its originator. Self-sufficiency, smart contracts can be self-sufficient to obtain data resources in the blockchain. Finally, smart contracts are decentralized and run automatically through network nodes without relying on a single centralized server.

C. THE MAIN CONTRIBUTIONS OF THIS PAPER ARE AS FOLLOWS

- We propose a method based on consortium blockchain to achieve data sharing and business collaboration among all participants in social security services in a multi-centralized, distributed sharing, tamper-proof, traceable, and consensus-trusted manner.
- We have developed smart contracts and algorithms for automatic approval of proof materials in social security services, and provide mutual consensus trust solutions by verifying the data of multiple participants at the same time.
- We combine the consortium blockchain Hyperledger Fabric with the decentralized storage of Inter-Planetary File System (IPFS) to overcome storage limitations.
- Our proposed consortium blockchain-based social security service solution is universal and can meet the needs of other government service applications with minimal modification and customization.

III. DESIGN OF SOCIAL SECURITY SERVICE SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

In this section, we describe the system design in detail, as well as the decomposition details of each module of the solution, and show the execution process of smart contracts and algorithms. Figure 1 shows the architecture diagram of the social security service system based on blockchain technology. The whole system adopts a module layered design, which is mainly divided into three layers, namely the system application layer, the smart contract layer and the blockchain

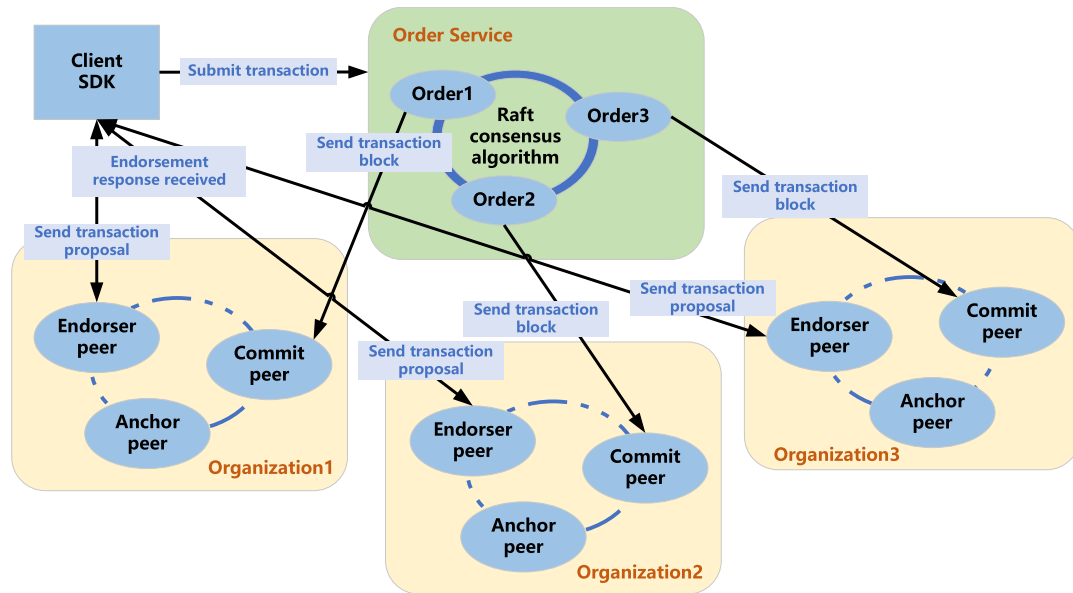


FIGURE 2. The basic structure function flow chart of fabric.

protocol layer. In the system application layer, users can use web browsers, apps or small programs to operate online; in the smart contract layer, we have designed four smart contracts to implement specific business functions of social security services; the blockchain protocol layer provides a method of storing large data and electronic documents of social security business, which is relatively slow to store on the blockchain. The decentralized storage system IPFS assists in storing large-capacity files, uploads and stores the corresponding hashes of the files on the blockchain, and manages, traces and tracks them through the blockchain. The role of each part of the system is also explained in more detail below.

A. SYSTEM PARTICIPANTS

In order to facilitate the social security service process on-chain, as shown in Figure 1. Participants are entities responsible for performing functions in smart contracts. Participants include citizens who are temporarily or permanently incapacitated, as well as citizens whose life is difficult due to various reasons, who can apply for material assistance online. It also includes enterprises and employees who pay social security insurance, but also staff of social security service agencies, managers in charge of auditing participants, which ensures trust and governance.

B. BLOCKCHAIN BASIC SUPPORT PLATFORM

The blockchain basic support platform chooses Hyperledger-Fabric. Hyperledger is an open source project launched by the Linux Foundation in 2015 to promote the cross-industry application of blockchain. A distributed ledger is constructed between each node in the network through P2P communication, and the ledger before the node is completely shared,

transparent and decentralized [23]. Hyperledger Foundation including leaders in finance, banking, IoT, supply chain, manufacturing and technology. Many blockchain projects have originated from this, the most famous of these projects being Fabric.

The blockchain basic support platform can be built by relying on cloud resources, constructed and monitored and managed by social security institutions, and public data will be uploaded to the chain to form an infrastructure for data security, open sharing and social integrity [24]. The Hyperledger used in this study is based on Fabric.

According to the technical characteristics of Fabric, combined with the specific business of social security services, in this blockchain support platform, each participating node or computer is peer-to-peer, and there is no difference in peer-to-peer (P2P) network. There is a central server, so each node can either send requests as a client or process and respond to requests as a server. The nodes in the network are divided into client nodes, peer nodes and order nodes [25]. The basic architecture of Fabric is shown in Figure 2.

In Figure 2, Fabric nodes are divided into client nodes (clients), peer nodes (peers), and ordering nodes (Order). In actual application development, the role of the client node is usually performed by the SDK or the client terminal. It can communicate directly with peer nodes and ordering nodes [26]. The client must connect to the peer node and execute Channel Code to query or update the data on the blockchain chain, and the node storage is responsible for storing the ledger data (such as licenses, certificates, approval documents) etc.) and the corresponding structured data. Querying data on the blockchain will return immediately, but update operations will require complex interactions between client nodes, peer nodes, and order nodes.

Ordering nodes provide a communication channel between client nodes and peer nodes to broadcast messages containing transactions [27]. Peer nodes are responsible for maintaining the data of the entire blockchain, and all peer nodes in the network jointly maintain the same and complete full data. Among them, the Endorser Peer is the peer node responsible for interacting with the client node. Its main function is to endorse the transaction (i.e., simulate execution), and the Commit Peer is responsible for processing the blocks sent by the ordering node. The main function of the peer node for verification is to append the newly formed block to the ledger and synchronize data with other nodes, which jointly ensures that each peer node in the network has the latest blockchain data [28].

The specific execution process for updating the data on the blockchain is as follows:

1. The client node calls the member service for identity authentication and obtains a certificate;
2. The client node calls the Channel Code by connecting to the peer node to generate a proposal response, which contains the proposal for data update;
3. The client node will create a transaction from all the responses, it will send the transaction to the Order node for sorting, the Order node will collect the transactions in the network and package them into blocks, and then distribute these blocks to all peer nodes;
4. The Peer node verifies the transaction in the block sent by the Order node. After the verification is successful, the local blockchain is updated.

C. SMART CONTRACT

We have developed five smart contracts to implement the specific business functions of social security services. The smart contracts are written in Go language. The first smart contract (SC) is the registration SC, which ensures that only authorized participants can communicate on-chain and execute function calls. It has the functions of registering rescuers, paying social insurance employees, and managers of social security service agencies. The control of permissions is completed by mapping the state databases LevelDB and CouchDB on the Peer node. The remaining four smart contracts all inherit the variables and functions of Registration SC. This is because the SC checks that the caller is registered and authorized before making any calls. Enrollment SC can also be used to help assess eligibility for roles such as approvers, applicants. Other smart contracts are used to implement the business processing of social security services (ie, social insurance SC, social relief SC, social welfare SC, minimum living security SC, and their functions and process sequences will be described in detail in the next section.

D. MICROSERVICE ARCHITECTURE DESIGN

The blockchain-based social insurance service management model takes into account business review and user diversity, and needs to support multiple application scenarios and different types of user terminals. Therefore, the Spring

Cloud-based microservice architecture is selected to adapt to subsystems with different functions [29]. This research is based on the single architecture built by Spring Boot. The main advantages of Spring Boot are as follows: First, the configuration is simple, using YAML A Markup Language as the project configuration file, shielding the traditional Spring MVC about XML, JavaConfig and other complex configurations and implementation principles. The second is the convenience of project establishment. It provides a series of POM (POM is the Maven configuration file) to simplify Maven dependencies, and repackages them through Spring Boot, finally realizing an easy-to-deploy and easy-to-maintain distributed system development framework. The third is to run independently. SpringBoot has built-in tomcat, which can run and execute functions independently in a jar package without the assistance and cooperation of other files. The fourth is automatic loading. Spring Boot [30] scans all beans in the path where the startup class is located by default, and automatically configures beans for package/class jars in the project classpath, which greatly simplifies the work.

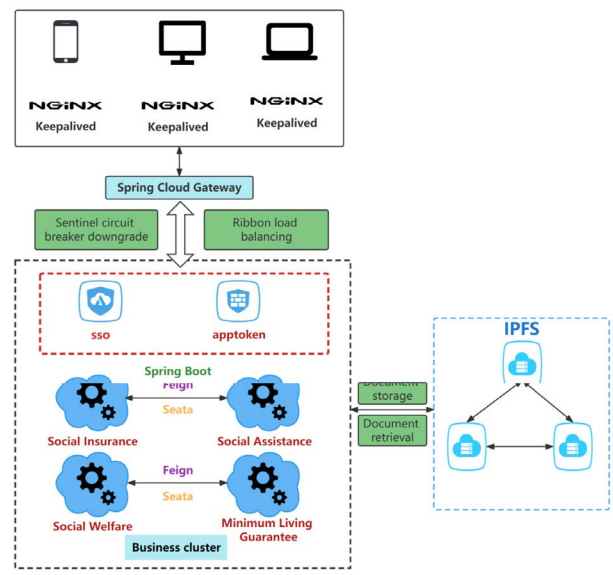


FIGURE 3. Social security service microservice architecture diagram.

There are many users participating in the business of social security services, and the network needs to continuously process a large amount of information and data, which will cause great pressure during peak periods [31]. The model that needs to be built should adapt to this kind of work with high concurrency and rapid response. state, so choose Nginx to build user-side load balancing. Using Spring Cloud Gateway to provide reverse proxy and API routing management functions, Sentinel uses traffic as the entry point to protect the stability of platform services from multiple dimensions such as traffic control, circuit breaker downgrade, and system load protection, and Ribbon provides server-side load balancing. Through SSO(Single Sign On) and APP token, it interacts with the four services of the platform's Social

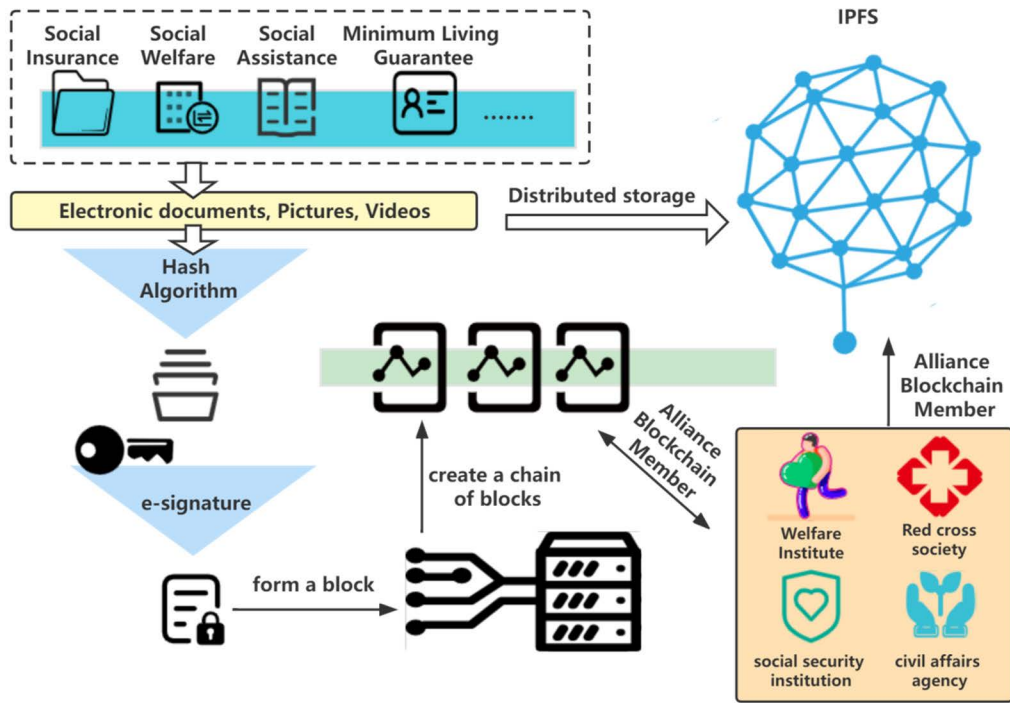


FIGURE 4. Blockchain and IPFS bidirectional storage process.

Insurance, Social Assistance, Social Welfare, Minimum Living Guarantee, which can ensure the security of the model. The social security service microservice structure diagram is shown in Figure 3.

E. OFF-CHAIN STORAGE IPFS

Distributed storage systems like IPFS can store files, images, and videos of large sizes to cope with the storage space constraints of blockchains. In our method, electronic documents, pictures, and videos of the four businesses of Social Insurance, Social Assistance, Social Welfare, and Minimum Living Guarantee are stored off-chain. Users upload documents, pictures, and videos, and the management staff will review them. After approval, the blockchain nodes will automatically sign and seal the reviewed electronic documents using the digital signature algorithm, and then upload them to the IPFS decentralized storage system, as shown in Figure 4. These documents are placed on the IPFS system, and the hashes of these documents are available on the blockchain ledger. Since blockchain technology is immutable, institutions such as Welfare Institute, Red cross society, social security institution, civil affairs agency, etc. in the consortium blockchain can verify the stored information and access it to perform business operations.

F. SEQUENCE OF OPERATIONS

In this subsection, we present the main system operation sequence diagrams in the form of functions and events.

Sequence diagrams also explain the interactions between various stakeholders and smart contracts.

The sequence diagram shown in Figure 5 demonstrates the interaction of Insured, Social insurance agency, and IPFS with smart contracts. The insured is registered on the blockchain through the Registration Smart Contract deployed by the Social insurance agency. After the stakeholder has successfully registered, a unique identification code will be created as a reference for processing social security business. The insured then fills in the information and submits the application through the Social insuranceSmart Contract. Social insurance agency handles applications and conducts background checks. After verification, if the conditions are met, a certificate of participation will be issued. At the same time, the platform informs the insured person of the status of the application in a timely manner in the form of text messages and emails.

Figure 6 illustrates the interaction between rescue applicants, civil affairs departments, neighborhood committees, IPFS, and smart contracts. After the applicant registers, the rescue applicant calls the function ApplicationforAid, and uploads the applicant’s family information, income status, property status and other supporting documents to IPFS. After the review department accepts the request for uploading the application materials, it invites the neighborhood committee to pass the household inspection and authorize the application materials to the stakeholders. The IPFS hash of the file is stored on the blockchain to enable authorized stakeholders to verify the authenticity of the report.

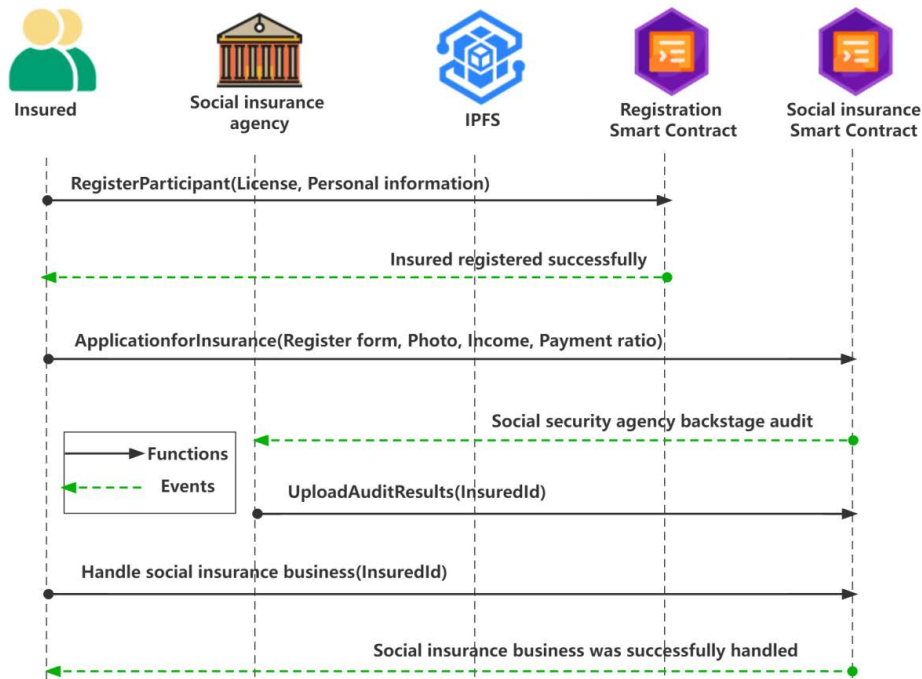


FIGURE 5. Sequence diagram showing the interaction between the insured, the social security institution, IPFS, and the smart contract.

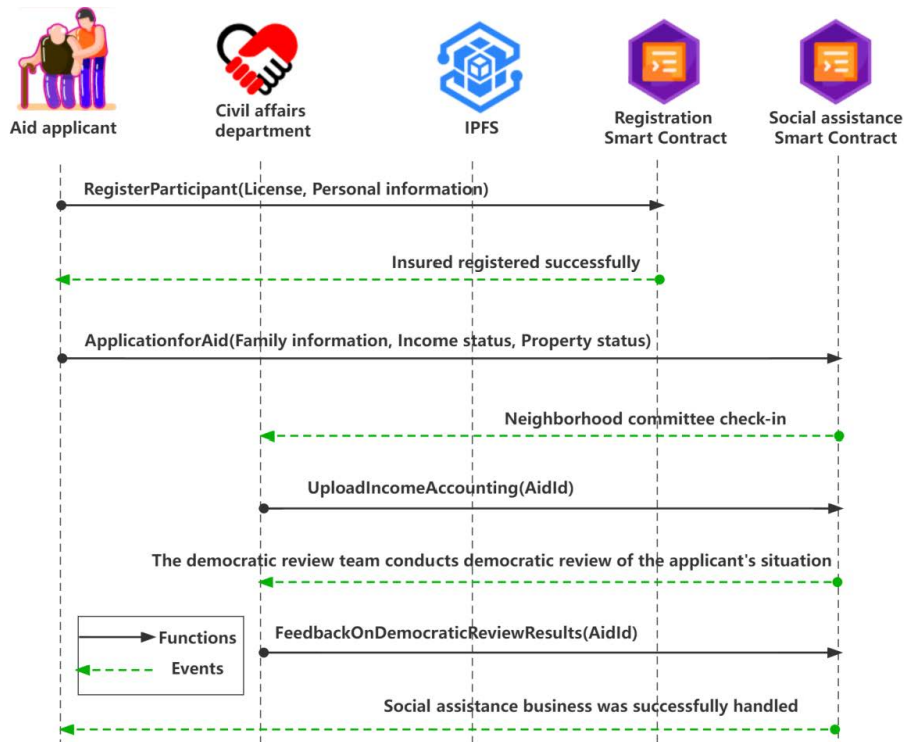


FIGURE 6. Sequence diagram showing the interaction between rescue applicants, civil affairs departments, IPFS, and smart contracts.

According to the information verification and household survey, the sub-district organization accounting team will comprehensively evaluate and calculate the family income

and family property as required, and call the function Upload-Income Accounting to feed back the amount of assistance. The democratic review team conducts democratic review on

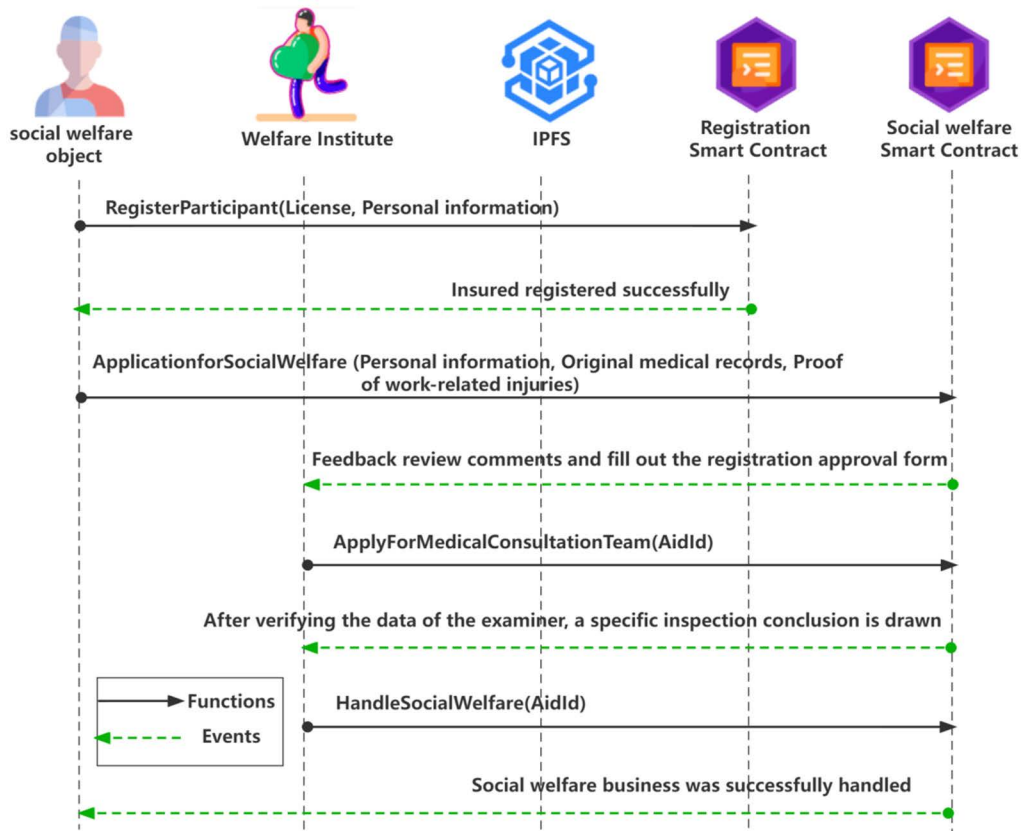


FIGURE 7. Sequence diagram showing interaction between social welfare object, Welfare Institute, IPFS and smart contracts.

the authenticity and integrity of the applicant family’s personnel, family income and property, and calls the function `FeedbackOnDemocraticReviewResults` to complete the notification of the democratic review results.

Social welfare is used to help police officers, military personnel, and ordinary people injured on duty. Figure 7 illustrates the interaction between the social welfare object, the Welfare Institute, the hospital consultation team, IPFS, and smart contracts. After the social welfare object is successfully registered, the function `ApplicationforSocialWelfare` is called, and the personal information, Original medical records, Proof of work-related injuries and other certification documents are uploaded to IPFS. After the review department accepts the request for uploading the application materials, it invites the county-level welfare department to accept and review it, and authorize the application materials to the stakeholders.

After reviewing and meeting the conditions, call the `ApplyForMedicalConsultationTeam` function to form a hospital consultation team, and after verifying the photo and ID card of the examiner, arrange a medical examination and issue a conclusion. After the review is passed, the `HandleSocialWelfare` function can be called for social welfare distribution.

IV. IMPLEMENTATION DETAILS

In this section, we implement a blockchain-enabled social security service solution and explain the details of the algorithm. The smart contract in Fabric is also called Chaincode, which realizes the operation of the ledger data by calling the chaincode, and is the medium for the interaction between the application and the bottom layer. Unlike Ethereum, the Fabric chain code and the underlying ledger are separate. When upgrading the chain code, it is not necessary to migrate the ledger data to the new chain code, which truly realizes the separation of logic and data. Fabric chaincode supports writing in multiple languages, including golang, Java, and node.js. This article uses Go language to create and deploy smart contracts in the VSCode environment, execute them on the Hyperledger fabric platform, and run in the docker virtual machine. Since the blockchain is not suitable for storing large files, in the implementation of our solution, we decided to use the IPFS decentralized storage option, combined with the hash value of the files stored on the chain. Next, we will introduce the implementation details of the three main smart contracts, namely Social Insurance SC, Social Relief SC, and Social Welfare SC, with explanations attached to each algorithm.

A. SOCIAL INSURANCE BUSINESS

Algorithm 1 demonstrates the function of the social insurance smart contract. The person applying for social insurance needs to provide Register form, ID card, Bank card, Photo, Income, Payment ratio as input. The contract will determine whether it is a registered user. If it is a registered user, the next step is to create a social insurance processing request. The social insurance smart contract retrieves the status data stored in couchDb in the fabric platform according to the ID number, and checks whether the social insurance personal information registration form is filled in correctly and whether the ID card is within the validity period. After checking the income and payment coefficient, judge whether the bank card balance is sufficient. After all the above conditions are met, a notification of successful review of the materials will be returned to the staff. The staff informed the deduction precautions, and at the same time delivered an insurance agreement to the insured personnel, and the social insurance business was completed.

Algorithm 1 Social Insurance Business

```

1 InPut: Register form, ID card, Bank card, Photo,
  Income, Payment ratio
2 Output: Status of applying for social insurance
3 if FunctionCaller is not the insured then
4 | Return to unregistered state.
5 end
6 else
7 | If Register form == fill in completely  $\wedge$  Income
  == valid  $\wedge$  ID card == valid  $\wedge$  Bank card ==
  enough balance
8 | then
9 | The social security institution signs a social
  insurance premium withholding business with
  the bank, and deducts the premiums on a
  regular basis according to the salary income
  and payment ratio.
10 | end
11 | else
12 | Approval failed, please carefully check whether
  the submitted information is correct.
13 | end
14 end

```

B. SOCIAL ASSISTANCE APPLICATION AND VERIFICATION

Algorithm 2 demonstrates the function of the social assistance smart contract. Applicants for social assistance need to provide Family information, Income status, Property status, Employment status, and ID card as input. The social relief smart contract will judge whether the function caller is a registered user, and then retrieve the status data stored in couchDb according to the ID number, and check whether the basic information of the applicant is correct. Check whether the family member information is complete and whether

the ID card is within the validity period. Check income status and property situation with reference to employment situation to determine whether relief is needed. After all the above conditions are met, a notification of successful review of materials will be returned to the neighborhood committee. The staff will investigate and verify the relevant certificates and family conditions provided by the applicant, and determine the amount of assistance based on the actual living standards of the individuals or families receiving social assistance.

Algorithm 2 Businesses Applying for Social Assistance

```

1 InPut: Family information, Income status, Property
  status,
  Employment status, ID card
2 Output: Status of applying for social assistance
3 if FunctionCaller is not the Aid applicant then
4 | Return to unregistered state.
5 end
6 else
7 | If Family information == fill in completely  $\wedge$ 
  Income status == need relief  $\wedge$  ID card == valid  $\wedge$ 
  Property status == need relief
8 | then
9 | Meet the conditions for applying for social
  assistance, and notify the neighborhood
  committee to investigate and verify the
  applicant's certificate and family situation.
10 | end
11 | else
12 | Approval failed. Not meeting the conditions for
  applying for social assistance
13 | end
14 end

```

C. SOCIAL WELFARE APPLICATION

Algorithm 3 demonstrates the function of the social welfare smart contract. The applicant for social welfare needs to provide Personal information, Original medical records, Proof of work-related injuries, ID card, Income status as input. The social welfare smart contract will first retrieve the status data stored in couchDb according to the ID number to determine whether the function caller is a registered user. Then proof-read that the personal information filled in by the applicant is complete, whether the original medical record is valid, whether the certificate of injury due to work is valid, whether the ID card is within the validity period, and refer to the income status to determine whether social welfare needs to be issued. After the verification is completed, a notification of the successful review of the materials will be returned to the staff of the Social Welfare and Work Injury Affairs Administration. The staff shall determine the amount of social welfare payment based on the actual income level of the individual.

Algorithm 3 Social Welfare Application Service

```

1 InPut: Personal information, Original medical records,
   Proof of work-related injuries, ID card, Income status
2 Output: Status of applying for social welfare
3 if FunctionCaller is not the Social welfare object then
4   | Return to unregistered state.
5 end
6 else
7   If Personal information == fill in completely  $\wedge$ 
   Original medical records == valid  $\wedge$  ID card ==
   valid  $\wedge$  Proof of work-related injuries == valid
    $\wedge$  Income status == need relief
8   then
9     Satisfy the conditions for applying for social
       welfare, notify the staff of the Social Welfare
       Affairs Bureau of the injury caused by work,
       and issue living allowances.
10  end
11  else
12    If the application materials do not match, the
       materials will be returned or supplemented.
13  end
14 end

```

V. SYSTEM SIMULATION AND EXPERIMENT

Our blockchain-based social security service solution consists of four smart contracts such as Social Insurance SC, Social Assistance SC, Social Welfare SC and Minimum Living Guarantee SC. In this section, the smart contract key functions of the proposed method are tested and verified.

The experimental environment is Intel(R) Core(TM) i7-10510U CPU 1.80GHz, memory 32.0 GB, win10 64-bit operating system, and the test is to use VSCode (version 1.62) and HYPERLEDGER EXPLORER to implement and evaluate the execution of smart contracts. Each function checks the contract state before executing, and only registered users can execute functions based on their roles. Before testing social service smart contracts, users first register in Registration SC. The following subsections show the test results of the smart contract.

To evaluate the functionality of smart contracts, we deployed Social Insurance SC, Social Assistance SC, Social Welfare SC, and Minimum Living Guarantee SC in

0x280504.0dbf9439cf62d954314e249676f1ab215c0d11213abc6b606a23ac374, 0x2.7e63a106249aa491ef68cb10cb0c1040bd08d0c6913859b21e4f8169187b28, 0x2.67b6fbc76125c0cfab33b17da71a85f936774171d7889aaa9ef036b323abb, 0xcd8ea428363ebc3c8dd3eabadc6865909cabef0471368130713ca23db5a703f block address. Figure 8 shows the deployment of smart contracts in the test system.

Transactions and logs for key smart contract functions are shown below, as they are used during testing, the inputs used in the functions do not represent real data, they are only hypotheses for testing purposes. Users store photos and proof

materials in IPFS, and upload the corresponding connection address when calling the smart contract.

A. SOCIAL INSURANCE BUSINESS APPLICATION

After registering in the system, the person applying for social insurance will call the “ApplicationforInsurance” function to provide basic information such as ID card, Income, and Payment ratio. Figure 9 shows that the smart contract retrieves the status data stored in couchDb in the fabric platform according to the ID card, and returns a notification that the audit material is successful when the conditions are met.

B. SOCIAL INSURANCE BUSINESS APPLICATION

After registering in the system, the person applying for social assistance will call the “ApplicationforAid” function to provide basic information such as ID card, Employment status, and Property status. Figure 10 shows the social assistance smart contract. According to the information uploaded by the applicant, after judging that the conditions are met, a notification of successful review of the materials will be returned.

C. SOCIAL WELFARE APPLICATION

Applicants for social welfare upload Original medical records, Proof of work-related injuries to the IPFS storage platform, and then call the “ApplicationforSocialWelfare” function to provide basic personal information such as ID card and Employment status. Figure 11 shows that after the smart contract judges whether the conditions for issuing social benefits are met, it returns a notification that the review materials are successful.

VI. DISCUSS

This section discusses general aspects of the proposed blockchain-based social security service system. Generally, blockchain-based solutions discuss and analyze the costs involved in the implementation and execution of the solution; however, since our solution is built on the Fabric consortium blockchain, there is no Ethereum gas cost, Therefore, there are no fees involved. This section first presents a safety analysis of our proposed approach, and also shows how our solution is general and can be adapted to the needs of specific social security applications. Finally, we compared with existing solutions.

A. SECURITY ANALYSIS

Integrity: The solution based on the Fabric Alliance blockchain provides the tracking of social security service business process application processing. Accessibility of social security related information by recording all transactions on the ledger. Furthermore, trust between participants is achieved through tamper-proof logs. The application, approval and other actions taken by participating entities on the chain are guaranteed to be immutable through consensus algorithms and distributed storage.

Accountability: Accountability is necessary for emerging technologies such as blockchain to help users perform their activities in a safe and trustworthy manner. Every action

Smart Contract	Block Hash	version	Timestamp
Social Insurance SC	280504b0dbf9439cf62d954314e249676f1ab215c0d11213abc6b06a23ac374	1.0	2022-03-29T10:57:31.000Z
Social Assistance SC	2a7e63a106249aa491ef68cb10cb0c1040bd08d0c6913859b21e4f8169187b28	1.0	2022-03-29T10:55:29.000Z
Social Welfare SC	e2f67b6fbc76125c0fab33b17da71a85f936774171d7889aaa9ef036b323abb	1.0	2022-03-29T09:36:16.000Z
Minimum Living Guarantee SC	ced8ea428363ebc3c8dd3eabadc6865909cabef0471368130713ca23db5a703f	1.0	2022-03-29T10:25:01.000Z

FIGURE 8. Smart contract deployment in the test scenario.

Transaction Details
✕

Transaction ID:	063f84584cd718610dcecdc0687e38ca9c160febe5ecea4e21882e3ae1ce9b83
Validation Code:	VALID
Payload Proposal Hash:	75d5b4893b3ea7e542d0edb4c8bc6aa35f72f0a7d42ef47c0c9d740aa73ec5a3
Creator MSP:	Insured
Smart Contract Name:	Social Insurance SC
Type:	ENDORSER_TRANSACTION
Time:	2022-03-29T15:35:11.723Z
InVoke:	[ChainCode cmd] ApplicationforAid -> INFO [{"ID card":"BAG5689213256892126896","name": "Lucy", "gender":"Female","age":38,"Employment Information":"IBC","address":{"street":"1 New Orchard Road Armonk.", "city":"New York","country":"United States"},"links":{"income":"\$2k per month", "Payment ratio":"8%","photo":"http://www.he-ipfs.com/diagraming/623c92eb0791290709585f4a"}]}
Response:	Social insurance business materials are reviewed and approved.

FIGURE 9. Successful implementation of social insurance smart contracts.

on the chain uses identity management using Membership Service Provider MSP [32], which imposes non-repudiation. Each participating entity has a unique private key, and all transactions are signed by the caller’s private key.

Availability: The Fabric Consortium blockchain is known for its decentralization and distributed ledger. All transaction data accessed and recorded by all participants will not be lost even in the event of a node failure, as they are stored on each participant node, this feature ensures the continuous operation of the blockchain in the social security business.

Additionally, confidentiality is critical to ensuring that the solution protects the privacy and medical rights of social

security applicants, so our solution is implemented using a consortium blockchain. In our solution, registration and role authorization are mandatory, because the system will be used in the social security field where applicant information must be kept secret, and only registered and authorized parties can perform function calls. After successfully registering the SC, a public-private key pair will be assigned to associate the identity to ensure it. Also, depending on the private network chosen, information is encrypted when communicating. Other networks rely on channels and group participating entities [33]. Roles and access rights are delegated to an MSP.

Transaction Details	
Transaction ID:	e2f67b6fbc76125c0cfab33b17da71a85f936774171d7889aaa9ef036b323abb
Validation Code:	VALID
Payload Proposal Hash:	ced8ea428363ebc3c8dd3eabadc6865909cabef0471368130713ca23db5a703f
Creator MSP:	Insured
Smart Contract Name:	Social assistance SC
Type:	ENDORSER_TRANSACTION
Time:	2022-03-29T18:35:11.716Z
InVoke:	[ChainCode cmd] ApplicationforAid -> INFO [{"ID card":"BAB565254178921636982","name":"LiLy","gender":"Female","age":55,"Employment status":"Not employed","Family information":{"parents":"Mark,Marry","sons and daughters":"Lucy"},"links":{"income":"\$200 per month","Property status":"Total property \$2000","photo":"http://www.he-ipfs.com/diagraming/4Tf8otBHCL"}}]
Response:	Social assistance business materials are reviewed and approved.

FIGURE 10. Successfully executed social assistance smart contract.

Transaction Details	
Transaction ID:	d36fa6fa3a5ad19df5711ab71aee9eee9b3f374aa0bf75ec9c67372400132a67
Validation Code:	VALID
Payload Proposal Hash:	0bfb3f1ddfc2589f62b25885a5775f2e0c8ffcb2c8e7d8eda57a6cb218d3945
Creator MSP:	Insured
Smart Contract Name:	Social welfare SC
Type:	ENDORSER_TRANSACTION
Time:	2022-03-29T17:21:01.616Z
InVoke:	[ChainCode cmd] ApplicationforSocialWelfare -> INFO [{"ID card":"BAB266132217931320697","name":"Mark","gender":"Male","age":65,"income":"\$200 per month","Employment status":"retired","Proof of work-related injuries":{"Work injury approval unit":"IBC","proof material":"http://www.he-ipfs.com/diagraming/f8otBHCL"},"Original medical records":{"time of injury":"2009-10-11","type of injury":"leg injury","proof material":"http://www.he-ipfs.com/diagraming/623ca50c5653bb072bbc4126"}}]
Response:	Social welfare business materials are reviewed and approved.

FIGURE 11. Successful implementation of social welfare smart contracts.

B. COMPARISON WITH EXISTING SOLUTIONS

Table 1 compares existing social service solutions with ours. [14] is based on non-blockchain technology and studies the

social security field, e-government data exchange methods, using data links to achieve interoperability to ensure interoperability between social security institutions from different

TABLE 1. Comparison with existing solutions.

Study	Topoc Domain	Prototype	Security Analysis	Decentralized	Traceability	Smart Contracts
[14]	E-government data exchange methods in the field of social security	Yes	Yes	No	No	No
[13]	The application of blockchain in social insurance	Yes	No	Yes	Yes	No
[25]	Application of blockchain in social system	Yes	No	Yes	No	No
[26]	Smart contracts with blockchain in the public sector	Yes	Yes	Yes	Yes	No
Our Study	Blockchain-Enabled Social Security Services	Yes	Yes	Yes	Yes	Yes

regions, but the system is centralized and does not guarantee trustworthiness and traceability between different institutions of social security. The solution proposed in [13] is implemented based on consortium blockchain, which explains how to improve the efficiency of data sharing among social security institutions, focusing on data security communication, one of the limitations of this work is that it does not show Testing and coding details of smart contracts. The solution in [34] relies on IoT devices and focuses on researching the combination of IoT and blockchain to establish a multi-participant distributed trust framework with good authenticity, immutability, and traceability. [35] proposed a solution for the public service sector to implement smart contracts to eliminate intermediaries to simplify government service processes and improve public transparency, but it also did not show coding details. Our proposed solution provides three main services for social security business, namely Social Insurance SC, Social Assistance SC, Social Welfare SC. Additionally, it is fully decentralized using IPFS's decentralized storage, and our research shows full smart contract implementation and testing details.

C. GENERALIZE

Our proposed smart contract-enabled social security service solution based on blockchain technology not only facilitates social security applicants, but also contributes to the burden on staff. It is convenient to handle social security business online. At the same time, our proposed solution is also general, and by editing smart contracts, new functions can be added according to business processes, thus adapting to other government services that require approval. In addition, new roles and approval processes can be added. The solution is designed to help users independent of physical location, applicants apply online, and staff approve online. Therefore, our solutions are not limited to the social security business.

VII. CONCLUSION

In this paper, we propose a solution based on Hyperledger Fabric blockchain technology, where smart contracts enable

social security services. Unlike Ethereum, which mainly consumes Gas when executing smart contracts, Hyperledger Fabric's smart contracts run in a docker virtual machine, does not need to consume Gas. The solution we propose can help users apply for social insurance, social welfare, social assistance and minimum living guarantee at home during the epidemic. At the same time, the relevant application processing records are stored on the blockchain platform, and the trust, accountability, integrity, transparency and privacy of the blockchain are ensured by utilizing the features of the blockchain such as trustworthiness, tamper resistance, and distributed sharing. We demonstrate the integration of blockchain and IPFS storage systems to facilitate secure accessibility and traceability of documents, photos, and videos related to the transaction of social security services. Reduce the need to carry paper certificates for approval, solve problems such as the difficulty of staff verification, and the repeated submission of clerks. Our proposed system and its implementation details, as well as smart contracts and their algorithms, are introduced and studied in this article for the social security business processing process, so as to provide more convenience for staff and the public. At the same time, the characteristics of fabric channel isolation and private data are used to ensure effective protection of private data and improve the efficiency of public utility services. At the same time, this research could help provide better social security services for people in rural and remote areas. Compared with other existing technical solutions, our solution has more advantages in terms of reliability, traceability, reliability and convenience.

REFERENCES

- [1] J. Zhou, "Opportunities and challenges of smart human society construction in the era of big data," *Mod. Inf. Technol.*, vol. 3, no. 18, pp. 184–186, 2019.
- [2] F. Zhong, "Research on Xi Jinping's dialectical thinking and its value of the times," M.S. thesis, West China Normal Univ., Nanchong, China, 2021.
- [3] J. H. Xiao, "Strengthening the 'three spirits' and deepening the reform of human resources and society," *Policy*, no. 6, pp. 40–41, 2018.
- [4] X. Xiong, X. H. Yu, and L. Huang, "Logical connotation, evaluation index and realization path of basic public service accessibility," *Reform Strategy*, vol. 37, no. 8, pp. 69–79, 2021.
- [5] C. Xu, "Research on the informatization construction of Municipal People's social system under the background of 'Internet plus,'" M.S. thesis, Shanxi Univ., Taiyuan, China, 2020.
- [6] Z. Liu, "Research on problems and strategies of informatization development of human resources and social security system," M.S. thesis, Heilongjiang Univ., Harbin, China, 2017.
- [7] N. J. Gu, "The valley is quiet research on e-government data sharing design based on blockchain," *Inf. Secur. Commun. Confidentiality*, no. 4, pp. 91–97, 2020.
- [8] J. Q. Zhang, "Research on the problems and countermeasures of social insurance construction of 'smart people's society' in Taiyuan," M.S. thesis, Taiyuan Univ. Technol., Taiyuan, China, 2021.
- [9] Z. Zhang, "Research on the application of blockchain technology in human resources and social security system," *J. Hebei Softw. Vocational Tech. College*, vol. 23, no. 4, pp. 16–19, 2021.
- [10] J. P. Yang, "Research on the informatization construction of the human resources system under the background of 'internet plus,'" *Electron. Technol. Softw. Eng.*, no. 7, pp. 243–244, 2021.
- [11] T. Huang, "Design and implementation of data analysis system of Renshe University," M.S. thesis, Shandong Univ., Jinan, China, 2016.
- [12] H. P. Liang, "Research and practice on staffing data sharing mechanism of organization, organization, finance and human resources and social security," *China's Institutional Reform Manage.*, no. 9, pp. 53–55, 2021.

- [13] J. Xu, "Research on the application of blockchain technology in social insurance management in Dalian," M.S. thesis, Liaoning Normal Univ., Dalian, China, 2021.
- [14] F. Delgado, J. R. Hiler, R. Ruggia, S. Otón, and H. R. Amado-Salvatierra, "Using microdata for international e-government data exchange: The case of social security domain," *J. Inf. Sci.*, vol. 47, no. 3, pp. 306–322, Jun. 2021.
- [15] Y. Zheng, P. Li, F. Wei, and T. Yang, "Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–28, Feb. 2021.
- [16] F. Delgado, J. R. Hiler, and R. Ruggia, "Solutions for electronic exchange of social security information in an international context," *Profesional Inf.*, vol. 21, no. 4, pp. 361–368, 2012.
- [17] R. Navarrete and S. Lujan-Mora, "Use of embedded markup for semantic annotations in e-government and e-education websites," in *Proc. 4th Int. Conf. eDemocracy eGovernment (ICEDEG)*, New York, NY, USA, Apr. 2017, pp. 71–78.
- [18] I. Eyal, "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.
- [19] K. Wust and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Piscataway, NJ, USA, Jun. 2018, pp. 45–54.
- [20] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.
- [21] C.-S. Hsu, S.-F. Tu, and Z.-J. Huang, "Design of an e-voucher system for supporting social welfare using blockchain technology," *Sustainability*, vol. 12, no. 8, p. 3362, Apr. 2020.
- [22] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [23] Y. J. Wu, W.-J. Liu, and C.-H. Yuan, "A mobile-based barrier-free service transportation platform for people with disabilities," *Comput. Hum. Behav.*, vol. 107, Jun. 2020, Art. no. 105776.
- [24] Y. C. Gao, J. Gao, and D. Q. Li, "Application practice of blockchain in the security protection of human resources and social security data assets and sensitive information," *Inf. Netw. Secur.*, vol. 2, pp. 118–121, Jan. 2020.
- [25] Y. Li, "Agricultural product traceability system based on blockchain technology," M.S. thesis, Nanchang Univ., Nanchang, China, 2021.
- [26] X. Xu, M. J. Rothrock, A. Mohan, G. D. Kumar, and A. Mishra, "Using farm management practices to predict *Campylobacter* prevalence in pastured poultry farms," *Poultry Sci.*, vol. 100, no. 6, Jun. 2021, Art. no. 101122.
- [27] H. Hasnah, R. Hariance, and M. Hendri, "Analysis of the implementation of Indonesian sustainable palm oil-ISPO certification at farmer level in west Pasaman regency," *IOP Conf. Ser., Earth Environ. Sci.*, vol. 741, no. 1, May 2021, Art. no. 012072.
- [28] W. Cai, L. Yu, R. Wang, N. Liu, and E. Deng, "Research on application system development method based on blockchain," *J. Softw.*, vol. 28, no. 6, pp. 1474–1487, 2017.
- [29] M. Chen, M. A. G. von Keyserlingk, S. Magliocco, and D. M. Weary, "Employee management and animal care: A comparative ethnography of two large-scale dairy farms in China," *Animals*, vol. 11, no. 5, p. 2357, Apr. 2021.
- [30] L. Montoro-Dasi, A. Villagra, S. Vega, and C. Marin, "Influence of farm management on the dynamics of *Salmonella enterica* serovar infantis shedding and antibiotic resistance during the growing period of broiler chickens," *Vet. Rec.*, vol. 188, no. 10, p. e302, Apr. 2021.
- [31] L. Wu, X. Liu, H. Yang, and X. Ma, "How agricultural management practices affect nitrogen transportation and redistribution under the drying-rewetting process of loessial sloping lands?" *Agricult., Ecosyst. Environ.*, vol. 315, Aug. 2021, Art. no. 107440.
- [32] E. Androulaki, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15.
- [33] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain architectures for physical internet: A vision, features, requirements, and applications," *IEEE Netw.*, vol. 35, no. 2, pp. 174–181, Mar. 2021.
- [34] S. Li, T. Qin, and G. Min, "Blockchain-based digital forensics investigation framework in the Internet of Things and social systems," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1433–1441, Dec. 2019, doi: 10.1109/TCSS.2019.2927431.
- [35] J. A. T. Casallas, J. M. Cueva-Lovelle, and J. I. Rodríguez Molano, "Smart contracts with blockchain in the public sector," *Int. J. Interact. Multimedia Artif. Intell.*, vol. 6, no. 3, p. 63, 2020.



SONG TANG was born in Runan, Henan, China, in 1988. He received the master's degree in chemical engineering inspection machine automation from Jiangnan University, in 2015.

From 2015 to 2021, he was a Software Research and Development Technical Manager and the Project Manager, working at Hebei Huaye Jike Company. During this period, he was responsible for the big data project of drug circulation in Hebei Province. Since 2021, he has been working as a Blockchain Technology Research and Development Engineer and worked with the Institute of Applied Mathematics, Hebei Academy of Sciences. During this period, he was responsible for the research and application of blockchain underlying technology. So far, he has published six academic papers, obtained three software copyrights, and one invention patent.

Prof. Tang is a member of China Computer Federation.



ZHIQIANG WANG was born in Jingmen, Hubei, China, in 1977. He received the B.S. and M.S. degrees from the Shijiazhuang Mechanical Engineering College, Shijiazhuang, in 1999 and 2002, respectively, and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, in 2012.

From 2002 to 2006, he was a Lecturer with the Management Engineering Department, Shijiazhuang Mechanical Engineering College. Since 2012, he has been an Associate Professor with the Institute of Applied Mathematics, Hebei Academy of Sciences. He is the author of more than 20 articles and five inventions. His research interests include operations research, high-performance solution of large-scale optimization problems, machine learning of spatiotemporal data, blockchain, and privacy computing. He is a member of China Computer Federation.



JIA DONG was born in Luancheng, Hebei, China, in 1985. He received the master's degree in power electronics and power transmission from the Taiyuan University of Science and Technology, in 2014.

From 2014 to 2017, he worked as an Assistant Engineer in the second research room of the Institute of Applied Mathematics, Hebei Academy of Sciences. Since 2017, he has been working as an Engineer in the second research room of the Institute of Applied Mathematics, Hebei Academy of Sciences. Since November 2021, he has been working as the Deputy Director of the second Research Office of the Institute of Applied Mathematics, Hebei Academy of Sciences. He has published ten academic papers. His research interests include automatic control, intelligent control, and optimization.

Prof. Dong is a member of China Computer Federation.



YANDONG MA was born in Laiyuan, Hebei, in 1981. He received the bachelor's degree from the Daqing Petroleum Institute, in 2005, and the master's degree from Hebei University, in 2008.

From August 2008 to November 2020, he worked as an Assistant Researcher with the Institute of Applied Mathematics, Hebei Academy of Sciences. Since December 2020, he has been working as an Associate Researcher with the Institute of Applied Mathematics, Hebei Academy of Sciences. He is the author of two EI and five scientific and technological core papers and the holder of two invention patents. His research interest includes machine learning algorithm research and application. He is a member of China Computer Federation.