Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 3707906, 11 pages
https://doi.org/10.1155/2021/3707906

Research Article

A Blockchain-Based Auto Insurance Data Sharing Scheme

Xiaoguang Liu,[1,2,3] **Hengzhou Yang**,[3] **Gaoping Li**,[1,3] **Hao Dong**,[2,3] **and Ziqing Wang**[4]

[1]*School of Mathematics, Southwest Minzu University, Chengdu, Sichuan 610041, China*
[2]*Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, Guangxi 541004, China*
[3]*The Key Laboratory for Computer Systems of State Ethnic Affairs Commission, Southwest Minzu University, Chengdu, Sichuan 610041, China*
[4]*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China*

Correspondence should be addressed to Xiaoguang Liu; dtcr-gg@163.com

Received 30 July 2021; Accepted 9 November 2021; Published 24 November 2021

Academic Editor: Jianhui Lv

Auto electronic insurance policy and electronic maintenance list record the entire process of auto owners purchasing auto insurance and repairs after accident, respectively. They play a vital role in auto owners' applications for claims and insurance company's judgment on whether to settle the claims. However, the privacy of insurance policy and the "information island" resulting from the nonsharing of data between users make the claim has low efficiency. The notable features of blockchain technology are decentralization and tamper-proof, which can well solve data sharing and privacy protection. This paper proposes a blockchain-based auto insurance data sharing scheme to improve the existing auto insurance claim system. The scheme includes four main bodies: auto owner, insurance company, 4S Shop, and government authority. In the proposed scheme, the data sharing of authorized users is realized through proxy reencryption. Finally, we have analyzed the security and performance of the solution. The analysis results show that the proposed scheme can meet many security features such as user access control and data tamper resistance and has an ideal calculation and communication cost.

1. Introduction

With the constant development of society, the auto is everywhere in our life. However, some subjective or objective factors will inevitably cause damage to the auto during the use of the auto. It makes more and more people start to buy insurance for their autos. Now, the auto insurance policy and maintenance list have been digitized with the construction of the smart city. Electronic insurance policy has the advantages of convenient use, low cost, and timeliness and at the same time provides effective evidence for insurance claims. For the time being, these digital documents involve the privacy of auto owners, which shows that privacy protection is a key problem that digital insurance policy must face. The electronic insurance policy and the maintenance list are usually stored and managed by the insurance company and the 4S Shop, respectively. For example, in the process of reviewing claims, the insurance company needs to know the information of insurance purchased by the auto owner and the maintenance case of the auto. The policy information is stored in the insurance company's database, but the insurance company is not clear about the auto's maintenance case. If the insurance company solely relies on the words of the auto owner, it is easy for the auto owner to cheat the insurance and cause losses to the company. Therefore, we propose a scheme based on blockchain to solve the above problem. In the scheme, the insurance company can apply to legally obtain the maintenance records stored in the 4S Shop, and make a quick review to avoid the losses due to the "information island."

1.1. Related Works. Since the advent of blockchain [1], people have never stopped researching it. From the initial application in finance to the present, all walks of life are

advocating the "blockchain+" model [2, 3]. The insurance industry also began to join the "blockchain+" model in 2015 and actively try and explore the application of blockchain technology in its own business. As the third largest application scenario in blockchain applications, insurance is usually combined with other fields, such as the insurance and financial fields, auto insurance and maintenance services, and medical insurance and medical fields [4, 5]. Zhao [4] described the current research and application of the insurance industry to blockchain and predicted the trends of "blockchain+insurance." Popovic et al. [5] summarized and gave the issues to be considered when using blockchain technology to solve insurance business problems. Note that in current various industries, the main research about blockchain focuses on information protection, data application, data storage, data sharing, etc., among which data storage and data sharing are the focuses of research [3, 6, 7]. For example, Ekblaw et al. [8] proposed a decentralized record management system that uses blockchain technology to process EMRs. The immutable feature of the blockchain ensures the accuracy of EMRs. However, the scheme did not set a data access strategy, leading to the risk of data leakage. Guo et al. [9] proposed an attribute-based multiauthority signature scheme, which authorizes multiple institutions to manage user attributes on the blockchain. But this scheme is difficult to resist collusion attacks by authorized agencies. Roehrs et al. [10] used the blockchain to build a patient-centric medical architecture model. Unfortunately, the model only integrates the medical data of different medical institutions into one view. These data are still stored on the blockchain, occupying a large amount of storage space on the blockchain. Given this situation, Hua et al. [11] outsourced and stored the data in the cloud after being encrypted, which not only protects patient privacy but also releases storage space of the blockchain. Fu and Fang [12] did further research based on the OPAL/Enigma encryption platform; in NTT services, better encryption algorithms are used to enforce distributed privacy. The scheme uses a trusted certification mechanism to replace proof of work to improve the consensus algorithm of the system. Liu [13] proposed a medical data sharing and protection scheme based on the hospital's private blockchain to improve the electronic health system of the hospital. Particularly, the proposed scheme is implemented by using PBC and OpenSSL libraries.

1.2. Motivation and Contribution. At present, since the development of blockchain technology itself is not particularly mature, and the application of blockchain in the insurance field has only been proposed with the construction of the smart city in recent years, the research on "blockchain +insurance" is still in its infancy. The existing research in this area has the following shortcomings [4, 5]: (1) The vast majority of studies only discuss whether it is feasible to apply blockchain to the insurance industry and did not give a specific plan. (2) A small number of studies have given specific application schemes such as data sharing, but there are many disadvantages, such as high cost.

The purpose of this article is to design a blockchain-based auto insurance data sharing model. It can be utilized to help the insurance company store and manage policy data, and share the auto maintenance record information so that a rapid claim settlement is realized and effectively reduces the loss of the insurance company. The solution should be able to protect private information and have an ideal calculation and communication cost. The main contributions of this paper are as follows:

(1) A blockchain-based sharing model of lightweight insurance policy data and auto maintenance records is proposed. By using proxy reencryption technology, this model can realize flexible and secure data sharing

(2) The scheme stores the data of the insurance company and the 4S Shop in their database separately and stores the signatures on the blockchain. This can not only improve the security of the scheme but also reduce all kinds of costs

1.3. Organization of This Paper. The rest of this article is structured as follows. First of all, the preliminaries are presented in Section 2. In Section 3, we give a blockchain-based auto insurance data sharing scheme. In Section 4, we analyze the security of the proposed scheme. In Section 5, we analyze the calculation and communication cost of the scheme. Finally, we summarize the proposed scheme in Section 6.

2. Preliminaries

2.1. Blockchain. The blockchain is mainly to solve the security problems and trust problems generated in the transaction process. It is a distributed database according to a chronological list. Generally, blockchain is divided into the public chain, the consortium chain, and the private chain [14, 15]. In the same blockchain system, all data or data characteristic values will be completely stored by each node. The blockchain structure is shown in Figure 1. A blockchain contains many blocks and the hash value of the previous block is connected to the hash value of the next block. In each block, information such as version number, timestamp, digital signature, and root hash value is stored. The main characteristics of blockchain technology are listed as follows [15]:

(1) Decentralization: there is no special node, and the status of each node is equal. All transactions on the same blockchain are completed by all nodes, and any node can access the data and information on the blockchain. The nodes do not affect each other, and the damage to individual nodes will not have any impact on the system

(2) Tamper resistance: modifying the data will result in a change in the hash value, and the current hash value will affect the hash value of the next node, which causes other nodes to make changes. Therefore, once the data information is written into the block, it

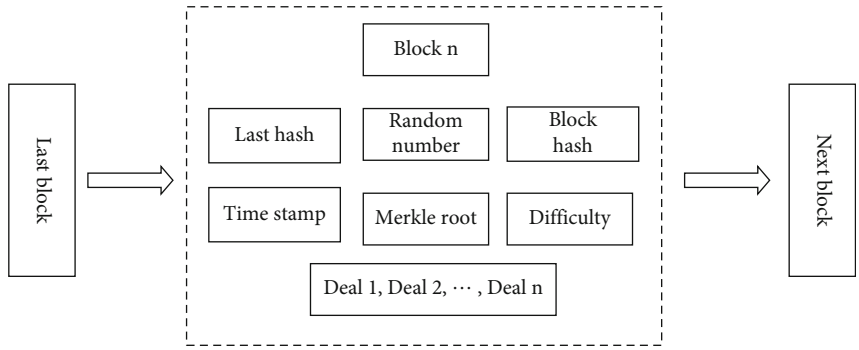

Figure 1: The structure of blockchain.

cannot be changed or canceled unless more than 51% of the nodes are controlled. But in theory, this is very difficult and costly

(3) Openness: in a short period, block transaction information will be copied to all other nodes in the network to realize the synchronization of data in the entire blockchain. Each node can trace the past of both parties to the transaction through its stored information of all transactions

(4) Autonomy: in the system, all nodes can play the role of protector to jointly maintain the entire blockchain system to ensure the reliability and security of information

(5) Anonymity: the identity of each account is encrypted by the algorithm in cryptography. Others can learn the information of this account, but they do not know the identity of the account. Any party on the blockchain will not know any private information of the other party

2.2. General Network Model. As shown in Figure 2, the general network model of the blockchain-based auto insurance data sharing scheme is mainly composed of four parties, which are the system manager, insurance company, 4S Shop, and the user who purchases auto insurance. In the model, the system manager plays a vital role in maintaining the normal operation of the entire network. Therefore, this role is usually played by a highly trusted institution such as government departments. When an auto owner needs to purchase auto insurance from an insurance company registered on the blockchain, he/she must first register with an authority to enter the blockchain. Then, the auto owner buys auto insurance from an insurance company. If the policy information is legal, the insurance company stores the policy information in its database and puts the owner's signature on the blockchain for broadcast reception and verification. If the verification is passed, the signature will be stored on the blockchain. When the auto is damaged, the owner sends the auto to a legal 4S Shop for repairs. If the maintenance record information is legal, the 4S Shop will store the maintenance record information in its database and put the owner's signature on the blockchain for broadcast reception and verification. If the verification is passed, it will be stored on the blockchain. Finally, when the insurance company obtains the permission of the auto owner during the claim review, it can check whether the auto repair is reasonable through the proxy reencryption and quickly make compensation.

2.3. Security Requirements. Under ideal circumstances, the system should meet the following basic requirements [16]:

(1) Security and privacy protection: insurance policy data and auto maintenance information cannot be illegally used by anyone. The system should be able to resist general malicious attacks and be able to track illegal behaviors

(2) Data access: after being authorized, auto owners can view all their data information, and the insurance company can access auto maintenance information under the authorization of the auto owner

(3) User control: the user can manage all his/her historical data, and no one can obtain the historical data without the user's consent

(4) Unified standards: in the model, all participants should use unified data standards and management schemes, which contribute to data sharing and improve system stability

2.4. Consensus Mechanism. A remarkable feature of blockchain technology is that in a decentralized system with decentralized decision-making power and no trust, nodes can reach a consensus on the validity of block data. DPOS is an effective and reliable entrusted proof mechanism [17]. From a certain point of view, it is similar to the board of directors' parliamentary system. All nodes elect 101 representative nodes with equal rights by way of election, and these supernodes will take turns to be responsible for generating a new block. When a node cannot perform its duties, it will lose its accounting rights and be delisted and replaced by a newly elected supernode. The energy consumption of DPOS is lower than that of the POW mechanism, and it is more decentralized than the POS mechanism. It can complete the consensus process faster and improve efficiency.

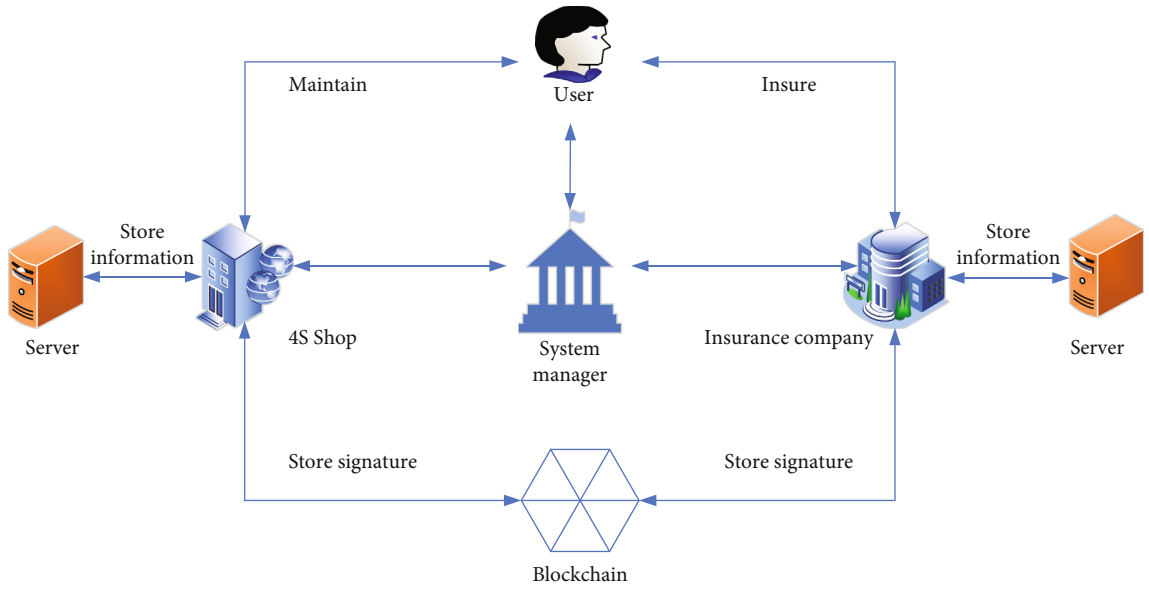

Figure 2: General network model.

2.5. Bilinear Mapping. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic multiplication groups of order p, where p is a prime number. If there is a bilinear mapping e: $\mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ satisfies the following properties, we call e as a bilinear pair [13].

(1) Bilinear: $e(P^a, Q^b) = e(P, Q)^{ab}$, where any $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p^*$

(2) Nondegeneration: there exists $P, Q \in \mathbb{G}_1$, such that $e(P, Q) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$

(3) Computability: for any $P, Q \in \mathbb{G}_1$, $e(P, Q)$ can be calculated in polynomial time

2.6. Proxy Reencryption. Proxy reencryption is an algorithm for reencrypting and decrypting ciphertexts, which was first proposed by Blaze et al. [18] in 1998. In some schemes, a part A entrusts a trusted third party or a semihonest proxy to convert the ciphertext encrypted with its public key into the ciphertext encrypted with the public key of the other party B. Then, B can use the private key to decrypt the ciphertext, that is, to realize data sharing. In the whole process, the encrypted data is very safe, and there is no need to disclose A's private key. The specific steps are as follows [19]:

(1) A uses its public key to encrypt the plaintext m; that is, $C_A = E_A(m)$, where m is the file that A wants to send to B, and E is an asymmetric encryption algorithm

(2) B sends the request to A, and then, A (or proxy) generates a conversion key $PK_{A \longrightarrow B}$

(3) A sends C_A and $PK_{A \longrightarrow B}$ to the intermediate proxy

(4) The intermediate proxy converts the ciphertext C_A to C_B through $PK_{A \longrightarrow B}$. At this time, C_B is the ciphertext obtained by encrypting the plaintext m with B's public key. It is worth noting that in this step, the proxy only provides conversion service and cannot obtain plain text

(5) The proxy sends the ciphertext C_B to B

(6) B decrypts C_B with its private key to obtain the plain text m

3. Proposed Auto Insurance Data Sharing Scheme

In this section, we will propose an auto insurance claim scheme based on the alliance blockchain of the insurance company, 4S Shop, policyholder, and the system manager. The property proxy reencryption scheme in [20] is utilized. It has provided a data sharing mechanism for the member of this blockchain. The notations used in this paper are given in Table 1.

As shown in Figure 3, the system manager SM, the insurance company IS_i, the 4S Shop $4S_j$, and the policyholder $PH_{i;j;n}$ are the four main kinds of participants in the network. SM is the management institution that is a trusted third party and responsible for verifying node identity, generating the master key and system parameters, and verifying the signature of data. Insurance company IS_i and 4S Shop $4S_j$ first register with SM. If a person $PH_{i;j;n}$ insures for his/her auto with an insurance company, he/she must register with SM and set his/her public key and private key. If SM's verification has successfully passed, the policy information of $PH_{i;j;n}$ will be stored in the server, and the signatures of $PH_{i;j;n}$ and IS_i will be stored on the blockchain. When the policyholder's auto has an accident, $PH_{i;j;n}$ contacts IS_i to identify the auto and then IS_i checks policy information. If the requirements are met, then it can quickly enter the claim process. IS_i and

Table 1: Notations.

Notations	Description
SM	System manager/government
IS_i	ith insurance company
$4S_j$	jth 4S Shop
$PH_{i;j;n}$	nth policyholder
$\mathbb{G}_1$; $\mathbb{G}_2$	Cyclic groups
g	A generator of the group $\mathbb{G}_1$
k ; l ; l_1	Security parameters
p	Large prime number
$\|\|$	String concatenation
$H_{(.)}$	Hash function
$ID_{(.)}$	Identity
F	Random function
$E_{(.)}$	Encryption
$D_{(.)}$	Decryption
$PK_{(.)}$	Public key
$SK_{(.)}$	Private key
$PID_{(.)}$	Pseudo-identity

$PH_{i;j;n}$ first decide which $4S_j$ to repair the auto. Then, $4S_j$ repairs the auto and generates maintenance information. Particularly, the maintenance information of $4S_j$ about $PH_{i;j;n}$ will be stored in $4S_j$'s server, and the signatures of $PH_{i;j;n}$ and $4S_j$ will be stored on the blockchain. If other 4S Shop $4S'_j$ or insurance company IS'_i on this alliance blockchain wants to query the maintenance record information or policy information of $PH_{i;j;n}$, they should apply to the SM. If the application is approved, an agent first computes the conversion key. Then, SM generates the ciphertext of the maintenance records or policy information reencrypted by the $4S'_j$'s public key or IS'_i's public key and sends the ciphertext to $4S'_j$ or IS'_i. In the following, we will give a detailed introduction of the proposed scheme, which includes six phases, i.e., initialization of system phase, insurance company join phase, 4S Shop join phase, policyholder join phase, signature store phase, and data sharing and search phase.

3.1. Initialization of System Phase

(1) Firstly, SM inputs a security parameter 1^k and selects the bilinear map e and two multiplicative groups $\mathbb{G}_1$ and $\mathbb{G}_2$, which have the same prime order p, and g is a generator of $\mathbb{G}_1$. Secondly, SM chooses three secure hash functions $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_2 \longrightarrow \{0,1\}^k$, and $H_3 : \mathbb{G}_1 \times \{0,1\}^k \times \{0,1\}^l \longrightarrow \mathbb{Z}_p^*$ and a random function $F : \mathbb{G}_1 \times \mathbb{G}_2 \times \{0,1\}^k \longrightarrow \{0,1\}^{l-l_1} \| \{0,1\}^{l_1}$, where l and l_1 are both security parameters. Lastly, SM randomly picks $x \in \mathbb{Z}_p^*$ as the system master key, sets the pubic key $Y = g^x$, selects random elements $g_1, g_2, u, v, d \in \mathbb{G}_1$, and publishes $\{p, e, g, g_1, g_2, u, v, d, Y, H_1, H_2, H_3, F, l, l_1, \mathbb{G}_1, \mathbb{G}_2\}$

(2) The insurance company IS_i randomly picks $x_i \in \mathbb{Z}_p^*$ as its private key and computes public key $PK_i = g^{x_i}$

(3) The 4S Shop $4S_j$ randomly selects $x_j \in \mathbb{Z}_p^*$ as its private key, and the public key is set as $PK_j = g^{x_j}$

(4) The policyholder $PH_{i;j;n}$ randomly chooses $x_n \in \mathbb{Z}_p^*$ as his/her private key and computes the public key $PK_{i;j;n} = g^{x_n}$

3.2. Insurance Company Join Phase.

When a new insurance company decides to join the alliance blockchain, it needs to follow those steps combining with SM.

(1) IS_i sends its identity ID_i to SM

(2) SM verifies its identity; if passes, SM randomly selects $\lambda_i \in \mathbb{Z}_p^*$ and computes $PID_i = E_{SM}(ID_i \oplus \lambda_i) \| \lambda_i$ as IS_i's pseudo-identity

(3) IS_i receives PID_i from SM through a secure channel

3.3. 4S Shop Join Phase.

If a new 4S Shop $4S_j$ wants to join the alliance blockchain, it must carry out the following steps combining with SM.

(1) $4S_j$ sends its identity ID_j to SM

(2) SM verifies its identity; if passes, SM randomly selects $\lambda_j \in \mathbb{Z}_p^*$ and computes $PID_j = E_{SM}(ID_j \oplus \lambda_j \| \lambda_j)$ as $4S_j$'s pseudo-identity

(3) $4S_j$ receives PID_j from SM through a secure channel

3.4. Policyholder Join Phase.

If a person buys auto insurance from an insurance company IS_i, he/she will become a policyholder $PH_{i;j;n}$. Then, he/she needs to do the following steps, and the index n manifests the policyholder as the nth policyholder of IS_i.

(1) $PH_{i;j;n}$ sends its identity $ID_{i;j;n}$ to SM

(2) SM verifies its identity; if passes, SM randomly selects $\lambda_n \in \mathbb{Z}_p^*$ and computes $PID_{i;j;n} = E_{SM}(ID_{i;j;n} \oplus \lambda_{i;j;n} \| \lambda_{i;j;n})$ as $PH_{i;j;n}$'s pseudo-identity

(3) $PH_{i;j;n}$ receives $PID_{i;j;n}$ from SM through a secure channel

(4) $PH_{i;j;n}$ sends its pseudo-identity $PID_{i;j;n}$ to IS_i and then buys auto insurance in IS_i. At the same time, IS_i randomly selects $\delta \in \mathbb{Z}_p^*$ as the evidence for the policyholder and sends δ to $PH_{i;j;n}$

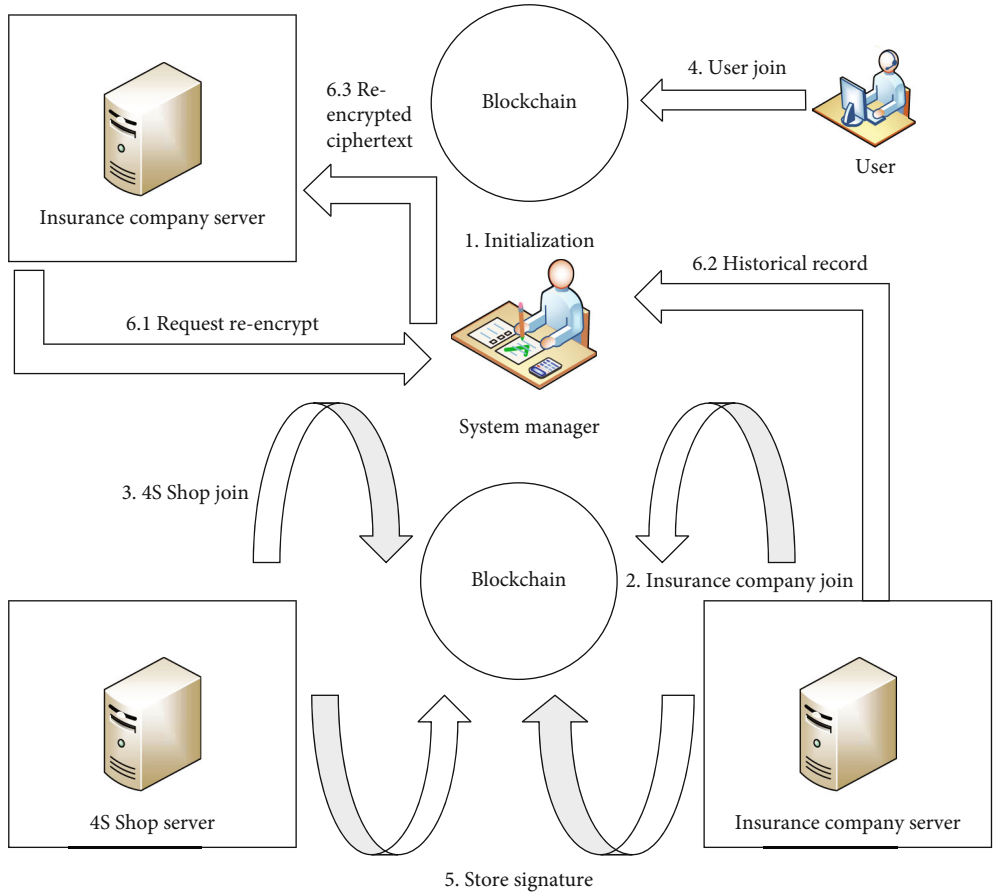

Figure 3: Proposed architecture.

(5) IS_i gives the policy information m_1; then, IS_i inputs $PK_{i;j;n}$, Y, m_1, randomly selects $r \in \mathbb{Z}_p^*$, and computes $\bar{C}_1 = g_1^r$, $\bar{C}_2 = PK_{i,j,n}^r$, $\bar{U} = e(Y, g_2)^r$, $\bar{C}_3 = H_2(U)$, $K = e(g, g)^r$, $\bar{C}_4 = [F(K, \bar{C}_1, \bar{C}_3)]_{l-l_1} \| \{[F(K, \bar{C}_1, \bar{C}_3)]_{l_1} \oplus m_1\}$, $h = H_3(\bar{C}_1, \bar{C}_3, \bar{C}_4)$, and $\bar{C}_5 = (u^h v d)^r$. IS_i stores the ciphertext $\bar{C}_{i;j;n} = (\bar{C}_1, \bar{C}_2, \bar{C}_3, \bar{C}_4, \bar{C}_5)$ in its server and signs the message m_1

(6) When policyholder's auto has an accident, $4S_j$ repairs the auto and generates maintenance information m_2. Then, $4S_j$ inputs $PK_{i;j;n}$, Y and m_2, randomly selects $r \in \mathbb{Z}_p^*$, and computes $C_1 = g_1^r$, $C_2 = PK_{r,j,n}^r$, $U = e(Y, g_2)^r$, $C_3 = H_2(U)$, $K = e(g, g)^r$, $C_4 = [F(K, C_1, C_3)]_{l-l_1} \| \{[F(K, C_1, C_3)]_{l_1} \oplus m_2\}$, $h = H_3(C_1, C_3, C_4)$, and $C_5 = (u^h v d)^r$. $4S_j$ stores the ciphertext $C_{i;j;n} = (C_1, C_2, C_3, C_4, C_5)$ in its server and signs the message m_2

3.5. Signature Store Phase. In a general DPOS, it needs to elect 101 legitimate participant delegates to record data on the blockchain. In our scheme, the insurance company and 4S Shop are two unrelated departments and have unique professional knowledge. Thus, the general DPOS is not suitable for the alliance blockchain. Because how to elect the delegates is a troublesome problem, and it also needs to take communication and calculation time. In our scheme, we proposed a lightweight and high-efficiency consensus mechanism as we can see in Algorithm 1, and it can be seen as an improvement on DPOS. Each insurance company and 4S Shop can be seen as delegates, who are responsible for broadcasting and recording their own generated data on the blockchain. Due to the high reliability of government agency, it is chosen as the supernode (multiple government agencies can be selected as supernodes to ensure the reliability of the scheme). Moreover, we set up a credit score scheme for the insurance company and 4S Shop to guarantee our mechanism is reliable. *SM* has the right to verify the signature of the insurance company and 4S Shop, if an error signature is found, the credit score of a relevant insurance company or 4S Shop will be reduced. If the credit score is reduced more than three times, it will be expelled from the blockchain. The verification steps of *SM* are listed as follows:

(1) IS_i or $4S_j$ broadcasts the policy data or repair data on the blockchain, respectively

(2) *SM* uses PK_i or PK_j to verify the signature every minute, and then, every twenty legitimate signatures are stored in one new block of the alliance blockchain

1: $IS_i/4S_j$ broadcasts the policy/repair result $C_{i;j;n}$ on the alliance blockchain
2: *SM* verifies the signature
3: if the signature passes the verification
4: the signature is stored in one new block
5: else
6: return FAlSE
7: end if

Algorithm 1: Improved consensus mechanism.

(3) Once the signature is verified, other nodes of the alliance blockchain update their blocks

3.6. Data Sharing and Search Phase. The insured repairs the auto in other 4S Shops or purchases auto insurance from other insurance companies; that is, it may need to know the previous insurance policy and auto maintenance records. In this part, we give an example of an insurance company on how to know the auto maintenance information during the claim process. Therefore, after the insurance company obtains $PH_{i;j;n}$'s permission, the algorithm enters PK_j and PK_i and performs the following steps:

(1) $PH_{i;j;n}$ computes $U_1 = g^{r'}$ and $U_2 = g_2^{1/x_n} H_1(Y^{r'})$ and sends (δ, U_1, U_2) to *SM*, where $r' \in \mathbb{Z}_p^*$ is a random number

(2) *SM* verifies δ; if passes, it sends an extraction instruction about $PH_{i;j;n}$'s policy information to $4S_j$

(3) The agent computes $h = H_3(C_1, C_3, C_4)$; if $e(C_1, PH_{i;j;n}u^h vd) = e(g_1, C_2C_5)$, it computes $C'_2 = C_2^{rk_{i\leftrightarrow n}} = PK_i^r$ and outputs the ciphertext $C'_{i;j;n} = (C_1, C'_2, C_3, C_4, C_5)$ to IS_i, where the reencryption key $rk_{i\leftrightarrow n} = x_i/x_n \bmod p$. Otherwise, the stage will be terminated

(4) The server of $4S_j$ sends the encrypted m_1 to *SM*

(5) *SM* computes $h = H_3(C_1, C_3, C_4)$; if $e(C_1, PH_{i;j;n}u^h v d) = e(g_1, C_2C_5)$, then it computes $U_\alpha = U_2/H_1(U_1^x)$ and ensures $C_3 = H_2[e(C_2, U_\alpha^x)]$ is true. Otherwise, *SM* outputs $\perp$

(6) IS_i computes $K = e(C'_2, g)^{1/x_i}$; if $[F(K, C_1, C_3)]_{l-l_1} = (C_4)_{l-l_1}$, then IS_i will obtain the ciphertext $m_1 = (C_4)_{l_1} \oplus [F(K, C_1, C_3)]_{l_1}$. Otherwise, the stage will be terminated

4. Security Analysis

According to the security requirements given in Section 2.3, this section will analyze the solution from the following security attributes.

(i) Security and privacy: all nodes need to register with *SM* when applying to join the blockchain. *SM* checks whether the identities of the auto owner, insurance company, and 4S Shop are legal. Only nodes with legal identities are allowed to join. After the insurance company or 4S Shop registers with *SM*, *SM* will generate a fake identity for it. When the owner goes to insure or repair the auto, *SM* also calculates a false identity for the owner. In the follow-up process, all nodes use fake identities instead of real identities, and privacy is greatly protected. All transaction information is encrypted by asymmetric encryption, which can effectively prevent unauthorized node access. When the insurance company needs to query the auto owner's maintenance record, the proxy reencryption technology will be used with the owner's consent. When *SM* finishes the confirmation, the agent will convert the relevant maintenance record into a document that the insurance company can decrypt with its private key. In this way, data sharing between different institutions is realized under the premise of ensuring data privacy. Therefore, the solution has good privacy and security

(ii) Data access: this scheme uses proxy reencryption technology to realize data sharing between different institutions. For example, if an insurance company wants to obtain the relevant data stored in the 4S Shop, the insurance company needs to obtain the consent of the applicant. Then, the insurance company will obtain the reencrypted ciphertext and decrypt it with its private key to get the data

(iii) User control: the insurance policy and maintenance records are stored in the respective servers of the insurance company and the 4S Shop. For example, if the insurance company wants to obtain the relevant data of the 4S Shop, the insurance company must first obtain the consent of the applicant. Therefore, the policyholders can control access to data

(iv) Unified standards: in this scheme, we can use unified data standards, such as the keywords of auto damage, which is conducive to data sharing and protection

(v) Tamper resistance: in this solution, the encrypted insurance data and auto maintenance records are stored in the servers of the insurance company and the 4S Shop, respectively, and their signatures are stored on the blockchain. Since the server is not completely trusted, it may tamper with data. One is that the server first colludes with the signer to modify the original data, then resigning the data and replacing the original signature on the blockchain. However, due to the existence of the timestamp, the replaced signature can never be completely consistent with the original signature.

Table 2: Comparison of calculation time (ms).

	Encrypt	Decrypt	Reencrypt	Redecrypt
[22]	$2M + 1E + 2P = 50.87$	$1M + 3P = 62.50$	$1P = 20.04$	$1M + 4P = 82.54$
[23]	$2M + 3P = 64.88$	$1M + 4P = 82.54$	$1P = 20.04$	$1M + 5P = 102.58$
Ours	$3M + 2P = 47.22$	$1M + 3P = 62.50$	$2P = 40.08$	$1M + 5P = 102.58$

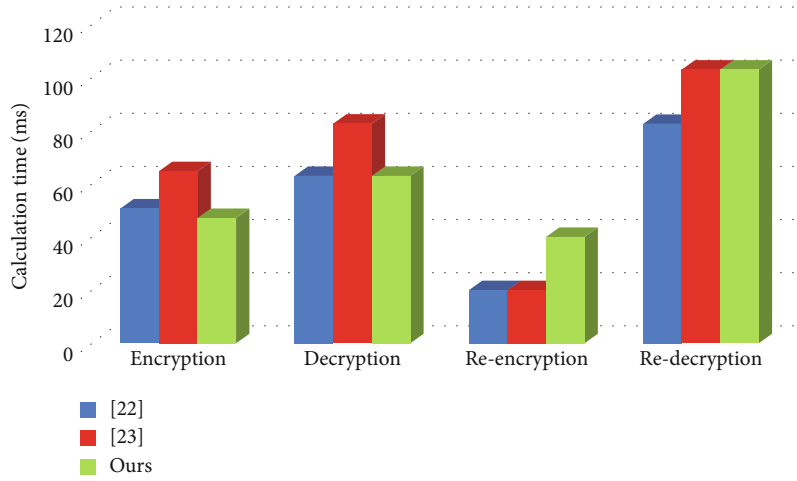

Figure 4: Comparison of calculation time.

Table 3: Comparison of communication cost.

Schemes	Communication cost (byte)
[22]	$8\lvert\mathbb{G}_1\rvert + 4\lvert\mathbb{Z}_p^*\rvert + 1\lvert x\rvert + 1\lvert ID\rvert + 3k + 2l$
[23]	$(n+3)\lvert\mathbb{G}_1\rvert + (n+2)\lvert\mathbb{Z}_p^*\rvert + 1\lvert x\rvert + 4\lvert ID\rvert + 2k + 2l$
Ours	$(n+5)\lvert\mathbb{G}_1\rvert + 5\lvert\mathbb{Z}_p^*\rvert + 1\lvert x\rvert + 2\lvert ID\rvert + 2k + 1l$

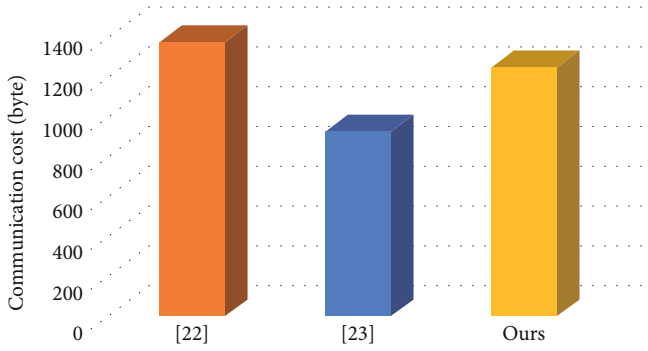

Figure 5: Comparison of communication cost.

Additionally, the signature stored on the blockchain will not be changed due to the immutable feature of the blockchain. The other one is the server forges the signature to modify the data and calculates the private key SK' which is the same as the private key SK of the signature node; that is, $SK' = SK$. However, according to the difficulty of discrete logarithms, this method is not feasible. In summary, the data signature stored on the blockchain is tamper resistance, and it also ensures that the data stored on the insurance company and 4S Shop servers are tamper resistance

(vi) Defend against modification attack: based on the above analysis, we know that it is difficult for the adversary to directly forge a new document to replace the target document, but we need to further consider the adversary's modification attack on the target document. In our scheme, we have two security mechanisms to resist this modification attack. The first is the signature verification mechanism. Under this mechanism, the insurance company, the 4S Shop, and the auto owner need to sign the insurance policy or the maintenance record sheet and then hand it over to SM to verify. Only the successfully verified document is valid. The voucher is based on a secure signature algorithm, and it is also impossible to forge or modify a document [21]. The second is the tamper resistance mechanism based on the blockchain. If the adversary cannot destroy the security of the blockchain, then the adversary cannot destroy the security of the system through a document modification attack. Besides, the use of timestamp also can prevent changes to the data. Therefore, the proposed scheme can resist the modification attack very well

5. Performance Analysis

In this section, we will compare the proposed scheme with two similar blockchain-based data sharing solutions [22, 23]. For the convenience of comparison, we use M to represent the multiplication operator, E to represent the power exponent operator in the finite field of prime numbers, and P to represent the bilinear pairing operator. It can be seen from [24] that the cost of a single multiexponentiation is about 1.2 times the cost of single exponentiation. The remaining operators are negligible due to their low calculation time.

In [25], they simulated the user's environment through Windows XP OS on Inter(R) Pentium IV 3.0 GHz processor and 512 MB RAM. At the same time, they simulated the C environment to run on a 32-bit Intel(R) PXA270 624 MHz processor and 128 MB of memory through Windows CE 5.2 OS. The system takes 20.04 ms to execute a bilinear pairing operator P, 2.38 ms to execute a multiplication operator M, and 5.31 ms to execute a power exponent operator E. In this article, we will use the basic test results in [25] to estimate the calculation cost.

According to Table 2 and Figure 4, the proposed solution takes less time in the encryption and decryption stages than the other two solutions. The time in the reencryption and redecryption stages is higher than the other two solutions, and the longest is 102.58 ms. But here the caveat is that the step of reencryption is completed by the agent, and its calculation ability is usually sufficient, so the extra time spent in our solution can be accepted. Particularly, the total time cost is decreased by 7% compared with the scheme in [23].

For the communication cost, the auto owner and the insurance company, the auto owner and the 4S Shop, and the insurance company and the 4S Shop in the three stages of data broadcasting, data verification, and data access are considered. In the proposed scheme, the auto owner $PH_{i;j;n}$ needs to send (U_1, U_2) to SM, where U_1 and U_2 are the elements of $\mathbb{G}_1$. If the insurance company wants to query the owner's maintenance records, the owner $PH_{i;j;n}$ will send the private key x_n to the SM, where x_n is the element of $\mathbb{Z}_p^*$. For insurance company and 4S Shop, it also needs to send the private key x_i or x_j to SM and receive the required history records, where x_i and x_j are also elements of $\mathbb{Z}_p^*$, and the ciphertext of the historical records is $C_{i;j;n}$. Also, insurance company and 4S Shop are responsible for broadcasting ciphertexts $C_{i;j;n} = (C_1, C_2, C_3, C_4, C_5)$, block ID, user pseudo-identities, public keys, and signatures on the blockchain. C_1, C_2, and C_5 are elements of $\mathbb{G}_1$, C_3 is an element of size k, and C_4 is an element of size l; the user's pseudo-identity is an element of the general ciphertext space (the length of the element is expressed as $|x|$), the public key is an element of $\mathbb{G}_1$, and the signature can be regarded as an element of the general ciphertext space. Therefore, the communication cost of our solution is $(n+5)|\mathbb{G}_1| + 5|\mathbb{Z}_p^*| + 1|x| + 2|ID| + 2k + 1l$.

Table 3 and Figure 5 show the comparison of communication cost. We assume that the size of the message sent in the alliance chain is $|x| = 160$ bits. When we encrypt the ciphertext with a key length of 80 bits, the size of q is 1024 bits. Therefore, the size of the element in $\mathbb{G}_1$ is 1024 bits, and the size of the element in $\mathbb{Z}_p^*$ is 2048 bits. However, we can use standard compression techniques [26] to reduce the size of elements in $\mathbb{G}_1$ to 520 bits (65 bytes), and the size of elements in $\mathbb{Z}_p^*$ is 1024 bits (128 bytes). In addition, the length of $|ID|$ is 8 bits, which occupies one byte, and the length of both k and l is 512 bits. When only one user is considered, the communication cost of scheme [22] is $8|\mathbb{G}_1| + 4|\mathbb{Z}_p^*| + 1|x| + 1|ID| + 3k + 2l = 8 \times 65 + 4 \times 128 + 1 \times 20 + 1 \times 1 + 3 \times 64 + 2 \times 64 = 1373$ bytes, the communication cost of scheme [23] is $(n+3)|\mathbb{G}_1| + (n+2)|\mathbb{Z}_p^*| + 1|x| + 4|ID| + 2k + 2l = 4 \times 65 + 3 \times 128 + 1 \times 20 + 4 \times 1 + 2 \times 64 + 2 \times 64 = 924$ bytes, and the communication cost of ours is $(n+5)|\mathbb{G}_1| + 5|\mathbb{Z}_p^*| + 1|x| + 2|ID| + 2k + 1l = 6 \times 65 + 5 \times 128 + 1 \times 20 + 2 \times 1 + 2 \times 64 + 1 \times 64 = 1244$ bytes. The proposed scheme's total communication cost is decreased by 10% compared with scheme [22]. The communication cost of scheme [23] is lower than ours, but this is only for a single user. As the number of users continues to grow, the advantages of the proposed scheme will be revealed.

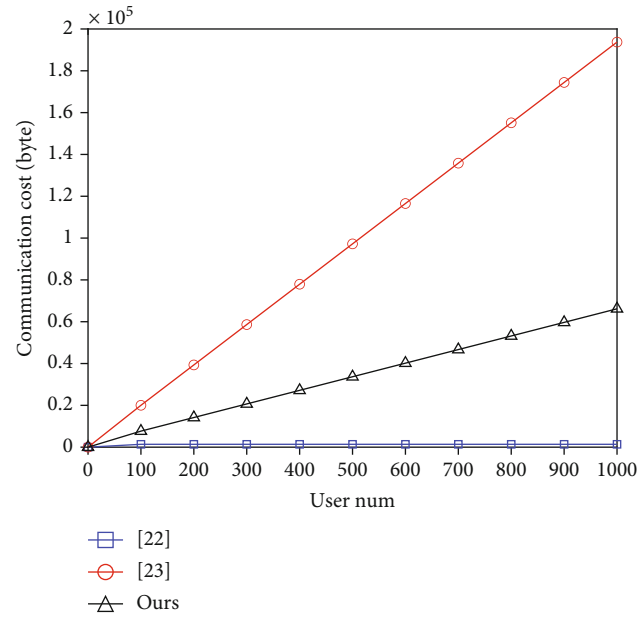

Figure 6: Impact of the number of users on calculation time.

With the increase of blockchain network users, the required calculation cost and communication cost will also increase. Next, we will analyze and compare the changing trend of the communication cost and calculation cost of our solution and other solutions when the user scale changes. The analysis results are shown in Figures 6 and 7. It can be seen from Figure 6 that the calculation costs of [22] and ours continue to increase with the number of users, but the growth rate is much lower than the solution proposed in [23]. It can be seen from Figure 7 that the communication cost of the solution proposed in [22] is not affected by the number of users n and always remains at a low level. The communication costs of [23] and ours are linearly positively correlated with the

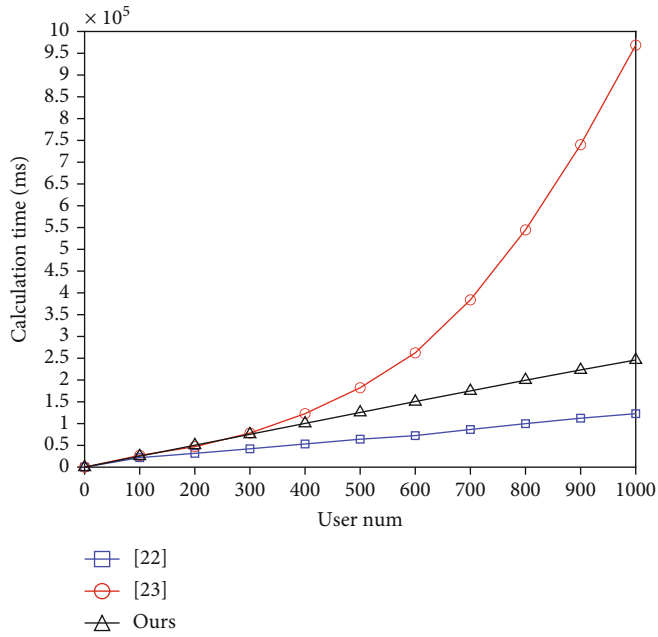

Figure 7: Impact of the number of users on communication cost.

number of users n. However, it can be seen that the communication cost of [23] is the highest, and the gap with the other two schemes is also getting bigger with the continuous increase of n. In conclusion, the proposed scheme has higher comprehensive performance.

6. Conclusion

The basic features of blockchain technology make it very suitable for data protection and sharing. This paper proposes a blockchain-based insurance claim data sharing model. For example, the insurance company can access the user's auto maintenance record through proxy reencryption technology and realize multiuser data sharing while protecting data privacy. The analysis results show that the proposed scheme meets many security requirements and has higher comprehensive performance compared with the existing two schemes.

Data Availability

All data included in this study are available upon request by contact with the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest concerning the publication of this paper.

Acknowledgments

This work is supported by the Fundamental Research Funds for the Central Universities of Southwest Minzu University (No: 2020NYB17), the Fund of Guangxi Key Laboratory of Cryptography and Information Security (No: GCIS202121), the National Natural Science Foundation of China (No: 61976047), the Key Fund Project of Sichuan Provincial Department of Education (No: 17ZA0414), and the Sichuan Science and Technology Program (No: 2017JY0230).

References

[1] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: beyond bitcoin," *Applied Innovation Review*, vol. 2, pp. 1–19, 2016.

[2] L. J. Kish and E. J. Topol, "Unpatients–why patients should own their medical data," *Nature Biotechnology*, vol. 33, no. 9, pp. 921–924, 2015.

[3] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. K-ishigami, "Blockchain contract: securing a blockchain applied to smart contracts," in *2016 IEEE International Conference on Consumer Electronics*, pp. 467-468, Las Vegas, USA, 2016.

[4] L. Q. Zhao, "The analysis of application, key issues and the future development trend of blockchain technology in the insurance industry," *American Journal of Industrial and Business Management*, vol. 10, no. 02, pp. 305–314, 2020.

[5] D. Popovic, C. Avis, M. Byrne et al., "Understanding blockchain for insurance use cases: a practical guide for the insurance industry," *British Actuarial Journal*, vol. 25, no. 13, pp. 1–23, 2020.

[6] A. Bogner, M. Chanson, and A. Meeuw, "A decentralised sharing app running a smart contract on the ethereum blockchain," in *The 6th International Conference on the Internet of Things*, pp. 177-178, New York, USA, 2016.

[7] A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy*, pp. 839–858, San Jose, USA, 2016.

[8] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in health care: \med "rec" prototype for

electronic health records and medical research data," in *2016 International Conference on Open and Big Data*, pp. 1–13, Bethesda, USA, 2016.

[9] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[10] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *Journal of Biomedical Informatics*, vol. 92, pp. 103140–103140, 2019.

[11] J. Hua, G. Shi, H. Zhu, F. Wang, X. Liu, and H. Li, "CAMPS: efficient and privacy-preserving medical primary diagnosis over outsourced cloud," *Information Sciences*, vol. 527, pp. 560–575, 2020.

[12] D. Q. Fu and L. Fang, "Blockchain-based trusted computing in social network," in *The 2nd IEEE International Conference on Computer and Communications*, pp. 19–22, Chengdu, China, 2016.

[13] X. G. Liu, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019.

[14] M. Mettler, "Blockchain technology in healthcare: the revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services*, pp. 1–3, Munich, Germany, 2016.

[15] Z. Zheng, S. A. Xie, H. N. Dai, X. P. Chen, and H. M. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data*, pp. 557–564, Honolulu, USA, 2017.

[16] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[17] Y. Yuan and F. Y. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 38, pp. 68–75, 2016.

[18] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 127–144, Zagreb, Croatia, 1998.

[19] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *2007 ACM Conference on Computer and Communications Security*, pp. 185–194, Alexandria, USA, 2007.

[20] L. F. Guo and B. Lu, "Efficient proxy re-encryption with keyword search scheme," *Journal of Computer Research and Development*, vol. 51, no. 6, pp. 1221–1228, 2014.

[21] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[22] Y. X. Ji, *Blockchain-based user location information security sharing scheme*, Master's thesis, Xidian University, 2019.

[23] S. Lanlan, *Research on cloud storage and sharing of re-encrypted ciphertext based on block chain attribute agent*, Master's thesis, Jiangxi University of Science and Technology, 2019.

[24] J. H. Zhang and J. Mao, "An efficient RSA-based certificateless signature scheme," *Journal of Systems and Software*, vol. 85, no. 3, pp. 638–642, 2012.

[25] J. W. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2014.

[26] K. A. Shim, "CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2016.