Hindawi
Journal of Sensors
Volume 2022, Article ID 6182502, 12 pages
https://doi.org/10.1155/2022/6182502

Research Article

A Crowdsourcing Information Obtaining Scheme Aiming at Senior Netizens Based on Blockchain

Yanlin Qin, Xueguang Zhou, and Guoheng Wei

Department of Information Security, Naval University of Engineering, Wuhan 430033, China

Correspondence should be addressed to Guoheng Wei; wgh7929@aliyun.com

Received 24 October 2021; Accepted 2 December 2021; Published 8 February 2022

Academic Editor: Min Xia

Senior netizens play a unique role in crowdsourcing information obtaining, but the traditional crowdsourcing information obtaining scheme based on intermediary platform cannot satisfy the senior netizens' strong reliability on anonymity. Malicious intermediary platform may leak out the privacy information of both parties. Data stored in intermediary platform may be intercepted, tampered, and fraudulently used by attackers, so smooth crowdsourcing information transactions cannot be ensured. In order to achieve secure and reliable crowdsourcing information obtaining, blockchain technology with decentralization and nontampering was used to propose a crowdsourcing information obtaining scheme, which is independent on intermediary platform. During processes of requirements releasing, information submitting, and rewarding, privacy protection techniques were used to preserve the anonymity of participants and confidentiality of data. Compared with the existing protocols, the proposed scheme has obvious advantages in privacy protection.

1. Introduction

The concept of crowdsourcing was proposed by Howe [1] and refers to outsourcing tasks to unspecified mass networks in a free and voluntary way. The basic model of traditional crowdsourcing includes the outsourcer, the contractors, and the crowdsourcing intermediary, which constitute the crowdsourcing operation organization. The outsourcer issues requirements and the intermediary provides tasks; the contractors submit the information, and the intermediary feedbacks contractors' submission. Crowdsourcing activities often involve many people in bidding for a task, and the evaluation process is mainly based on the satisfaction of the outsourcer of the task. According to the purpose of crowdsourcing, it can be divided into crowd wisdom [2], crowd creation, crowd voting, and crowdfunding. Crowdsourcing information obtaining activities are crowd wisdom activities, in which the outsourcer attracts netizens to participate voluntarily, and the contracting netizens collect and provide the information to the outsourcer through Web pages, newspapers, and magazines and field investigations, and the outsourcer screens the effective crowdsourcing information manually and systematically and gives appropriate rewards to the participants. In the crowdsourcing information obtaining scheme in this paper, the contractors mainly consist of senior netizens, because the space-time extension and anonymity of the network attract senior netizens to stay on the Internet for a long time, which is an important force to participate in network activities. However, in the traditional crowdsourcing information obtaining scheme that relies on the intermediary platform, it is difficult to ensure senior netizens' strong requirement of anonymity, and the intermediary platform, driven by its interests, may disclose the private data of the outsourcer and the contractors in the process of crowdsourcing information transactions. At the same time, attackers will take various measures to intercept, tamper, and fraudulently use key data stored in the intermediary platform. Once the intermediary platform is attacked, it will directly threaten the fluent operation of the whole crowdsourcing transaction mechanism.

The main work of this paper is as follows:

(1) Establish a decentralized and nontampered crowdsourcing information obtaining framework based on blockchain. Before joining the crowdsourcing information obtaining blockchain, the key generation

center generates certificateless public and private key pairs, including initialization parameter generation and nodes' public/private key pair generation

(2) Design the release algorithm of the crowdsourcing information requirements. The certificateless multireceiver anonymous signcryption scheme is used to complete the release of the requirements, and the blockchain address of the outsourcer, the information requirements, and reward is encrypted together. Except for the intended contractors, other nodes cannot know the information such as requirements and rewards. In the signcryption information issued by the outsourcer, the blockchain address of the contractor is hidden to prevent other nodes in the network from tracking its identity through the blockchain address of the contractor. At the same time, each contractor only uses its private key and blockchain address in the process of unsigncrypt and does not need addresses of other contractors, thus, ensuring mutual anonymity among contractors

(3) Design the submission algorithm of the crowdsourcing information using the idea of random address, the outsourcer generates a temporary public key address and records it in the blockchain. The contractor uses its long-term private key to calculate the temporary private key for the information submission. After receiving the crowdsourcing information returned by the contractor, the outsourcer decrypts and verifies it, thus, realizing the confidentiality of the crowdsourcing information and preventing the identity of the contractor from being exposed in the process of submitting the information many times

(4) Design the reward accounting algorithm of the crowdsourcing information. The outsourcer determines the reward accounting of crowdsourcing information by generating ring signcryption, so as to prevent the leakage of identity privacy in the process of awarding. The contractor uses the temporary private key to decrypt the ring signcryption of the outsourcer and confirm the legal reward from the outsourcer. When using legal rewards, the contractor only needs to use its temporary private key to complete the signature, and the payee can verify the signature by using the temporary public key of the contractor recorded in the blockchain. Because the temporary public key addresses of the contractor are different in each crowdsourcing information transaction, the consumer anonymity of the contractor is realized

(5) Analyze the privacy protection effect and operation efficiency of the scheme proposed in this paper. In terms of privacy protection, this scheme is compared with existing information sharing schemes based on blockchain, mainly from three dimensions: outsourcer privacy protection, contractor privacy protection, and transaction data privacy protection. By comparison, it is verified that this scheme has obvious advantages over other schemes in privacy protection and has higher calculation efficiency

2. Relevant Work

Traditional crowdsourcing information obtaining is composed of the outsourcer, the crowdsourcing intermediary platform, and the contractors, and the crowdsourcing information obtaining task is completed through 9 steps. In the traditional process of obtaining crowdsourcing information, the outsourcer and the contractor need to release and submit the information through the intermediary crowdsourcing platform, which brings extra cost to both parties. On the other hand, there is no completely trusted intermediary in the real network, and the malicious crowdsourcing intermediary platform may sell the private information of both parties in crowdsourcing information transactions for its own benefits. At the same time, once the intermediary platform is attacked, the whole crowdsourcing transaction mechanism will be paralyzed and chaotic. Therefore, we can introduce decentralized blockchain technology into crowdsourcing information transaction to remove the dependence on crowdsourcing intermediary platform. The traditional crowdsourcing information obtaining process is shown in Figure 1.

Because blockchain technology has the characteristics of no center, anti-tamper, and anonymity, scholars have applied blockchain technology to the field of network information sharing. Rawat et al. [3] designed a multimember information sharing framework based on blockchain technology, in which nodes in blockchain can share network security protection schemes, and analyzed possible attack behaviors in the system based on game theory. Huang et al. [4] designed a network security threat intelligence sharing model based on blockchain to solve the privacy protection demand of users in the process of threat intelligence sharing. However, this model directly uses the anonymity of users' accounts in the blockchain to protect the identity privacy of both parties in the threat intelligence sharing, which can only provide weak anonymity. In the frequent information sharing process between the two parties, attackers can infer the true identity of users by analyzing the correlation between transactions, statistical characteristics, and transaction amounts. At the same time, the status of the threat intelligence center in the model is not equal to that of the organization, and the organization needs to register at the threat intelligence center when joining the threat intelligence sharing blockchain. Wang et al. [5] proposed a private data sharing model of medical blockchain based on ring signature. However, this model only considers the anonymity protection of transaction outsourcer and lacks the anonymity protection mechanism of contractor. At the same time, the ring signature message is not encrypted, which easily leads to the leakage of users' private data. He et al. [6] proposed an incentive mechanism for crowdsensing applications based on blockchain technology, which uses digital signature and watermarking technology

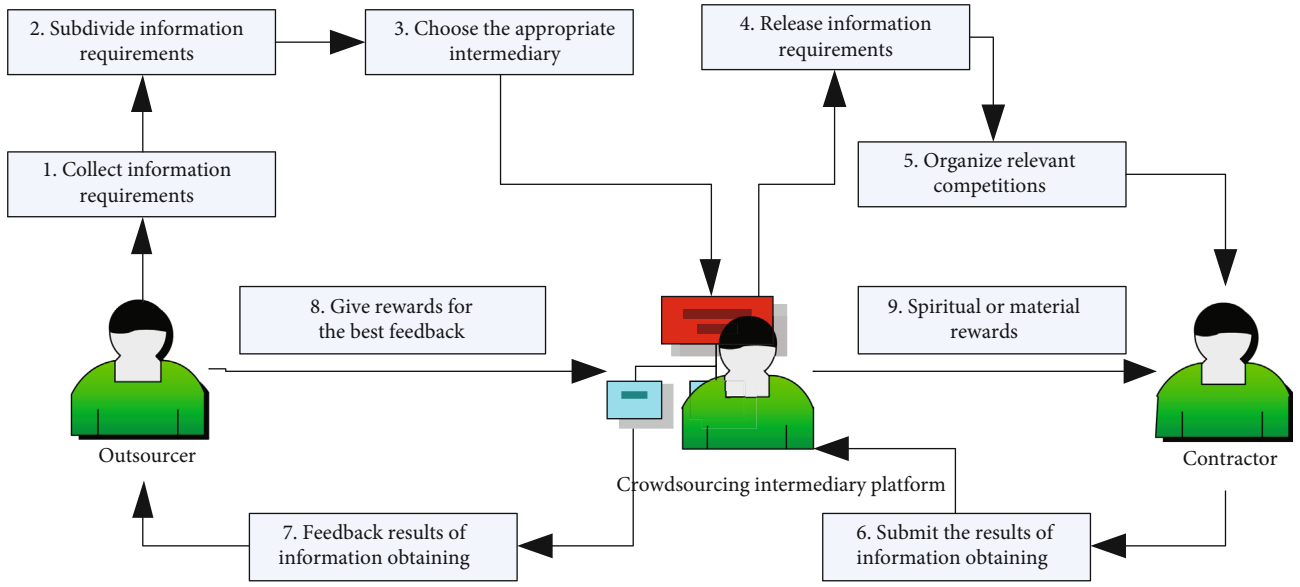

Figure 1: Flowchart of traditional crowdsourcing information obtaining.

to prevent the sensing data from being tampered and used under false pretences, but this scheme does not protect the confidentiality of the sensing data and the identity privacy of the sensing users. Cheng et al. [7] designed a framework of network threat intelligence sharing and rating system based on blockchain, but did not give technical details to protect the confidentiality of threat intelligence and the anonymity of nodes. Cai et al. [8] designed the application framework of Internet public welfare crowdfunding platform on blockchain, but also did not involve specific measures to protect the privacy of platform users and the security of crowdfunding data. Xu et al. [9] designed a privacy protection scheme for electronic health records based on blockchain and homomorphic encryption, which uses proxy reencryption technology to protect the security of patient's privacy data. However, the protection of patient's identity privacy only depends on the anonymity of the patient's Ethereum address, and there is still the risk of identity being tracked and leaked during the frequent use. Sandro et al. [10] designed a secure sharing framework of personal health data based on blockchain, which mainly relies on the anonymity of blockchain addresses to protect user's personal privacy. Li et al. [11] established a trusted big data sharing model without center by using blockchain and smart contract, but the privacy protection of data provider and data demander mainly depends on the anonymity of blockchain address. Mohammad et al. [12] proposed a data sharing framework based on licensed blockchain to ensure real-time authentication of shared data and tracking audit of data access in blockchain. The scheme uses the public key of data subject to encrypt access records, which protects the privacy of data subject, but does not protect the privacy of data accessor. Fan et al. [13] proposed a data sharing scheme for content-centric 5G networks based on blockchain. The scheme issues identity certificates to each user and uses encryption technology to ensure the confidentiality of data in the network, but it lacks protection measures for the identity privacy of data sharing parties in blockchain. Qiao et al. [14] designed a data sharing scheme for 5G IoT based on blockchain to solve the privacy of transactions under the chain, but did not discuss the privacy protection strategy of both parties in the chain cash withdrawal transaction.

The research of blockchain's application in information sharing in other industries has made some progress, but these research results cannot be directly applied to crowdsourcing information obtaining. It is difficult to meet the special needs of both parties of crowdsourcing transactions for personal identity privacy and transaction privacy. To solve the above problems, this paper designs a crowdsourcing information obtaining scheme based on blockchain. The scheme uses a certificateless multireceiver anonymous signcryption scheme with anonymous to release crowdsourcing information requirements and rewards, which not only protects the confidentiality of information requirements but also ensures the anonymity of the outsourcer and the contractor. To generate a temporary public-private key pair for the contractor, the contractor uses the temporary private key to signcrypt the collected crowdsourcing information to ensure the secrecy of the returned information and the identity untraceablity of the contractor. The One-Time-Pad ring signcryption algorithm is used to ensure the anonymity of the outsourcer in the reward payment transaction and the secrecy of the reward amount, and at the same time, the untraceability of the contractor in the process of using the reward for consumption is realized.

3. Background Knowledge

3.1. Blockchain Technology Foundation. Blockchain is a distributed ledger that records transaction data permanently [15], which is formed by linking some ordered data structures (also called blocks). All nodes in the blockchain

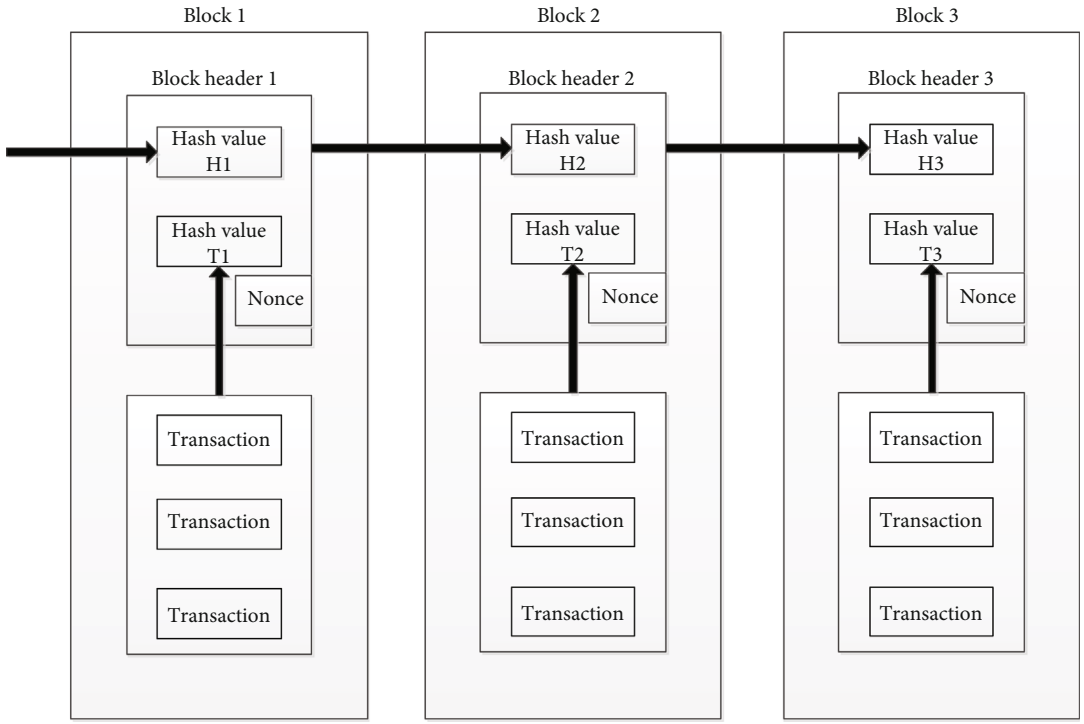

Figure 2: Data structure of blockchain.

network share a complete ledger, and once the transactions recorded in any ledger are released, it is difficult to modify them. Due to the difference of decentralization degree, there are two forms of blockchain [16]: the unlicensed chain and the licensed chain. The unlicensed chain is completely decentralized, and nodes are free to join and exit. It is suitable for a completely open and highly autonomous application environment. In the licensed chain, there are a few nodes that have higher authority than ordinary nodes. When joining, the nodes need to be authorized by the central node. The licensed chain is mainly suitable for small-scale internal data sharing.

The data structure of blockchain consists of transaction records and blocks [17]. First, both parties create a new transaction and broadcast it to the blockchain. Miner nodes package and merge the transactions generated and verified to be legal within a certain period into blocks, compete for the bookkeeping right through the Proof of Work (PoW) mechanism, and then add the new blocks to the blockchain.

The core unit of blockchain is block, which is composed of block header to ensure the orderly and complete block data and block body containing several transaction records. The block header stores the hash value of the block header of the previous block, Merkleroot, which is the overall hash value of all transaction data in this block, and a random number named nonce, timestamp, and other structured information; The block body is used to record the summary information of all verified transactions and a Merkle Tree [18] which ensures that transactions cannot be tampered. Figure 2 shows the data structure of blockchain.

3.2. Unlicensed Signcryption Scheme [19]. The scheme includes signer (ID_A), signcryption receiver (ID_B), and key generation center (KGC). The algorithm includes seven steps:

(1) *Setting of System Parameter*. Enter the security parameter η, KGC sets the system public parameters, generates the system master key s, and keeps it secretly

(2) *Setting of Partial Public and Private Keys*. Enter system parameters, master key s and user's identity ID_i, and KGC sets user's partial public and private key (D_i, u_i)

(3) *Setting of User's Secret Value*. Taking system parameters and user's identity ID_i as input, the user sets its secret value x_i and keeps it secretly

(4) *Setting of Complete Private Key*. Taking system parameters, user's identity ID_i, partial private key u_i, and secret value x_i as inputs, the user sets its complete private key (x_i, u_i)

(5) *Setting of Complete Public Key*. Taking system parameters, user's identity ID_i, partial public key D_i, and secret value x_i as inputs, the user sets its complete public key (X_i, D_i)

(6) *Signcryption*. Take system parameters, message m, signer's identity ID_A, private key (x_A, u_A), receiver's identity ID_B, and public key (X_B, D_B) as input, the signer outputs the signcryption σ of message m

(7) *Verification of Signcryption*. Take system parameters, σ, signer's identity ID_A, public key (X_A, D_A), receiver's identity ID_B and private key (X_B, D_B) as

input, receiver performs decryption and verification, then outputs that m is "True" or "Rejected"

3.3. CryptoNote Protocol [20]. To protect the identity anonymity of blockchain nodes, that is, to prevent attackers from gradually analyzing the identity information corresponding to their addresses through transaction records. The following is a brief description of the process of using one-time public and private keys to protect the anonymity of the contractor's identity in CryptoNote protocol: assume that the contractor's public and private key pair is $(A, B)/(a, b)$, which satisfies $A = aG$, $B = bG$. Both parties conduct transactions through the following steps:

(1) The outsourcer randomly selects an integer r and calculates $R = rG$; use the public key (A, B) of the contractor to calculate the one-time transaction public key $P = H(rA)G + B$

(2) The outsourcer initiates the transaction and releases R, P, and the transaction amount on the blockchain

(3) The contractor calculates $P' = H(aR)G + bG$ by using its private key and compares it with the one-time public key included in the transaction initiated by the outsourcer. If it is consistent, it is determined that it is the legal contractor of the transaction

(4) The legal contractor calculates the one-time private key $x = H(aR) + b$ corresponding to the one-time public key and uses this private key to sign and consume the transaction revenues

4. A Crowdsourcing Information Obtaining Scheme Based on Blockchain

4.1. Overall Description of the Scheme. Because the contractors of the crowdsourcing information obtaining scheme in this paper are senior netizens in the network, and the senior netizens often have characteristics such as self-dependence, independence, alertness, and low self-exposure, the anonymity of the network plays a vital role in stimulating senior netizens to participate in crowdsourcing information obtaining. The unlicensed blockchain can be completely decentralized, allowing nodes to freely join and exit the network. This high autonomy is completely consistent with the strong dependence of senior netizens on network anonymity, which can give full play to their own advantages. Therefore, this paper designs a crowdsourcing information obtaining scheme in unlicensed blockchain. The network nodes include the outsourcer node, the contractor node, and the miner node. Among them, miner nodes compete to obtain the bookkeeping right through the PoW mechanism, verify the crowdsourcing transactions, and package the verified transactions into the new block. All miners are jointly responsible for the maintenance of the blockchain. For the sake of simplification, it is assumed that there is one outsourcer node F and multiple contractor nodes $J_1, J_2, \cdots, J_k$ in the network, and the scenarios of multiple outsourcers and multiple contractor nodes can be discussed similarly. Before joining the crowdsourcing information obtaining blockchain, the outsourcer node and the contractor node need to generate their own public and private key pairs and blockchain transaction addresses.

The crowdsourcing information obtaining scheme based on blockchain mainly consists of the following three stages:

(1) *Release Stage of Crowdsourcing Information Requirements.* The outsourcer collects information requirements and sends the requirements and reward to the contractor (senior netizens). The release algorithm of the crowdsourcing information requirements in 4.3 will be used in this stage

(2) *Submission Stage of Crowdsourcing Information.* The contractor makes full use of its superior resources to collect the information meeting the task requirements and submit the required information to the outsourcer. The submission algorithm of crowdsourcing information in 4.4 will be used in this stage

(3) *Evaluation and Reward Stage of Crowdsourcing Information.* The outsourcer evaluates the quality, timeliness, and benefit of the crowdsourcing information submitted by the contractor, selects the best result to pay remuneration, and realizes the incentive for the contractor to participate in the crowdsourcing information collection. The reward accounting algorithm of the crowdsourcing information in 4.5 will be used to generate a reward transaction and broadcast the transaction to the crowdsourcing information obtaining blockchain. The basic architecture of crowdsourcing information obtaining scheme based on blockchain is shown in Figure 3

4.2. Initialization Settings. Before joining the crowdsourcing information obtaining blockchain, the outsourcer node and the contractor node first generate certificateless public and private key pairs.

Client wallet performs the following steps to set system parameters and generate certificateless public and private key pairs for nodes:

(1) Generation of initialization parameters

Select elliptic curve addition group G with large prime order q, P is a generator of G; define the following four secure Hash functions:

$$H0 : \{0,1\}^* \times G \times G \longrightarrow Z_q^*, \tag{1}$$

$$H1 : G \times \{0,1\}^* \times G \longrightarrow Z_q^*, \tag{2}$$

$$H2 : G \longrightarrow \{0,1\}^*, H3 : \{0,1\}^* \longrightarrow Z_q^*, \tag{3}$$

$$H4 : G \longrightarrow Z_q^*. \tag{4}$$

$s \in Z_q^*$ is the master key of the client wallet, $PK_m = sP$ is its corresponding public key, and the system parameters $(q, PK_m, H_0, H_1, H_2, H_3, H_4)$ are disclosed to the public.

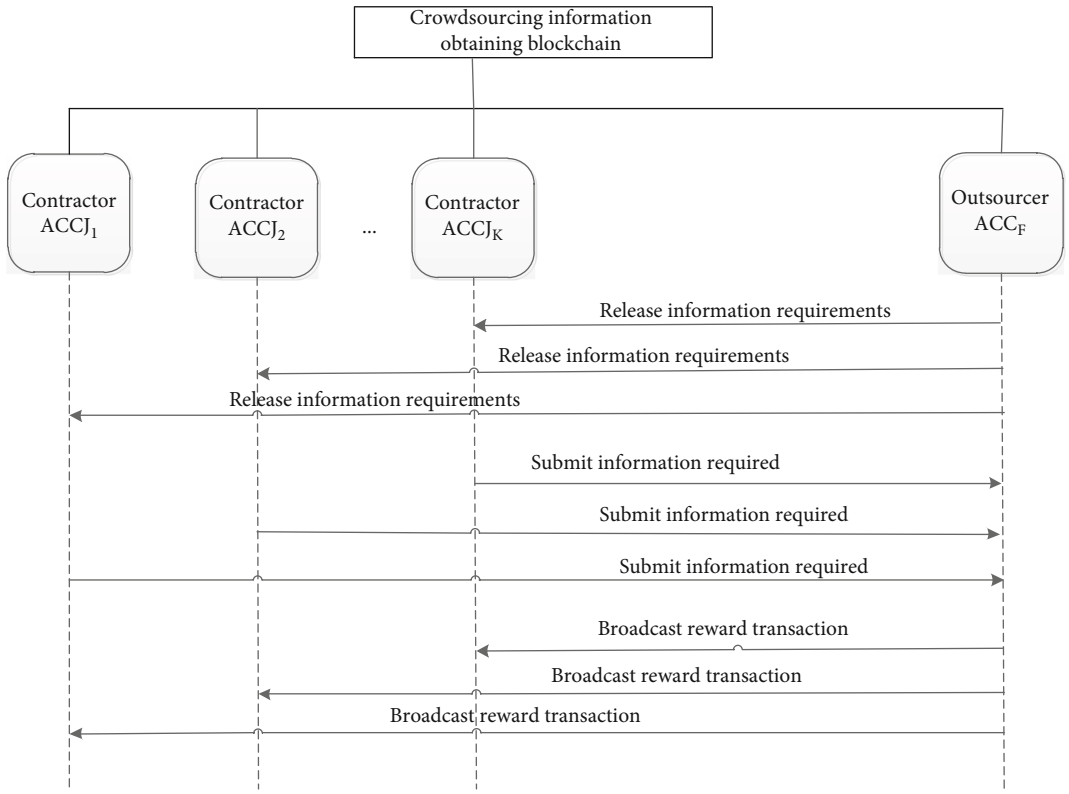

Figure 3: Basic architecture of crowdsourcing information obtaining scheme based on blockchain.

(2) Generation of node's public/private key pair

Node ID_i selects a random number $x_i \in Z_q^*$ as its secret value, calculates $X_i = x_i P$, and sends $X_i \| ID_i$ to the client wallet.

Client wallet selects random number $d_i \in Z_q^*$ and calculates

$$D_i = d_i P, u_i = d_i + sH_0(ID_i, D_i, X_i). \quad (5)$$

Then, returns to part of the user's partial public-private key pair D_i/u_i and the node ID_i obtains its complete public-private key pair $(X_i, D_i)/(x_i, u_i)$.

According to the key generation algorithm, the public and private key pair generated for the outsourcer node is $(X_F, D_F)/(x_F, u_F)$, and then the blockchain address is $ACC_F = H_0(ID_F, D_F, X_F)$ calculated from the public key; the certificateless public-private key pair of the contractor node is $(X_{J_i}, D_{J_i})/(x_{J_i}, u_{J_i})$, and the blockchain address is $ACC_{J_i} = H_0(ID_{J_i}, D_{J_i}, X_{J_i})$, $1 \le i \le k$.

4.3. Release Algorithm of the Crowdsourcing Information Requirements. The first stage of the crowdsourcing information obtaining scheme based on blockchain is the release of information requirements and rewards: the outsourcer collects the information requirements of decision makers, subdivides the information requirements, and sends the information requirements and rewards to the senior netizens (contractors) positioned in the early stage. In order to ensure the identity anonymity of the outsourcer and the contractor in the process of releasing crowdsourced information requirements and to realize the privacy of crowdsourcing information and rewards, the certificateless multireceiver anonymous signcryption scheme proposed in reference [19] is used to sign the requirements and rewards. Set $M = (T \| \text{requirements} \| \text{reward})$, where T is a timestamp.

The outsourcer releases M by the following algorithm:

(1) Randomly select a number $r_1 \in Z_q^*$ calculate $R_1 = r_1 P$ and $h = H_1(R_1 + X_F, ACC_F, M, D_F)$, $\text{SIG} = r_1 + x_F / x_F + hu_F$

(2) Randomly select $r_2 \in Z_q^*$, calculate $R_2 = r_2 P$

$$C = H_2(R_2) \bigoplus (M \| ACC_F \| SIG); \quad (6)$$

(3) Calculate $y_i = H_3(ACC_{J_i})$, $1 \le i \le k$, and calculate Lagrange interpolation polynomial

$$f_i(x) = \prod_{1 \le j \ne i \le k} \frac{y - y_j}{y_i - y_j} = c_{i1} + c_{i2} y + \cdots c_{ik} y^{k-1}, \quad (7)$$

where $c_{i1}, c_{i2}, \ldots, c_{ik} \in Z_q^*$

(4) Calculate

$$Y_i = r_2\left(X_{J_i} + D_{J_i} + ACC_{J_i}PK_m\right), V_i = \sum_{j=1}^{k} c_{ji}Y_j, \quad (8)$$

$$1 \le i \le k \quad (9)$$

(5) The outsourcer broadcasts ciphertext $\sigma = (V_1, V_2, \cdots, V_k, R_1, C)$ to the group of the contractors

After receiving it, the contractor executes the following algorithm for unsigncryption:

(1) Calculate

$$y_i = H_3\left(\mathrm{ACC}_{J_i}\right), \quad (10)$$

$$Y_i' = V_1 + y_i V_2 + \cdots y_i^{k-1} (\mathrm{mod}\, q) V_k. \quad (11)$$

Calculate $R_2' = (x_{J_i} + u_{J_i})^{-1} Y_i'$, recover the original message and signature $(M \| \mathrm{ACC}_F \| \mathrm{SIG}) = H_2(R_2') \oplus C$.

(2) Get the blockchain address ACC_F of the outsourcer from the recovered message, and then calculate

$$h' = H_1(R_1 + X_F, ACC_F, M, D_F); \quad (12)$$

(3) Verify the equation by using the public key (X_F, D_F) and address ACC_F of the contractor

$$h' = H_1\left(\mathrm{SIG}\left(X_F + h'(D_F + \mathrm{ACC}_F\mathrm{PK}_m)\right), \mathrm{ACC}_F, M, D_F\right). \quad (13)$$

Whether it is true or not, if so, the contractor confirms that the received signcryption is truly from the address ACC_F, otherwise, it refuses the signcryption.

In the above algorithm, the outsourcer encrypts its blockchain address, information requirements, and reward amount, which makes it impossible for other nodes in the blockchain to know from which blockchain address the information requirements are released, except for the nodes in the intended contractor group. At the same time, in the signcryption information released by the outsourcer, the blockchain address of each contractor is also hidden. Not only can the nodes outside the contractor group not know the blockchain address of the contractor but also the contractor only uses its private key and blockchain address in the decryption process and does not use the address of other contractors. This ensures that each contractor cannot know each other's blockchain address, that is, it can achieve mutual anonymity, which is consistent with the contractor's requirement for privacy protection.

4.4. Submission Algorithm of the Crowdsourcing Information. After receiving the crowdsourcing information requirements released by the outsourcer, the senior netizens voluntarily decide whether to join the crowdsourcing information obtaining blockchain network based on their own expertise and accumulated network resources. After collecting the required information, the contractor submits the information to the outsourcer. Although there is no direct relationship between the blockchain address of the contractor and the identity of senior netizens, which ensures the anonymity of the contractor to a certain extent, the contractor still has the risk of leaking his identity in the process of using the same address for multiple crowdsourcing information transactions with the outsourcer. Therefore, this paper uses the idea of random address in CryptoNote [20]. First, the outsourcer performs the following steps to generate a temporary public key address for each intended contractor and record it in the blockchain:

(1) Randomly select a number $t_{i1}, t_{i2} \in Z_q^*$, calculate $T_{i1} = t_{i1}P$, $T_{i2} = t_{i2}P$, $1 \le i \le k$

(2) Calculate the temporary public key address of this crowdsourcing information transaction $\mathrm{ACC}_{J_i}' = (X_{J_i}', D_{J_i}') = (H_4(t_{i1}X_{J_i})P, H_4(t_{i2}(D_{J_i} + \mathrm{ACC}_{J_i}\mathrm{PK}_m))P)$, $1 \le i \le k$

(3) Record T_{i1}, T_{i2}, and $\mathrm{ACC}_{J_i}' = (X_{J_i}', D_{J_i}')$, $1 \le i \le k$, in the blockchain

The contractor uses its long-term private key (x_{J_i}, u_{J_i}), to calculate the temporary private key $(x_{J_i}', u_{J_i}') = (H_4(x_{J_i}T_{i1}), H_4(u_{J_i}T_{i2}))$ for the information submission this time, and then executes the following algorithm to signcrypt $I = (T \| \text{information data})$ and return the signcryption to the outsourcer:

(1) Randomly select a number $z_i \in Z_q^*$, calculate $Z_i = z_iP$, $h_i = H_1(Z_i + X_{J_i}', ACC_{J_i}', I, D_{J_i}')$

(2) Generate the signature of I

$$\mathrm{SIG}_{J_i} = \frac{z_i + x_{J_i}'}{x_{J_i}' + h_i u_{J_i}'}; \quad (14)$$

(3) Calculate

$$V_{J_i} = \left(z_i + x_{J_i}'\right)(X_F + D_F + \mathrm{ACC}_F\mathrm{PK}_m), \quad (15)$$

$$C = H_2\left(V_{J_i}\right) \oplus \left(I \| \mathrm{SIG}_{J_i}\right). \tag{16}$$

Send signcryption $\sigma = \{Z_i, C\}$ to the outsourcer F.

After receiving the signcryption returned by the contractor, the outsourcer performs the following steps to decrypt and verify:

(1) Calculate $V_F = (Z_i + X'_{J_i})(x_F + u_F)$

(2) Recover the data returned by the contractor

$$I \| \mathrm{SIG}_{J_i} = H_2(V_F) \oplus C. \tag{17}$$

(3) Calculate

$h_i = H_1(Z_i + X'_{J_i}, ACC'_{J_i}, I, D'_{J_i})$ and verify

$$h_i = H_1\left(\mathrm{SIG}_{J_i}\left(X'_{J_i} + h_i D'_{J_i}\right), \mathrm{ACC}'_{J_i}, I, D'_{J_i}\right). \tag{18}$$

Whether it is true or not, if it is true, confirm that the information comes from the contractor corresponding to the blockchain address ACC'_{J_i}.

In the above algorithm, the contractor uses the temporarily generated private key to submit the data, so as to ensure the confidentiality of the data and prevent exposing its identity in the process of submitting. Normally, in order to protect the contractor's enthusiasm to collect information, no disciplinary measures are taken for the contractor submitting information with low quality. If very few contractors maliciously submit irrelevant data for many times, the outsourcer can trace the blockchain address information of the malicious contractor according to the corresponding relationship between its retained contractor blockchain address and the temporary address, thus, excluding the malicious contractor address from the contractor set in the future information requirements release.

4.5. Reward Accounting Algorithm of the Crowdsourcing Information. In order to encourage the contractor to complete the collection and submission of crowdsourcing information with high quality, the following is the reward accounting algorithm of the crowdsourcing information. After receiving the information provided by the contractor, the outsourcer screens out valuable information manually and systematically and pays appropriate remuneration to the corresponding contractor. The higher the quality of the submitted crowdsourcing information, the higher the amount of reward. At the same time, in order to realize the identity anonymity of the outsourcer and the contractor and the reward confidentiality in the process of crowdsourcing information reward transaction, the following One-Time-Pad ring signcryption algorithm [21] will be improved and the following reward accounting algorithm of crowdsourcing information will be given to ensure that the transaction record will not expose the specific identity of the outsourcer and the contractor in the blockchain and will not expose the reward amount m:

(1) The outsourcer selects the one-time random key k_F, calculates the corresponding public key $K_F = k_F P$, and then constructs the public key set $\{K_1, K_2 \cdots, K_n\}$, which does not contain the one-time public key K_F

(2) The outsourcer selects $a_i, b_i \in Z_q^* (1 \le i \le n)$ to set the attribute value for the public key in the public key set:

$$A_i = a_i P + b_i K_i, B_i = a_i H_2(K_i) + b_i k_F H_2(K_F), 1 \le i \le n. \tag{19}$$

Select $a_F, b_F \in Z_q^*$ to set the attribute value for the random public key K_F:

$$A_F = a_F P, B_F = a_F H_2(K_F). \tag{20}$$

(3) Set $s_i = b_i$, $c_i = a_i$, $1 \le i \le n$

(4) Calculates $s_F = H_0(m, A_1, A_2, \cdots, A_n, A_F, B_1, B_2, \cdots B_n, B_F) - \sum_{i=1}^{n} s_i$.

(5) Calculate $c_F = a_F - s_F k_F$, and

$$X_F = (m, s_1, s_2, \cdots, s_n, s_F, c_1, c_2, \cdots, c_n, c_F). \tag{21}$$

(6) Select random number v_F and calculate

$$V_F = v_F P, C = H_2(V_F) \bigoplus X_F. \tag{22}$$

(7) Calculate $W_F = v_F(X'_{J_i} + D'_{J_i})$

The above algorithm is the process of generating ring signcryption by the outsourcer.

(8) Define the reward transaction of crowdsourcing information as <time stamp T, $\{K_1, K_2, \cdots, K_n, K_F\}$, ACC'_{J_i}, (W_F, C) >, and broadcast the transaction to the crowdsourcing information obtaining blockchain

After receiving the award transaction broadcasted by the outsourcer, the contractor uses its long-term private key (x_{J_i}, u_{J_i}), calculates $(X'_{J_i}, D'_{J_i}) = (H_4(x_{J_i} T_{i1})P, H_4(u_{J_i} T_{i2})P)$, and compares it with the temporary public key address AC C'_{J_i} of the contractor recorded in the transaction. If it is consistent, it is determined that the crowdsourcing information provided by itself has received the reward from the

outsourcer and then performs the following steps to decrypt and verify the ring signcryption of the outsourcer:

(1) Calculate with its temporary private key

$$V_{J_i} = \left(x'_{J_i}, u'_{J_i}\right)^{-1} W_F. \tag{23}$$

(2) Restore the ring signature $X_F = H(V_{J_i}) \oplus C$

(3) Calculate $A'_i = c_i P + s_i K_i$

$$B'_i = c_i H_2(K_i) + s_i k_F H_2(K_F), \tag{24}$$

$$A'_F = c_F P + s_F K_F, \tag{25}$$

$$B'_F = c_F H_2(K_F) + s_F k_F H_2(K_F). \tag{26}$$

(4) Verify the equation

$$s_F + \sum_{i=1}^{n} s_i = H_0\left(m, A'_1, A'_2, \cdots, A'_n, A'_F, B'_1, B'_2, \cdots B'_n, B'_F\right). \tag{27}$$

Whether it is true, if so, confirm that the electronic money is the legal reward from the outsourcer for providing crowdsourcing information, otherwise, refuse it.

When the contractor uses the obtained reward for consumption, it only needs to use its temporary private key to sign m, without using its long-term private key; the payee uses the temporary public key address of the contractor recorded in the blockchain for verification. Because the temporary public key addresses of the contractor are different from each other in each crowdsourcing information transaction, the nodes in the crowdsourcing blockchain cannot link the real identity of the contractor with its consumption behaviors, thus, realizing the consumer anonymity of the contractor.

5. Privacy Protection and Efficiency Analysis of our Scheme

5.1. Privacy Protection Analysis. The crowdsourcing information obtaining scheme based on blockchain is mainly realized by the certificateless multireceiver anonymous signcryption scheme [19] and one-time pad ring signature algorithm [21] in the stage of crowdsourcing information requirements release, crowdsourcing information submission by the contractor and crowdsourcing information evaluation and reward. The security of the algorithm has been proved in detail in relevant references, so it will not be described in detail. In this paper, based on the above algorithm, the idea of temporary public key address and temporary private key is introduced to protect the identity anonymity and data privacy of the outsourcer and the contractor. The privacy protection effect of the scheme is analyzed emphatically below:

(1) *Releasing of Information Requirements*. In this stage, the outsourcer signed the blockchain address, released requirements, and reward together with the public key of the contractor, so that other nodes in the blockchain network could not know the specific information requirements and could not track the specific identity information of the outsourcers from the release of the crowdsourcing information task. In addition, in the signcryption released by the outsourcer, Lagrange interpolation polynomial is used to hide the blockchain address of each contractor, so as to prevent the blockchain address of each contractor from being exposed in the blockchain. Meanwhile, each contractor in the contractor node set only uses its private key and blockchain address information to decrypt the signcryption, and cannot use the addresses of other contractors, thus ensuring mutual anonymity among each contractor

(2) *Submission of Crowdsourcing Information by the Contractor*. In this stage, the contractor does not directly use the private key corresponding to its blockchain address to submit the collected crowdsourcing information, but the outsourcer first uses the public key of the contractor to generate the temporary public key of the contractor for this submission, and then the contractor uses the temporary private key corresponding to the temporary public key to signcrypt and transmit the collected information to the outsourcer. Because the contractor uses different temporary private keys every time, it can ensure the confidentiality of the data and prevent its identity from being exposed in the process of submitting the crowdsourcing information many times

(3) Evaluation and Reward Stage of Crowdsourcing Information. In this stage, in order to prevent the identity of the outsourcer from leaking in the process of multiple awards, the outsourcer uses a ring signcryption algorithm to sign the reward amount and then publishes the crowdsourcing information reward transaction in the blockchain. Attackers cannot associate the reward transaction with the real address of the outsourcer, and at the same time, the temporary public key address of the contractor is published in the transaction to prevent attackers from tracking its identity by using the public key address of the contractor

(4) When the contractor uses the obtained for consumption, it only needs to use its temporary private key to sign the reward m, and the payee uses the contractor's temporary public key address for verification. Because the contractor's temporary public key

Table 1: Comparison of privacy protection property.

	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	Ours
Privacy protection of outsourcer	Weak anonymity	Strong anonymity	×	×	×	Weak anonymity	Weak anonymity	Weak anonymity	Weak anonymity	×	×	Strong anonymity
Privacy protection of contractor	Weak anonymity	Weak anonymity	×	×	×	Weak anonymity	Weak anonymity	Weak anonymity	×	×	×	Strong anonymity
Privacy protection of transaction data	No protection of transaction amount	×	×	×	×	√	√	√	√	√	√	√

Table 2: Statistics of scheme's calculation cost.

	Release algorithm	Submission algorithm	Reward accounting algorithm
Outsourcer	$(k^2 + k + 2)$SM	$(4k + 3)$SM	$(2n + 3)$SM
Contractor	$(k + 2)$SM	4SM	$(2n + 3)$SM

address is different from each other in each transaction, it realizes the anonymity of the contractor's consumption

In the following, the privacy protection performance of the scheme in this paper is compared with the existing information sharing scheme based on blockchain. Here, we define the scheme that only relies on the anonymity of user's blockchain address to protect the anonymity of user's identity as satisfying weak anonymity and define the scheme that uses other special technologies to ensure the anonymity of user's identity as satisfying strong anonymity. The results are shown in Table 1. The scheme in this paper has obvious advantages over other schemes in privacy protection.

5.2. Efficiency Analysis. In this section, the calculation efficiency of this scheme is quantitatively evaluated. The calculation cost of the scheme mainly depends on the calculation amount of the outsourcer and the contractor in the release of the requirements, the submission of the information, and the reward accounting. In order to improve the calculation efficiency, the above algorithms do not use bilinear pairing operation and exponential operation on multiplication group [22], but mainly use scalar multiplication operation on elliptic curve to design. "SM" is used to represent scalar multiplication operation on elliptic curve. Table 2 shows the calculation statistics of the outsourcer and the contractor in the scheme. Because other operations (hash operation and point addition operation) consume much less time than scalar multiplication operation, they are not included in the statistics here.

Among them, the parameter k is the number of contractors in the crowdsourcing blockchain, and n is the number of public keys in the public key set in the ring signature algorithm (which is a fixed parameter). If choose a 160-bit elliptic curve group on a hypersingular curve over a 512-bit finite field based on PBC library (Version 0.5.14), one SM operation takes about 1.51 ms [23]. It can be seen from Table 2 that the calculation cost of the outsourcer in the three algorithms of crowdsourcing information obtaining scheme is $O(k^2)$, $O(k)$, and $O(1)$, which are all effective polynomial time algorithms; as a contractor with weak computing power, the computational overhead in the three algorithms is $O(k)$, $O(1)$, and $O(1)$ separately, which are all effective polynomial time algorithms with less computation, especially in the submission and reward accounting algorithms that the contractor frequently participates in.

6. Conclusion

On the basis of traditional crowdsourcing information obtaining scheme based on intermediary platform, this paper designs a crowdsourcing information obtaining scheme aiming at senior netizens based on blockchain. The scheme does not need intermediary platform, and in order to satisfy the absolute dependence of senior netizens on personal anonymity, the scheme uses the certificateless multireceiver anonymous signcryption scheme to release information requirements and rewards, so as to ensure the identity anonymity of the outsourcer and the contractor and the confidentiality of crowdsourcing information. In the submission stage, a temporary public-private key pair is generated for the contractor, and the contractor uses the temporary private key to sign and return the data to ensure the identity anonymity of the contractor in the process of submitting information for many times; in the process of reward accounting, the outsourcer uses the one-time temporary public key of the contractor to signcrypt the reward, so as to ensure the anonymity of its identity and the secrecy of the remuneration, and at the same time realize the untraceability of the consumption. Compared with the privacy protection of similar schemes, this scheme has obvious advantages.

Data Availability

The experimental data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Howe, "The rise of crowdsourcing," *Wired Magazine*, vol. 14, no. 6, pp. 1–4, 2006.

[2] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell, "A survey of mobile phone sensing," *IEEE Communications Magazine*, vol. 48, no. 9, pp. 140–150, 2010.

[3] D. B. Rawat, L. Njilla, K. Kwiat, and C. Kamhoua, "iShare: blockchain based privacy-aware multi agent information sharing games for cyber-security," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 425–431, Piscataway, NJ, March 2018.

[4] H. Kezhen, L. Yifeng, and F. Dengguo, "Cyber security threat intelligence sharing model based on blockchain," *Journal of Computer Research and Development*, vol. 57, no. 4, pp. 836–846, 2020.

[5] W. Ruijin, Y. Suzhe, L. Y. T. Yucheng, and Z. Fengli, "Medical blockchain of privacy data sharing model based on ring signature," *Journal of University of Electronic Science and Technology of China*, vol. 48, no. 6, pp. 886–892, 2019.

[6] H. Yunhua, L. Mengru, L. Hong, S. Limin, X. Ke, and Y. Chao, "A blockchain based incentive mechanism for crowdsensing applications," *Journal of Computer Research and Development*, vol. 56, no. 3, pp. 544–554, 2019.

[7] C. Yexia, F. Jun, and C. D. Yuejin, "Research on threat intelligence sharing and rating technology based on blockchain," *Information and Communications Technology and Policy*, vol. 2, pp. 19–24, 2020.

[8] C. Mingzhang, W. Lin, and W. Jiang, "Research on the application of blockchain technology in the field of internet public welfare crowdfunding," *Library and Information*, vol. 2, pp. 76–80, 2020.

[9] X. Wenyu, W. Lei, and Y. Yunxue, "Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption," *Journal of Computer Research and Development*, vol. 55, no. 10, pp. 2233–2243, 2018.

[10] S. Amofa, E. B. Sifah, K. O. -B. Obour Agyekum, S. Abla, X. Qi, C. G. James, and G. Jianbin, Eds.J. Gao, "A blockchain-based architecture framework for secure sharing of personal health data," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–6, Vitkovice, September 2018.

[11] L. Yue, H. Junqin, and Q. Shengzhi, "Big data model of security sharing based on blockchain," in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 117–121, Cheng Du, China, August 2017.

[12] M. J. M. Chowdhury, A. Colman, M. A. K. J. Han, and P. Sarda, "Blockchain as a notarization service for data sharing with personal data store," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 1330–1335, New York, USA, August 2018.

[13] F. Kai, R. Yanhui, W. Yue, L. Hui, and Y. Yingtang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *The Institution of Engineering and Technology*, vol. 12, no. 5, pp. 527–532, 2018.

[14] Q. Kang, Y. Wei, W. Lingwei, and T. Hongbo, "Data sharing scheme for 5G IoT based on blockchain," *Chinese Journal of Network and Information Security*, vol. 6, no. 4, pp. 45–55, 2020.

[15] D. Valadeolmillos, Y. Mezquita, and A. Gonzalez Briones, "Blockchain technology: a review of the current challenges of cryptocurrency," in *International congress on Blockchain and Applications*, pp. 153–160, Atlanta, USA, 2019.

[16] H. Xuan, Y. Yong, and W. FeiYue, "Security problems on blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 45, no. 1, pp. 206–225, 2019.

[17] Z. Jun, Z. Haining, and T. Yi, *Blockchain Technology Guide*, China Machine Press, Beijing, 2016.

[18] Z. Shiqin, H. Ru, H. Tao, L. Jiang, W. Shuo, and F. Wei, "Survey of blockchain: principle, progress and application," *Journal on Communications*, vol. 41, no. 1, pp. 134–151, 2020.

[19] Q. Yanlin, W. Xiaoping, and H. Wei, "Efficient certificateless multi-receiver anonymous signcryption scheme," *Journal on Communications*, vol. 37, no. 6, pp. 129–138, 2016.

[20] N. Van Saberhagen, "CryptoNote v 2.0," 2020, http://coinpaprika.com/storage/cdn/jwhitepapers/1611.pdf.

[21] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, pp. 22970–22975, 2018.

[22] MIRACL, "Multiprecision integer and rational arithmetic C/C++ library," 2020, https://indigo.ie/mscott/.

[23] D. Sheng, C. Jin, and L. Hui, "Efficient pairing-free CP-ABE based on ordered binary decision diagram," *Journal on Communications*, vol. 40, no. 12, pp. 1–8, 2019.