Hindawi
Security and Communication Networks
Volume 2021, Article ID 9992353, 10 pages
https://doi.org/10.1155/2021/9992353

Research Article

A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain

Sheng Gao,[1] **Qianqian Su**,[2] **Rui Zhang**,[2] **Jianming Zhu**,[1] **Zhiyuan Sui**,[1] **and Junsheng Wang**[3]

[1]*School of Information, Central University of Finance and Economics, Beijing 100086, China*
[2]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[3]*State Grid Blockchain Technology Laboratory, State Grid E-Commerce Co., Ltd., Beijing 100053, China*

Correspondence should be addressed to Qianqian Su; suqianqian@iie.ac.cn

Received 1 April 2021; Accepted 23 May 2021; Published 4 June 2021

Academic Editor: James Ying

Traditional identity authentication solutions mostly rely on a trusted central entity, so they cannot handle single points of failure well. In addition, most of these traditional schemes need to store a large amount of identity authentication or public key information, which makes the schemes difficult to expand and use in distributed situations. In addition, the user prefers to protect the privacy of their information during the identity verification process. Due to the open and decentralized nature of the blockchain, the existing identity verification schemes are difficult to apply well in the blockchain. To solve this problem, in this article, we propose a privacy protection identity authentication scheme based on the blockchain. The user independently generates multiple-identity information, and these identities can be used to apply for an identity certificate. Authorities use the ECDSA signature algorithm and the RSA encryption algorithm to complete the distribution of the identity certificate based on the identity information and complete the registration of identity authentication through the smart contract on the blockchain. On the one hand, it can realize the protection of real identity information; on the other hand, it can avoid the storage overhead caused by the need to store a large number of certificates or key pairs. Due to the use of the blockchain, there is no single point of failure in the authentication process, and it can be applied to distributed scenarios. The security and performance analysis show that the proposed scheme can meet security requirements and is feasible.

1. Introduction

Nowadays, in the Internet of Things (IoT) environment, a massive quantity of devices and sensors can feel each other through the internet to share and process data [1–3]. Users have lost control of sensitive data, which has caused concerns about data security to become one of the main obstacles to data sharing between parties [4, 5]. Take e-health systems as an example; with the popularity of wearable medical equipment, the application of the e-health system has obtained widespread attention and is constantly changing our living habits [6–8]. Through the e-health system, doctors can analyze the patient's physique data obtained by sensors in real time, realize the research on the effect of drugs, or provide patients with better medical care. In these scenarios, wearable medical sensors can obtain parameters related to the patient's health, such as blood pressure, heart rate, and body temperature. Through the internet, the collected health data are transmitted to the doctors. Internet-based medical treatment enables doctors to treat patients no longer limited to geographic locations, which not only reduces medical costs but also saves treatment time. Even if the patient is located in a remote area, doctors can monitor the patient's health in real time through the transmitted data and give targeted treatment plans.

In this scenario, the patient's medical data are an important information resource containing a large amount of sensitive information, which can be in the form of signals,

text, voice data, images, etc. This information needs to be effectively protected. However, since medical systems are vulnerable to cyberattacks, sharing sensitive patient information in an IoT environment may cause a series of serious security and privacy issues. For example, if the third party who obtains the information does not use the data as agreed, but instead sells or uses other forms of data abuse; this will pose a severe challenge to the privacy and safety of patients. In order to ensure that patients' data are not used by unauthorized people in the smart medical environment, an effective identity management solution must be used. Firstly, the amount of data generated by sensors in real-time medical treatment is very large, and the data formats are heterogeneous. Therefore, for terminals with limited processing capabilities, it is not feasible to encrypt data before transmitting the data. Secondly, since terminals often have limited storage capacity, it is not feasible to use existing identity management and verification methods that require storing a large number of key pairs. In addition, most of the existing solutions rely on a trusted third party to implement identity management and authentication, which not only leads to the potential danger of a single point of failure but also makes users lose control of their own identity information.

Recently, as a decentralized technology, blockchain [9–11] provides a feasible solution to ensure the data integrity. The advantage of blockchain technology is that, through the consensus mechanism, the distributed storage of medical data can be realized, and the modification or deletion of the data of a few participants will not affect other participants. It is an interesting idea to use blockchain to solve the problem of relying on trusted third parties in traditional identity authentication. For the key management [12] and user identity authentication [13], it is also necessary to resolve user anonymity, verifiability, and nonrepudiation [14–16].

In this paper, we propose a blockchain-based identity authentication scheme, which can realize anonymous user identity authentication and identity management without a lot of storage space. The main contributions of this paper can be summarized as follows:

(i) We propose a blockchain-based identity authentication scheme. By introducing the blockchain, users will generate their own identities and generate publicly verifiable information for those identities. Users store public information on the blockchain, thus solving the problem of relying on third parties to manage identity information. Users do not need to maintain a database of publicly verified information and can realize identity authentication by querying the blockchain, which saves the time delay of waiting for block confirmation. Therefore, during the identity authentication process, there is no need to rely on a trusted third party, and there is no need for users to store the identity information of other users.

(ii) The identity authentication scheme we proposed can support privacy preservation, including communication privacy protection and user identity privacy protection. By using the ECDSA signature scheme, the verifiability and unforgeability of the identity verification process are ensured. The communication process is encrypted by the RSA encryption algorithm to ensure the security of communication. In addition, the user can generate multiple identities, and the corresponding public information is not related, so the user's identity privacy can be effectively protected.

(iii) Our analysis and comparison proved that the proposed identity authentication scheme meets the security requirements, and the feasibility of the scheme was proved through simulation experiments.

1.1. Related Work. Traditional identity management solutions often rely on a centralized trusted third party [17, 18], where users' personally identifying information is controlled by an organization rather than the user himself/herself. This means that the third party has complete control over the user's information. Third-party entities may leak user information due to software vulnerabilities, hardware damage, and economic benefits. In addition, a centralized system inevitably brings a single point of failure problem, and due to the limited capacity of a single node, it is difficult to achieve effective identity authentication when the system user is very large, that is, it lacks scalability.

In order to solve the centralization problem, some studies have proposed federated identity management [15, 19, 20]. Allow users to log in to the system with the same identity in multiple different scenarios. Although this solution avoids the storage of a large amount of identity information to some extent, the user's identity is still controlled and managed by the joint service provider. At the same time, there have been many proposed schemes to help meet user privacy protection requirements [21–24]. They focus on user-centric identity management, enabling users to selectively authorize personal data under various conditions and display credentials provided in response to authentication requests.

Recently, some researchers have introduced blockchain technology into identity authentication [25–27]. In [15], the authors proposed a blockchain-based identity management and authentication scheme for mobile networks, where users' identifying information is controlled by the users themselves. In [13], the authors proposed a blockchain-based multi-WSN authentication scheme for IoT. In their scheme, the nodes of IoT are divided into base stations, cluster head nodes, and ordinary nodes according to capability, which are formed to a hierarchical network. A blockchain network is constructed among different types of nodes to form a hybrid blockchain model, including local chain and public chain. In this hybrid model, nodes' identity mutual authentication in various communication scenarios is realized, ordinary node identity authentication operation is accomplished by the local blockchain, and cluster head

node identity authentication is realized in the public blockchain. In [28], the authors proposed a new EHR paradigm which can help in dealing with the centralized problem of cloud-based EHRs. After that, they proposed an authentication scheme for blockchain-based EHRs. The proposed scheme is an identity-based signature scheme with multiple authorities which can resist the collusion attack out of N from $N-1$ authorities. In [29], the authors presented a permissioned blockchain-based identity management and user authentication (PBBIMUA) scheme for the e-health environment. The proposed scheme satisfies the security requirements of medical data.

It can be seen that the existing blockchain-based identity authentication schemes can be divided into two categories according to their application scenarios: multidomain and single domain. Among the multidomain authentication schemes, the existing schemes are difficult to solve the cross-domain system compatibility issues and the privacy security issues between different domains. In the single-domain authentication scheme, most of the information used for authentication is stored in the blockchain in plaintext messages. However, in the process of identity management and authentication, the openness and immutability of the blockchain will inevitably bring security risks and difficulties in changing identity information.

2. Preliminaries

In this section, we illustrate background knowledge used in this paper, including the definition of discrete logarithm and its security assumptions, chameleon hash algorithm, and description of the verifiable claim.

2.1. Blockchain. Blockchain [30] is a distributed hyperledger with irreversibility and traceability. Generally, the blockchain integrates various technologies such as cryptographic algorithms, P2P communication, consensus, and smart contracts and can establish trust relationships without a special trust relationship between peers and no trusted central authority. Cryptographic algorithms, such as hash functions and signature algorithms, can guarantee the integrity and unforgeability of information. P2P technology can realize point-to-point communication between nodes. The consensus mechanism (such as PoW, PoS, and DPos) is the core of the blockchain. The nodes participating in the consensus in the blockchain system are called miners. They are responsible for packaging the transaction data in the system into a block and obtain the accounting rights by participating in the consensus, thereby recording the block on the blockchain.

2.2. Elliptic Curve Digital Signature Algorithm. Elliptic Curve Digital Signature Algorithm (ECDSA) [31] is used to create a digital signature of the data (a file, for example) in order to allow one to verify their authenticity without compromising their security. We use Sign and Verify to represent the signing process and the verification process in ECDSA, respectively.

The signing process is as follows:

(1) Choose an elliptic curve $E_p(a,b)$ and the base point G

(2) Select the private key k ($k<n$, n is the order of G), and use the base point G to calculate the public key $K=kG$

(3) Generate a random integer r ($r<n$), and calculate the point $R=rG$

(4) Take the original data m and the coordinate values x, y of point R as parameters, and calculate $h=\mathrm{Hash}(m,x,y)$

(5) Calculate $s=r-h*k \bmod n$

(6) As the signature value, r and s, if one of r and s is 0, restart from Step 3

The verification process is as follows. After receiving the message m and signature value (r,s), the recipient performs the following operations:

(1) Calculation: $sG+H(m)P=(x_1,y_1)$ and $r_1=x_1 \bmod p$

(2) Verify the equation: $r_1=r \bmod p$

(3) If the equation holds, accept the signature; otherwise, the signature is invalid

2.3. RSA Encryption. RSA encryption algorithm [32, 33] is an asymmetric key encryption algorithm. The encryption key (i.e., public key) PK is public information, and the decryption key (i.e., secret key) SK needs to be kept secret. The encryption algorithm Enc and the decryption algorithm Dec are also public.

The specific description of the RSA algorithm is as follows:

(1) Choose two different large prime numbers p and q to calculate the product $n=pq$, $\varphi(n)=(p-1)(q-1)$

(2) Choose a large integer e arbitrarily and satisfy $\gcd(e,\varphi(n))=1$, and the integer e is used as the encryption key

(3) The determined solution key d satisfies $e\ d=1 \bmod \varphi(n)$

(4) The integers n and e are disclosed, and d is kept secret

(5) Encrypt the plaintext m ($m<n$ is an integer) into ciphertext c; the encryption algorithm is $c=\mathrm{Enc}(e,m)=m^e \bmod n$

(6) Decrypt ciphertext c into plaintext m; the decryption algorithm is $m=\mathrm{Dec}(d,c)=c^d \bmod n$

3. System Model

As shown in Figure 1, in the system model, we assume a blockchain network in which each member holds a related distributed ledger. The network systems are formed with the data owner (DO) and the data user (DU). In the e-health system, data owners are generally patients with wearable medical equipment, and data users are doctors

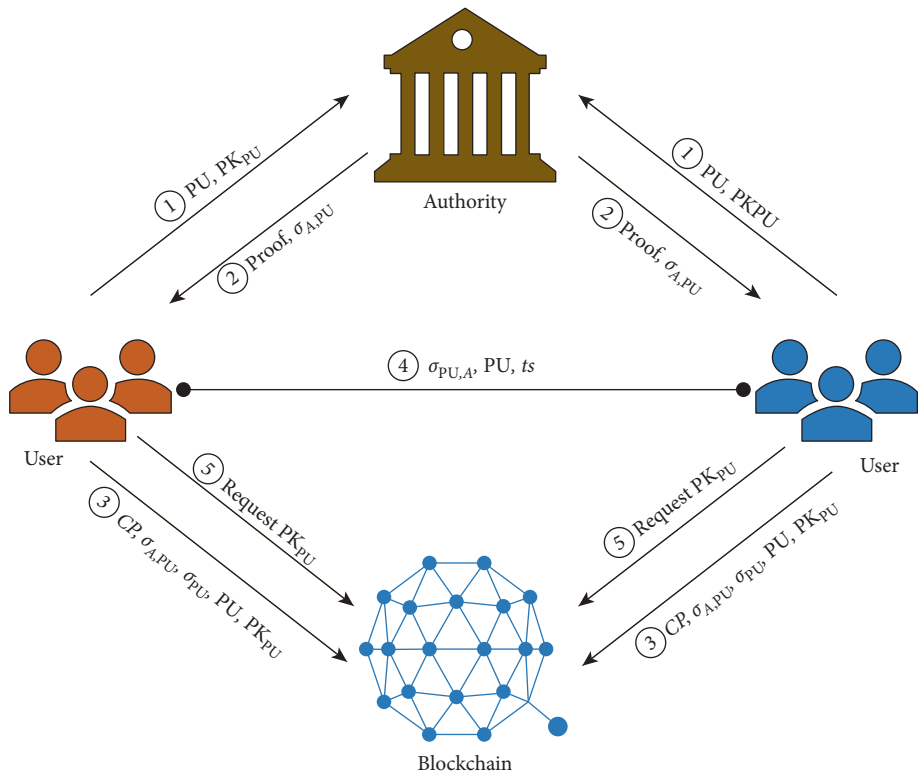

Figure 1: System model.

who provide medical assistance to patients. Users establish a blockchain network maintained by miners. Authority is responsible for the registration of users and providing the proof of their valid identity. The responsibility of the miner is to check the user's identity information and add this information to the blockchain as a transaction for mining user enrolment requests. After successful execution of the process, users can complete the authentication process by accessing the blockchain.

(i) User: the user realizes its own identity control and management by generating its own identity identification (PU) and its corresponding public and private keys. The user can have multiple independent PUs at the same time and store PUs and public and private keys locally. Only when necessary, the PU and public key are disclosed to other users. According to different roles, users can be divided into data owners (DO, such as patients) and data users (DU, such as doctors).

(ii) Authority: the authority is an entity that distributes certificates to users (Steps ① and ②), such as governments or medical management agencies. The certificate distributed to users contains the signature of the authorities and can be verified by other users. It is worth pointing out that although the authority distributes certificates to users, the authority does not participate in the verification process in the process of performing identity authentication (Step ④).

(iii) Blockchain: It is a consortium blockchain maintained by miners for publishing users' PU and public keys (Step ③). The miner is the execution node of the packaged transaction mining block in the blockchain. It verifies the signature of the transaction and stores the verified transaction on the blockchain. Any entity can read the information on the blockchain (Step ⑤).

4. The Proposed Identity Authentication Scheme

In this section, we first give the overview of our proposed privacy-preserving identity authentication scheme. In the following, we provide a detailed description of our scheme, which mainly consists of three phases: initialization, registration, and authentication.

4.1. Overview. In the privacy-preserving identity authentication scheme, the user independently generates their identity information (PU) and corresponding public and private key pairs (PK, SK). Before implementing the authentication process, the user should send PU and PK to the authority for registration in order to obtain a valid identity proof ($\mathcal{PF}$). It is worth noting that the user can generate several different (PU, PK, SK) certifications by different authorities to obtain multiple verifiable proofs. In order to achieve the authentication process, the user sends the publicly verifiable identity proof generated by the authority and the corresponding public information to the blockchain

network in the form of a transaction. The transaction is finally added to the blockchain. After that, the user in the system can query other users' public information through the blockchain and verify the user's identity. After the authentication is completed, the users can negotiate a session key through shared secret parameters to ensure the privacy of subsequent session information.

4.2. Details of the Proposed Scheme. Next, we divided the proposed system into three phases which are described in detail, namely, initialization phase, registration phase, and authentication phase. The overall process of authentication is shown in Figure 2.

4.2.1. Phase 1: Initialization. The initialization phase can be divided into two parts. One part is the authorities and the blockchain network initialization. The other part is the user initialization. Initially, the users and the authorities initialize the system, and the system constructs a permissioned blockchain network, where users (DO and DU) are the participant and the miners are the maintainer of the blockchain. The users write transactions in order to provide identity authentication function. The miners verify the transactions in order to provide valid information for identity authentication. Specifically, the users and the authorities establish a consortium blockchain, and the miners who maintain the blockchain network rely on a practical Byzantine fault tolerance (PBFT) consensus mechanism. They execute the following operations to initialize a series of system parameters:

(1) For two large primes p, q and an elliptic curve E_p, there is a nonregular elliptic curve additive cyclic group G of order q and a generator P of G. Choose SHA256 as the encryption hash function H, elliptic curve digital signature algorithm (ECDSA) as the signature algorithm Sig, and RSA encryption algorithm as the asymmetric encryption algorithm Enc.

(2) The identity of the authority is marked as $\text{AuthorityID}(A_i)$. The authority A_i generates public and private key pairs $(\text{PK}_{A_i}, \text{SK}_{A_i})$. Then, A_i publishes PK_{A_i} to the users in the system and the miner in the blockchain network.

(3) The identity of the user is marked as $\text{UserID}(U_i)$. The user U_i generates its own pseudo-identity PU_i and calculates PK_{PU_i} by choosing a secret key SK_{PU_i}. Then, PU_i pushes PK_{PU_i} to the other users in the system and the miners in the blockchain network.

(4) The users write a smart contract (SC) in order to provide the registration function, in which public and private key pairs are PK_{SC} and SK_{BC}.

(5) The public parameters can be represented as $(G, g, H, \text{Sig}, \text{Enc}, \text{PK}_{A_i}, \text{PK}_{\text{PU}_i}, \text{PK}_{\text{BC}})$.

4.2.2. Phase 2: Registration

(1) The user U_i sends $(\text{PU}_i, \text{PK}_{\text{PU}_i})$ to A_i through a secure channel.

(2) Upon receiving the user's message, A_i firstly verifies $(\text{PU}_i, \text{PK}_{\text{PU}_i})$. If PU_i has already been registered or it is invalid, PU_i rejects the request. Otherwise, A_i generates a verifiable proof $\mathscr{PF}_{A_i,\text{PU}_i}$ and its signature $\sigma_{A_i,\text{PU}_i} = \text{Sig}(\text{SK}_{A_i}, (H(\text{PU}_i), \text{PK}_{\text{PU}_i}, \mathscr{PF}_{A_i,\text{PU}_i}, \text{VT}))$ for PU_i, where VT is the valid time of the proof. Then, A_i sends $(\text{PU}_i, \text{PK}_{\text{PU}_i}, \mathscr{PF}_{A_i,\text{PU}_i}, \text{VT}, \sigma_{A_i,\text{PU}_i})$ to the user U_i through a secure channel.

(3) Upon receiving σ_{A_i,PU_i} from A_i, the user U_i sends the public information to the blockchain. Firstly, U_i generates a timestamp ts_r and then computes $\text{CP} = \text{Enc}(\text{PK}_{\text{BC}}, (\mathscr{PF}, \text{VT}))$ and signature $\sigma_{\text{FU}_i,R} = \text{Sig}(\text{SK}_{\text{PU}_i}, (H(\text{ts}_r), \mathscr{PF}_{A_i,\text{PU}_i}, \text{VT}, \sigma_{A_i,\text{PU}_i}))$. Finally, the user sends $(\text{PU}_i, \text{PK}_{\text{PU}_i}, \text{ts}_r, \text{CP}, \sigma_{A_i,\text{PU}_i}, \sigma_{\text{PU}_i,R})$ to the blockchain network.

(4) Upon receiving the message from PU_i, the miner verifies whether the timestamp ts_r is within the allowed range compared to the current time. If not, miner rejects the transaction; otherwise, miner continues to check whether the lifetime VT is within the allowed time. If not, miner stops the session. Otherwise, miner decrypts CP to get the proof and verifies the signature σ_{A_i,PU_i}. If the signature is valid, miner writes this transaction to the blockchain. The user can generate several PU_i and corresponding public and private keys to obtain verifiable proofs of different authorities and store them locally.

4.2.3. Phase 3: Authentication. After a user's PU_i and public key are added to the blockchain, the detailed authentication process is as follows:

(1) User U_i with identity PU_i first generates random value r and timestamp ts_a and computes signature $\sigma_{\text{PU}_i,A} = \text{Sig}(\text{SK}_{\text{PU}_i}, H(\text{PU}_i, r, \text{ts}_a))$. Then, U_i sends $(\text{PU}_i, r, \text{ts}_a, \sigma_{\text{PU}_i,A})$ to user U_j.

(2) Upon receiving the message from U_i, U_j first verifies the timestamp and the signature. If ts_a is not within the allowed range compared to the current time or the signature is invalid, U_j rejects the access request; otherwise, U_j searches for PK_{PU_i} on the blockchain with PU_i. If there is no PK_{PU_i}, U_j rejects the access request. Otherwise, U_j verifies the signature $\sigma_{\text{PU}_i,A}$ with PK_{PU_i}. If $\sigma_{\text{PU}_i,A}$ is invalid, U_j stops the session; otherwise, the user's identity is verified.

5. Security and Performance Analysis

5.1. Security Analysis. In this section, we first compare the proposed scheme with four other representative authentication schemes in terms of authentication, privacy preservation, scalability, and centralized trusted authority. Then, we introduce the security requirements and give the corresponding analysis.

The security requirements mainly include integrity, availability, scalability, nonrepudiation, identity authentication, and communication security. In addition, we

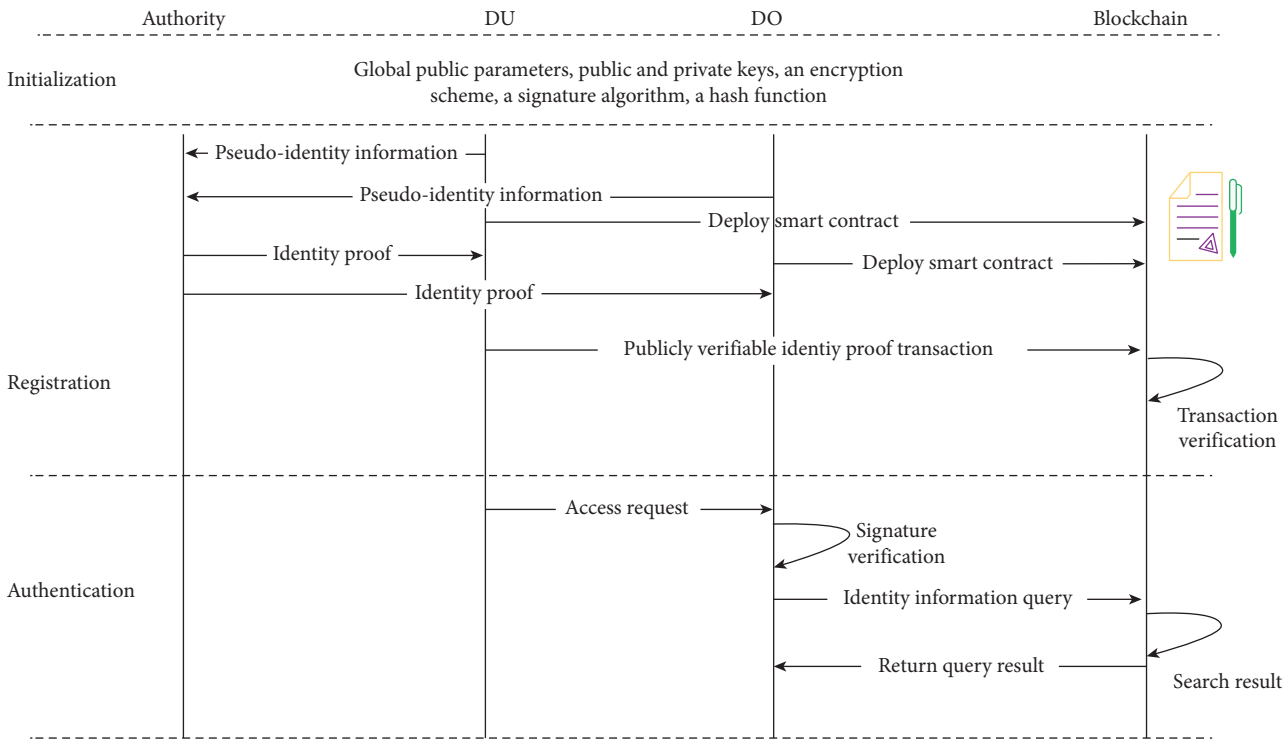

Figure 2: The process of authentication.

compared the solution with the existing blockchain-based solutions in a comprehensive function. The comparison results are shown in Table 1. It can be seen from the table that our scheme not only supports identity anonymity, authentication, nonrepudiation, scalability, and decentralized functions but also has more advantages in privacy protection and communication security. In particular, the proposed scheme does not need to wait for the block confirmation and cross-blockchain operations during the authentication process.

Table 1: Security features' comparison.

Features	[34]	[35]	[36]	[13]	[21]	Our
Identity anonymity	√	√	√	√	√	√
Authentication	√	√	√	√	√	√
Nonrepudiation	√	√	√	√	√	√
Privacy preservation	√	√	×	×	×	√
Scalability	—	—	√	√	√	√
Decentralized	—	—	√	√	√	√
Cross-blockchain	—	—	×	√	×	×
Blockchain confirmation	—	—	√	√	√	×

(i) Identity anonymity: identity anonymity means that other users cannot obtain the user's true information through the user's access request. In the proposed scheme, the user completes the identity registration by generating the identity information PU_i independently and uploads the corresponding valid proof to the blockchain network. First, the user can have multiple PU_i information independent of the real identity, and the PU_i information is also independent of each other. Secondly, in the process of performing authentication, users also use PU_i information independent of identity information, so the validity of user identity can be guaranteed.

(ii) Authentication: authentication means that two users need to be identified before they interact. The authentication scheme proposed in this paper is the identity information generated by the user independently, and the registration of the identity and the disclosure of the effective proof are completed by the blockchain network, that is, the effective proof is stored in the blockchain network. The authenticating party can identify the authenticated party by accessing the blockchain and realize identity authentication.

(iii) Integrity: the security requirements for integrity mainly include two aspects: data integrity and message integrity. Data integrity means that unauthorized users and devices cannot access and modify the data. Message integrity means that the message sent by the user and the device cannot be tampered with illegally during the interaction. The authentication process of this scheme is realized with the help of the blockchain. The core of the verification is that the user transmits the valid identity certificate to the blockchain network and stores it in the form of a transaction. In the blockchain network, every transaction will be verified by miners, so the integrity of the message can be guaranteed. In the proposed scheme, the user's data are stored on the blockchain network.

Once the verified data are stored, it will be difficult to be tampered with, so the data integrity can be effectively guaranteed.

(iv) Nonrepudiation: nonrepudiation means that users and devices cannot reject the operations they have implemented and the messages they send. Since the scheme is carried out through the blockchain, all operations are stored in the blockchain in the form of transaction records, and all access requests and transactions are signed; therefore, the scheme is undeniable.

(v) Scalability: scalability is one of the important security requirements of blockchain identity authentication. Due to the time delay characteristics of the blockchain, if users frequently complete identity authentication through transactions, it will consume a lot of resources and time. In the scheme designed in this paper, users only need to complete the corresponding proof data on the blockchain during the registration phase. In the identity authentication phase, there is no need to wait for block confirmation, and there is only a need to search the data on the blockchain to complete the identity authentication. For scalability requirements, this solution can be well adapted.

(vi) Privacy preservation: privacy protection mainly refers to the privacy and security of the user data and identity in the storage process. In the schemes in [13, 21, 36], the authority can know the identity of the user during the registration phase, and then the authority will store the information on the blockchain. In addition, the identity identifier used in the above solution is the unique identity of the device/user. This results in that the user's identity information is stored in the blockchain in the plaintext, which will result in the user's identity information not being protected during the communication process, and it also faces the security risks of the storage process. Different from using unique identities to achieve authentication, users in our solution can create multiple independent identities according to their needs. Although the authority can still know the user's identity, the user can hash the identity information and independently decide whether to store the information on the blockchain. In addition, when storing, the message is encrypted by an encryption algorithm, so the proposed scheme has more advantages in privacy protection. Therefore, the proposed scheme can more comprehensively realize privacy protection.

(vii) Communication security: communication security refers to the security of the user's communication data during the identity authentication process. In the scheme proposed in [13, 36], the certification information used for authentication not only contains the unique identities of the authenticated parties but is also transmitted in the blockchain network in the form of a plaintext. In the scheme proposed in [21], the security of communication is achieved by establishing a blockchain-level bubble, which can be seen as establishing a safe environmental space. Different from the method in the above schemes, the communication security in the proposed scheme is realized by cryptography methods. In the registration stage, the user uses public key information to register, and then when transmitting the identity certificate, the method of symmetric data encryption is used to ensure the security of data transmission. In the authentication process, on the one hand, the user does not need to send a complete certificate. On the other hand, the identity identifier used in the authentication is not unique. Therefore, the proposed scheme has obvious advantages in communication security.

(viii) Cross-blockchain: cross-blockchain authentication refers to whether a hybrid blockchain combining a private blockchain and a public blockchain is used in the process of implementing the authentication scheme. For different blockchains, each individual blockchain network is a relatively independent network. The block structure and the deployment of the consensus mechanism may be different, data information is difficult to interconnect and synchronize, and there is a problem of information islands. This makes it difficult to collaborate between different blockchain networks and greatly limits the development of blockchain applications. Therefore, avoiding the use of hybrid blockchains to complete identity verification and avoiding cross-domain identity verification are also issues that need to be considered. Different from the cross-blockchain identity authentication scheme designed in scheme [13], the proposed scheme in this article, only a single blockchain is used to record the credential information, thereby avoiding the security risks caused by cross-chain authentication.

(ix) Block confirmation: block confirmation refers to whether it is necessary to wait for a transaction during the identity authentication process. In the scheme proposed in [13, 36], the identity authentication process needs to invoke the smart contract in the blockchain, so it needs to wait for the execution of the smart contract and the confirmation of the relevant block, but in this proposed scheme, the verifier only needs to search the blockchain once to complete the identity verification without waiting for the confirmation of the transaction block. In terms of time cost, the authentication time of using smart contracts depends on the time to reach consensus in the blockchain. In the proposed scheme, the authentication time mainly depends on the search time for related information.

5.2. Performance Evaluation. In this section, we conduct experiments to evaluate the effectiveness and feasibility of our scheme. We employ the related cryptographic opera-

Table 2: Parameter definitions.

Symbol	Description	Size
G	Bit length of an element in G	512
PU_i	Bit length of an identity	256
ts	Bit length of a timestamp	32
r	Bit length of a random number	256
h	Bit length of a hash function	256
σ	Bit length of a signature	1024
$\mathscr{PF}$	Bit length of a proof	1024

tions in the C/C++ OPENSSL library [37]; the parameters used are shown in Table 2.

The complex calculations and large-capacity storage required in the authentication process are placed on the blockchain. In order to realize user identity authentication based on the blockchain, a valid and public identity proof is stored on the blockchain. In this part, we mainly analyze the performance of the registration process and the identity authentication process. Since there are few existing blockchain-based identity authentication schemes, starting from the core idea of the scheme, the feasibility of the scheme is analyzed by analyzing the calculation cost, the communication cost, and the storage cost of each process in the scheme.

In the registration phase, the user first sends a request message to the authority. After receiving the proof returned by the authority, the user sends a registration transaction to the blockchain network. From the user's point of view, it is necessary to execute the signature generation algorithm twice, the verification algorithm once, and the encryption algorithm once. Besides, the user needs to store the proof returned by A_i and the pseudo-identity information (PU_i) generated by himself. From the authority perspective, the signature generation algorithm needs to be executed once. For miners on the blockchain, it is necessary to execute the signature verification algorithm twice and the decryption algorithm once.

In the identity authentication phase, the user U_i first sends a request to the verifier U_j. After the verifier U_j completes the message integrity check, it visits the blockchain network and completes the identity authentication by querying whether valid identity information exists. It needs to be pointed out that, at this stage, the verifier U_j does not need to store any U_i's information, which reduces a lot of storage overhead for the verifier. Therefore, at this stage, the access requester U_i needs to execute a signature algorithm; the verifier U_j needs to execute a verification algorithm and a blockchain search request. The search process here can be implemented by miners or corresponding smart contracts.

In order to show the performance of the solution more intuitively, the communication cost and the calculation cost at different phases are shown in Figures 3 and 4, respectively. Through the above analysis, this solution meets expectations and is feasible in terms of computing and storage overhead.

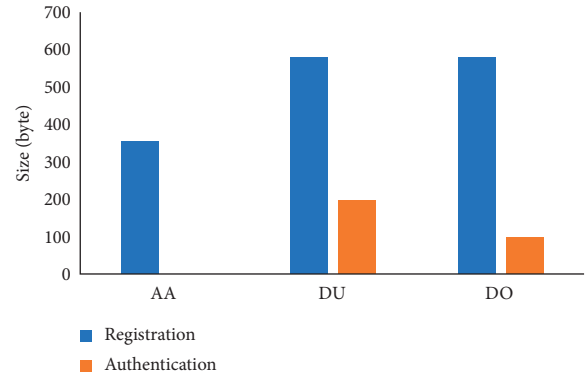

Figure 3: Communication cost.

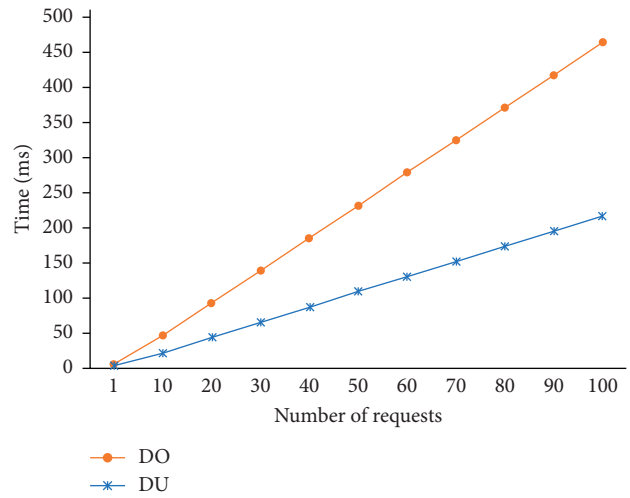

Figure 4: Calculation cost.

6. Conclusion

In this article, an identity authentication scheme based on blockchain-based privacy protection is proposed. The user generates identity information independently and completes the registration of identity certification through the blockchain. On the one hand, it can realize the protection of real identity information; on the other hand, it can avoid the storage overhead caused by the need to store a large number of certificates or key pairs. Due to the use of blockchain, there is no single point of failure in the authentication process, and it can be applied to distributed scenarios. Finally, the security analysis and performance evaluation demonstrate that the proposed scheme can meet the security requirements and is feasible.

Data Availability

The parameter 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.

Acknowledgments

This research was supported by the National Key R&D Program of China (Grant no. 2017YFB1400700), the National Natural Science Foundation of China (Grant no. 62072487), the Natural Science Foundation of Beijing (Grant no. M21036), and the National Statistical Science Foundation of China (Grant no. 2020LD01).

References

[1] N. Kumar, D. Acharya, and D. Lohani, "An IoT-based vehicle accident detection and classification system using sensor fusion," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 869–880, 2020.

[2] Y. Zhao, J. Zhao, L. Jiang et al., "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2020.

[3] Y. Liu, X. Ma, L. Shu et al., "Internet of Things for noise mapping in smart cities: state of the art and future directions," *IEEE Network*, vol. 34, no. 4, pp. 112–118, 2020.

[4] J. Xiong, R. Bi, M. Zhao, J. Guo, and Q. Yang, "Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 24–30, 2020.

[5] J. Xiong, J. Ren, L. Chen et al., "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1530–1540, 2019.

[6] F. Alshehri and G. Muhammad, "A comprehensive survey of the Internet of Things (IoT) and ai-based smart healthcare," *IEEE Access*, vol. 9, pp. 3660–3678, 2020.

[7] K. Monteiro, E. Rocha, E. Silva, G. L. Santos, W. Santos, and P. T. Endo, "Developing an e-health system based on IoT, fog and cloud computing," in *Proceedings of the 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)*, pp. 17-18, Zurich, Switzerland, December 2018.

[8] M. Elhoseny, G. Ramirez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[9] M. B. Mollah, J. Zhao, D. Niyato et al., "Blockchain for future smart grid: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, pp. 1–26, 2020.

[10] Z. Chen, Y. Tian, and C. Peng, "An incentive-compatible rational secret sharing scheme using blockchain and smart contract," *Science China Information Sciences*, vol. 64, no. 10, pp. 1–21, 2021.

[11] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17 545–17 556, 2018.

[12] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6193–6202, 2020.

[13] Z. Cui, F. Xue, S. Zhang et al., "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[14] J. Xiong, R. Ma, L. Chen et al., "A personalized privacy protection framework for mobile crowdsensing in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4231–4241, 2020.

[15] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6688–6698, 2020.

[16] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2792–2801, 2019.

[17] F. Wu, X. Li, A. Sangaiah et al., "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 82, p. 9, 2017.

[18] Z. Liu, Z. Liu, L. Zhang, and X. Lin, "MARP: a distributed mac layer attack resistant pseudonym scheme for VANET," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 4, pp. 869–882, 2020.

[19] U. Premarathne, I. Khalil, Z. Tari, and A. Zomaya, "Cloud-based utility service framework for trust negotiations using federated identity management," *IEEE Transactions on Cloud Computing*, vol. 5, no. 2, pp. 290–302, 2015.

[20] G. Bendiab, S. Shiaeles, S. Boucherkha, and B. Ghita, "FCMDT: a novel fuzzy cognitive maps dynamic trust model for cloud federated identity management," *Computers and Security*, vol. 86, pp. 270–290, 2019.

[21] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: a decentralized blockchain-based authentication system for IoT," *Computers and Security*, vol. 78, pp. 126–142, 2018.

[22] Q. Lai, L. Xu, M. Yuan, F. Wang, and H. Fang, "User privacy-preserving scheme based on anonymous authentication in smart grid," in *Proceedings of the International Conference on Security and Privacy in Digital Economy*, pp. 676–691, Quzhou, China, October 2020.

[23] A. K. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 37, no. 3, p. 9948, 2013.

[24] C. B. Avoussoukpo, C. Xu, and M. Tchenagnon, "Ensuring users privacy and mutual authentication in opportunistic networks: a survey," *International Journal of Network Security*, vol. 22, pp. 118–125, 2019.

[25] M. Wagner and B. McMillin, "An efficient blockchain authentication scheme for vehicular ad-hoc networks," in *Proceedings of the International Conference on Critical Infrastructure Protection*, pp. 87–109, Arlington National, VA, USA, 2020.

[26] A. Mohsin, A. Zaidan, B. Bahaa et al., "Blockchain authentication of network applications: taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Computer Standards and Interfaces*, vol. 64, pp. 41–60, 2019.

[27] W. A. Ali, N. M. Sahib, and J. Waleed, "Preservation authentication and authorization on blockchain," in *Proceedings of the 2019 2nd International Conference on Engineering Technology and its Applications (IICETA)*, pp. 83–88, Al-Najef, Iraq, August 2019.

[28] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41 678–41 689, 2019.

[29] X. Xiang, M. Wang, and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for e-health systems," *IEEE Access*, vol. 8, pp. 171 771–171 783, 2020.

[30] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 858–880, 2019.

[31] Z. Wu, R. Liu, and H. Cao, "ECDSA-based message authentication scheme for BeiDou-II navigation satellite system," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 4, pp. 1666–1682, 2018.

[32] K. Balasubramanian, "Variants of RSA and their cryptanalysis," in *Proceedings of the 2014 International Conference on Communication and Network Technologies*, pp. 145–149, Hefei, China, July 2014.

[33] F. Mallouli, A. Hellal, N. Sharief Saeed, and F. Abdulraheem Alzahrani, "A survey on cryptography: comparative study between RSA vs ECC Algorithms, and RSA vs El-Gamal algorithms," in *Proceedings of the 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 173–176, Paris, France, 2019.

[34] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[35] C. Chang and H. Tsai, "An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3346–3353, 2010.

[36] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–8, Aqaba, Jordan, October 2018.

[37] M. I. Mihailescu and S. L. Nita, *Cryptography Libraries in C/C++20*, Apress, Berkeley, CA, USA, 2021.