2020 16th International Conference on Mobility, Sensing and Networking (MSN) | 978-1-7281-9916-0/20/$31.00 ©2020 IEEE | DOI: 10.1109/MSN50589.2020.00031

BIA: A Blockchain-based Identity Authorization Mechanism

Xiaodong Ren*, Feilong Lin*✉, Zhongyu Chen*, Changbing Tang†, Zhonglong Zheng*, Minglu Li*
*College of Mathematics and Computer Science, Zhejiang Normal University, Zhejiang, P. R. China
†College of Physics and Electronic Information Engineering, Zhejiang Normal University, Zhejiang, P. R. China
Email: 15558698756@163.com, {bruce_lin, czy, tangcb, zhonglong, mlli}@zjnu.edu.cn

***Abstract*—The abuse of personal identity information is one of the most serious problems worldwide. Most social services or businesses use the identity authorization to confirm their validity and legality and the copies of users' identity certification are usually recorded by the service providers. It is easy to leak the users' identity information due to the untrustworthy service provider or single-point security failure, and various social problems are then caused. To deal with such problems, this paper proposes a Blockchain-based Identity Authorization mechanism (BIA). First, an Identity Authorization Module (IAM) is devised, which reads the identity certificate and transform the identity plaintext to ciphertext under the authorization by the user's identity certificate entity and password. IAM guarantees the security of identity information by keeping its plaintext off-line. Second, a Business Contract Module (BCM) is designed, which provides a general smart contract framework for identity authorization that can be adopted by most of social services or businesses. Third, a double-chain blockchain infrastructure is developed, whereby the encrypted identity information and service smart contracts are respectively recorded in the tamper-resistant, non-repudiable, and publicly verifiable way. Finally, a prototype system has been developed to verify the security, feasibility and effectiveness of the proposed BIA.**

***Index Terms*—Identity Authorization, Blockchain, Smart Contract, Security**

I. Introduction

Identity information is the basic social attribute of people, which directly or indirectly involves the personal information including home address, job, wealth, health condition, etc. Most social services or businesses require the personal identity authorization to confirm their validity and legality, e.g., banking business, health care, education, tourist accommodation etc. The copies of users' identity certifications together with the corresponding service contracts are reserved by the service providers. Such identity authorization manner remains a big security risk. The security of identity is depended on the service providers. It is easy to leak the users' identity information due to either the untrustworthy or the single-point security failure of the service providers, and causes various social problems [1, 2]. On the one hand, the copy of identity certificate can be reproduced without restriction, causing personal information to be unsafe. It is even used by criminals to conduct certain businesses without personal consent, bringing interests losing or more serious problems. On the other hand, there are also some illegal individuals who use the others information to obtain illegal benefits, but refuse to recognize the illegal behavior, which also bring obstacle and trouble to social governance. Identity security has always been the public threat worldwide but without an effective solution yet. The root of these problems is in lack of reliable record of the identity authorization. It is hard to distinguish whether the identity information was authorized by oneself or was maliciously used by others. Therefore, it is significant to establish a secure and reliable identity authorization record that can be publicly searched and verified for the security maintenance of personal information and social government.

The emerging technology blockchain, first introduced by bitcoin [3], has intrinsic advantages to deal with the secure identity authorization. Blockchain is essentially a collectively maintained data ledger by peer-to-peer network. It built a new decentralized trust without a third-party credit endorsement. In particular, with consensus protocol, the data ledger over blockchain network exhibits the features including tamper-resistant, non-repudiable, and publicly verifiable [4]. The cryptography technologies (such as public key and hash function) provide well security of users' personal identity and their transaction information. Besides, the smart contract technology [5] helps convert the traditional businesses to blockchain network and make the conduction of businesses in a transparent, traceable, and unforgeable manner. To sum up, blockchain can be used to solve the centralized services with high security risk or high service charges. For the identity authorization necessitated by broad applications as the prerequisite, blockchain has the great potential to solve its security issues.

In this paper, a blockchain-based identity authorization mechanism (BIA) is proposed, with the purpose to develop a tamper-resistant, non-repudiable, and publicly verifiable identity authorization approach to broad social services and businesses. To the best of our knowledge, this is the first work that studies the identity authorization method using blockchain technology. The innovation and contribution of this paper are summarized as follows:

- BIA constructs a decentralized identity authorization mechanism based on blockchain technology. A double-chain blockchain infrastructure is devised where the identity information and service contracts can be recorded, respectively. The identity registration sub-chain (IRC) is in charge of secure identity registration and authentication. The business proof sub-chain (BPC) provides business record with secure identity authorization.

978-1-7281-9916-0/20/$31.00 ©2020 IEEE
DOI 10.1109/MSN50589.2020.00031

- The Identity Authorization Module (IAM) is designed for identity registration and authentication. IAM reads the identity certificate and transforms the identity plaintext to ciphertext, and consequently the identity plaintext offline. The Business Contract Module (BCM) is designed, which provides a general framework of identity authorization for most social services or businesses. This paper fulfill the security and reliability of identity authentication in blockchain environment.
- The prototype of BIA is developed. In particular, the identity authorization terminal is realized by an off-the-shelf identity certificate reader with embedded OS and carried out the performance test of the prototype system. The running results on the prototype demonstrate the availability of the designed terminal as well as the feasibility and effectiveness of the proposed BIA.

The remainder of this paper is organized as follows. Sec. II simply reviews the works on blockchain technology and identity authorization. Sec. III gives an overview of the proposed BIA. The detailed design of BIA is introduced in Sec. IV. A prototype of BIA and corresponding running results are shown in Sec. V. Finally, the paper is concluded in Sec. VI.

II. Related Work

A. Blockchain Technology

Blockchain is a block-chain structure data ledger formed by storing the hash value of the previous block and logically anchoring each block [4, 6]. When the blockchain network is initialized, the first block is set as the genesis block. This genesis block defines the operating protocol of blockchain. All of the subsequent nodes joining the blockchain network follow the predefined protocol. Each node in the network maintains a blockchain ledger locally. At the same time, node obtain right to generate blocks by competing to solve a mathematical problem. The node that first solves the mathematical problem broadcasts the block to the network for verification by other nodes. After the verification is passed, the new block will be linked to the blockchain [7, 8]. Therefore, tampering with a transaction in the network requires recalculation of the mathematical difficulties of the corresponding block and all blocks after this block. Hence, the cost of attacking the network will be much higher than its benefits. The above-mentioned blockchain protocol and block data characteristics have achieved outstanding properties such as decentralization of blockchain network, non-tamperable ledger, and traceable verification of transactions.

The smart contract is a Turing-complete computer program executed automatically[9]. In a blockchain system, a smart contract has an independent address. Node activates a smart contract by sending transactions to its address. The smart contract will be processed according to the programmed business logic and finally the expected result [5]. Therefore, the smart contract running on the blockchain network is deterministic and has the general characteristics such as decentralization, transparency, trustworthiness. The proposed BIA developed several smart contracts to execute the identity authorization operations.

B. Identity Security

With the development of information technology, the security of identity has become a hot issue of widespread concern. Many efforts have been devoted to providing higher levels of personal identity security protection [10, 11].

For example, the work in [12] proposed a signature scheme based on pseudonyms, which used pseudonyms as proxy signatures to manage identity information. The work in [13] tried to protect identity information through third-party cloud service providers and token verification, but did not solve the single point of failure problem.

Some work dedicated to using blockchain technology to solve the security problem of identity information authorization. The work in [14] introduced a solution based on hybrid blockchain to solve the excessive dependence on third parties for identity authorization in traditional Multi-WSN (wireless sensor network), but there are requirements for the authorization environment. The work in [15] proposed a set of key derivation algorithms that provided anonymity and unlinkability to solve identity authorization privacy problems.

These existing works have solved the security of identity or optimization of privacy protection to a certain extent. However, most of them have not solved the problems of centralized single point failure or weak identity information authentication. Leveraging the technical advantages of blockchain, this paper aims to propose a general identity authorization mechanism that can build a decentralized, tamper-resistant, non-repudiable, and publicly verifiable recording system.

III. Overview of BIA

To deal with the secure identity authorization, a new mechanism named BIA is proposed in this paper. Leveraging blockchain technology, BIA provides a decentralized network infrastructure for identity authorization. This section presents the overview of BIA from the perspectives of system composition, work principle, and technical characteristic, respectively. The schematic architecture of BIA is shown by Fig. 1.

A. System Composition

BIA consists of three basic roles and two basic functional modules, which are presented as follows.

1) Roles: According to the participators involved in the identity authorization process in BIA, there are three kinds of roles named service provider, service requester and notary, respectively.

Service requester: The service requester who requests a service will call the corresponded service contract from BIA. After the acknowledgement of provided service items, the service requester will sign the contract with his/her identity authorization. Then, BIA will inform the service provider about service calling. After the called smart contract being further authorized by the service provider, the service requester can acknowledge that the service has been successfully invoked.

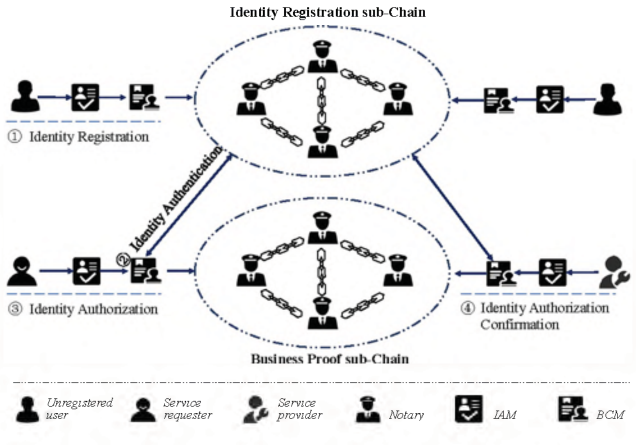

Fig. 1. Schematic architecture of BIA.

Service provider: The service provider provides some kind of business service to others. In BIA, one service is undertaken by the specific smart contract. When the service is requested (which is generally called by the service requester), service provider will check the involved service items in the contract and authenticate the identity of the service requester. If the contract is correctly called and the identity authorization from the service requester is valid, the service provider will sign the contract with his/her identity authorization. Then, the signed smart contract will be transmitted to the blockchain network for public proof.

Notary: All of the called smart contracts need to be broadcasted to the blockchain network. Notaries participate in the proof of the signed smart contracts. When one smart contract is received, the notary will examine the effectiveness of the service items and authenticate the both identity authorizations from service requester and service provider. If the service contract is correctly called and both identity authorizations are valid, the smart contract is accepted as a valid one and added to the blockchain ledger locally. When most of notaries have successfully verified the called smart contract, the proof process is considered being finished.

In BIA, a registered user can be any one of three kinds of roles which is determined by the position in the business service. There is no special restriction. Note that participates in one smart contract can be multiple, and the signing of the contract can also be extended to the multiple version easily. For concise description, the multiple-signing process is omitted here.

2) Functional Modules: The function of BIA is mainly undertaken by two functional modules, named the Identity Authorization Module (IAM) and the Business Contract Module (BCM), which are described as follows.

IAM: Functionally, IAM reads the identity information from identity certificates, e.g., typically the ID card in China, and encrypts the identity information and a key (defined and reserved by the user) to ciphertext. This function prevents the leakage of the plaintext of identity information. For high security, the RSA encryption algorithm can be used. Then, IAM generates the paired public key and private key based on the ciphertext of identity and user's key. Besides, IAM also undertakes the identity authentication before a user signs the smart contract. With the help of IAM, one can only sign a contract using the valid identity certificate and the reserved key. IAM can be solidified in to a hardware terminal, which will be introduced in Sec. V-A in detail.

BCM: BCM is in charge of the creation and management of smart contracts. Service providers can publish service contract involving detailed service items to BCM. BCM further provides a framework to package the service contract with digital signatures. Both service requester and service provider can sign the contract with digital signatures through IAM.

B. Work Process

In principle, the identity authorization process logically consists of four steps, named identity registration, identity authentication, identity authorization, and identity authorization confirmation, which are illustrated in Fig. 1 and presented in detail by Fig. 2.

Using Step 1, one can register to be a user of BIA network through IAM. IAM will output the encrypted identity information and call the identity authentication contract in BCM. After registration, the user will own an on-blockchain identity certificate recorded in the identity registration sub-blockchain (both identity registration sub-blockchain and business proof sub-blockchain will be further discussed later). When one service requester calls a service contract, Step 2 is trigged. IAM together with BCM will authenticate the identity of service requester. IAM will read the service requester's identity certificate and key, and encrypt them into cyphertext. Meanwhile, IAM will search the on-blockchain identity of the service requester by calling an identity authenticate contract in BCM and check that whether the identity certificate and key of the service requester is valid. If the identity is successfully authenticated, service requester can sign the contract with identity authorization, and which is the so-called Step 3. Step 4 is conducted by the service provider. If the service provider receives a called contract, the identity of service provider will be verified. If the verification is passed, then the service provider will confirm the service contract and authorize it using Step 2. Finally, the signed contract will be sent to the business proof sub-chain for proof.

C. Technical Characteristics

The technical characteristics of the proposed BIA can be summarized as follows. First, the IAM module is proposed, which encrypts the identity information using public key technology for identity security. IAM reads the identity certificate and transforms the identity plaintext to ciphertext under the authorization of the user's identity certificate entity and a reserved password. After reading and encryption, only the ciphertext is output from IAM and the plaintext will not be stored by IAM module. Additionally, IAM can be easily implemented by the off-the-shelf products. Second, the BCM

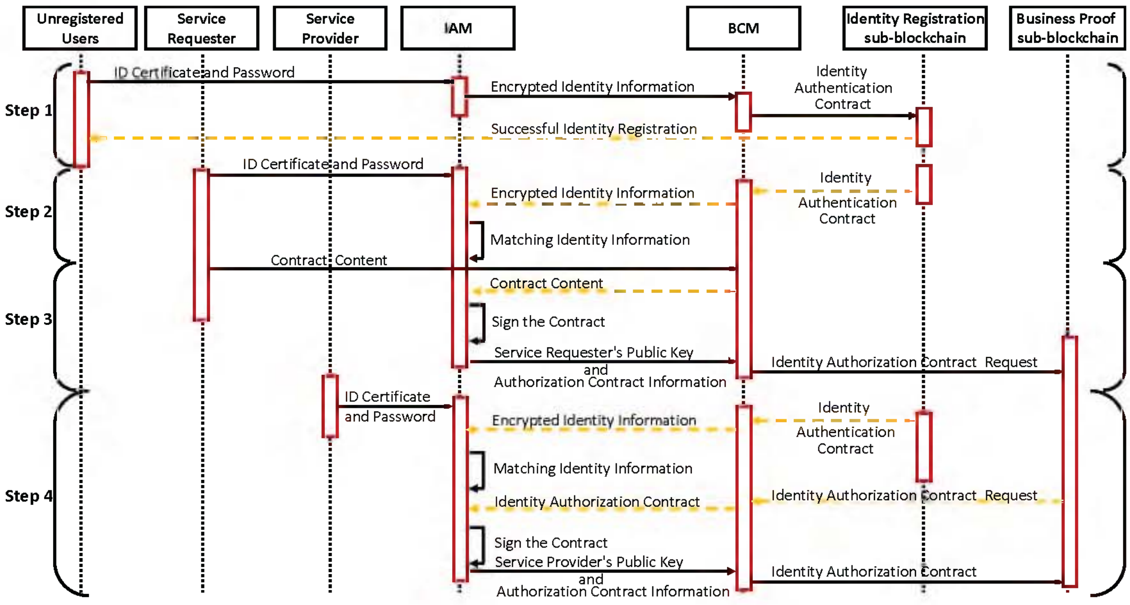
Unregistered Users
Service Requester
Service Provider
IAM
BCM
Identity Registration sub-blockchain
Business Proof sub-blockchain
Step 1
Step 2
Step 3
Step 4
ID Certificate and Password
Encrypted Identity Information
Identity Authentication Contract
Successful Identity Registration
ID Certificate and Password
Encrypted Identity Information
Identity Authentication Contract
Matching Identity Information
Contract Content
Contract Content
Sign the Contract
Service Requester's Public Key and Authorization Contract Information
Identity Authorization Contract Request
ID Certificate and Password
Encrypted Identity Information
Identity Authentication Contract
Matching Identity Information
Identity Authorization Contract
Identity Authorization Contract Request
Sign the Contract
Service Provider's Public Key and Authorization Contract Information
Identity Authorization Contract

Fig. 2. Work process of BIA

is designed, which provides a general framework for identity authorization that can be adopted by most of social services or businesses. In particular, adopted by the government, BIA has the potential to provide a social infrastructure for identity authorization protection. Moreover, the blockchain technology makes the identity authorization tamper-proof, undeniable, and publicly verifiable.

IV. Design Of BIA

In this section, the detailed design of BIA, including the double-chain infrastructure, the identity authentication contract, and the identity authorization contract, are successively introduced. The security analysis of BIA is also involved in this section.

A. Double-Chain Infrastructure

Considering the two kinds of basic requirements of identity authorization, BIA adopts a double-chain structure, which consists of the Identity Registration sub-Chain (IRC) and the Business Proof sub-Chain (BPC).

IRC: IRC undertakes the dedicated functions of on-blockchain certificate recording and identity authentication. To keep the high safety and reliability of IRC, the consortium blockchain is adopted in this work. The notaries (who have the qualification to proof identity registration and keep the ledger of IRC) are strictly appointed. For example, such as the official institutions for public affair administration or officially authorized security departments can be the notaries of IRC. Through IAM, one can register an on-blockchain and encrypted certificate on IRC and become a user of the BIA network. The IRC also provides the identity authentication for the submitted business contracts with identity authorizations. One user can only conduct the identity authorization when his/her identity certificate and key (input by IAM) correctly match to the registered on-blockchain identity certificate.

BPC: The BPC is devised to proof the business contract with identity authorization and record it on blockchain. One user can propose a business contract with bilateral or multilateral identity authorizations through the business smart contract provided by BCM. The proposed contract can be proofed with respect to the consensus on business operation conditions. In particular, the identity authentication with assistance from IRC. Once the business contract is proofed, it can be conducted in the blockchain environment in a transparent, trusted, and traceable way. The BPC can be realized by public, consortium, or even private blockchains, which has no restrictions. The notaries in BPC can be flexibly appointed with the consideration of the selected blockchain type.

B. Identity Authentication Contract

As previously mentioned, only the user successfully registered in IRC and matched credentials correctly, are allowed to authorize the service contract. Therefore, this paper designs an identity authentication contract. The parameters required for identity registration and authentication are shown in Table I. The user first completes the reading and authentication of identity information through IAM, which is then packaged into an authentication contract by BCM and broadcasts it to IRC. When the identity information has been successfully verified by the notaries, the user's registration is completed.

Rigorous identity authentication logics have been designed in IAM, which are shown in Fig. 3. The authentication process of identity includes two parts: identity certificate authentication and password authentication. Identity certificate authen-

TABLE I
IDENTITY INFORMATION COMPOSITIONS

Symbol	Description
u	The user's identity information.
p	User password information, two-factor authentication with identity information.
u'	Encrypted identity information by Hash function.
v	Hash results of the combination of identity information and password for registration.
S	Time-stamp to ensure uniqueness of the data.

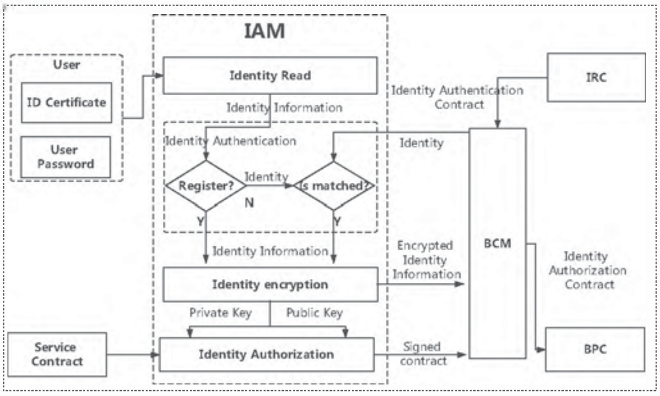

Fig. 3. Design of IAM.

tication is used to ensure that the contents of the credentials are valid, and password authentication used to confirm that the identity information is held in person. The password is relatively simple. In the high-level implementations, biometric authentication such as fingerprint information and iris can be used instead of passwords, thus to strengthen the security of identity information. In the following, the process of identity information registration and authentication are presented.

1) Identity Registration: Users using BIA to authorize identity first need to register personal identity in the IRC. Specifically, the identity u is first read through IAM and the initialization of the password p is required. Then, IAM uses hash algorithm to calculate u' and v for these two pieces of information. The process can be formulated as follows.

- Hash the identity information as the user's encrypted identity identifier:

$$u' = hash(u), \tag{1}$$

- Hash u and p as user encrypted identity information attributes:

$$v = hash(u \cup p), \tag{2}$$

- send u' and v to the BCM, then BCM generates a time-stamp S. Package three parts for the identity authentication contract and broadcast it to the IRC.

Finally, notaries will verify the identity authorization contract. If verification is successful, the contract will be written into the ledger, then the user is registered successfully.

```
Algorithm 1 Key generation
Require: Identity information $u$ and user password $p$;
Ensure: Public key $(n, e)$ and private key $(n, d)$;
Define two very large and unequal prime numbers $p$ and $q$, and calculate their product $n$.
Calculate $n$ Euler function $\varphi(n) = (p-1) \cdot (q-1)$;
Calculate an integer $e$ contenting $1 < e < \varphi(n)$, and make sure that $e$ and $\varphi(n)$ are inter-prime;
$a \leftarrow ASCII(HASH(u \cup p))$;
$a' \leftarrow \left\lceil \frac{a}{\varphi(n)} \right\rceil + a \bmod \varphi(n)$;
Let $e$ equal to the next prime number closest to $a'$;
Calculate the inverse element $d$ of $e$ for $\varphi(n)$ according to the extended Euclidean algorithm;
```

2) Identity Authentication: Authentication is to confirm that the current operation is performed in person. Before the service requester performs identity authorization and the service provider confirms the authorization request, both of them need the identity authentication. They both need to provide the identity certificate and password for authentication by IAM. IAM then communicates with the IRC through BCM to check whether the identity authentication contract of the user that has been registered. If the user has successfully registered, BCM will extract the encrypted identity information to IAM. IAM then verifies whether the information matches to the identity entered by the user. If the information is consistent, the user authentication is successful, and the following identity authorization process can be performed. If there is no record indicating that the user has not completed registration, the identity needs to be authenticated again after registration.

C. Identity Authorization Contract

This part presents the general framework of smart contract with identity authorization. As shown in Fig. 2, when a user requests a service, as the service requester, he/she will call a service contract from BCM. The terminal IAM will authenticate the identity of the service requester. After that, IAM will generate the paired keys based on the identity information to sign the smart contract. After the signing of the smart contract by service requester, it will be sent back to BCM and then to request the identity authorization from the service provider. The identity authorization of the service provider is similar, as illustrated by Fig. 2. The specific key generation process is shown in Algorithm 1. In the following, the detailed identity authorization, the confirmation of smart contract, and the contract verification are introduced.

1) Identity Authorization: To complete the authorization of identity, service requester needs to call a service contract T and check the public key K_i^{pub} of the service provider. Under this premise, the BCM sends the service contract T and the service requester's public key K_j^{pub} to the terminal IAM. Then, IAM performs identity authorization is as follows.

- IAM of service requester first uses service requester's private key K_j^{pri} to encrypt the service contract T as

TABLE II
COMPOSITIONS OF IDENTITY AUTHORIZATION CONTRACT

Symbol	Description
K^{pub}	Public key generated by the RSA algorithm.
K^{pri}	Private key generated by the RSA algorithm.
T	Service contract with detailed service items.
T'	The encrypted service contract that signed with private key.
T''	The encrypted service contract further encrypted by public key.
C	Identity authorization request waiting for authorization from service provider.
C'	Identity authorization contract as identity authorization certificate.

identity authorization. The authorized service contract T'_j can be formulated by:

$$T'_j = K_j^{pri} \xrightarrow{encrypt} T. \tag{3}$$

- Then use service provider's public key K_i^{pub} sent by the BCM to encrypt T'_j for security consideration:

$$T''_{ij} = K_i^{pub} \xrightarrow{encrypt} T'_j. \tag{4}$$

- After the encryption is completed, the IAM send the encrypted service contract T''_{ij} and service requester's public key K_j^{pub} to BCM, BCM integrates these two parts into an identity authorization contract request C:

$$C(K_j^{pub}, T''_{ij}) = T''_{ij} \cup K_j^{pub}. \tag{5}$$

- BCM sends the identity authorization contract request C to service provider through the network, and waits for service provider to confirm the authorization of the contract request C.

2) Contract Confirmation: In order to prevent malicious repetition of authorization by service requester, the service provider is required to confirm the authorization of the received identity authorization contract request C. First, service providers need to use IAM for registration, authentication and encryption before performing authorization contract confirmation operations. When service provider receives the identity authorization contract request C sent by service requester. The BCM checks whether it is a valid request, and then sends the request C to the IAM for decryption operation. The specific process is as follows:

- IAM of service provider first decrypts the service contract using the service provider's private key K_i^{pri} and gets the decrypted service contract is T'_j:

$$T'_j = K_i^{pri} \xrightarrow{decrypt} T''_{ij}. \tag{6}$$

- Then decrypt the T'_j using the service requester's public key K_j^{pub} in the contract, and finally send the decrypted service contract T to the BCM for confirmation by the service provider.

$$T = K_j^{pub} \xrightarrow{decrypt} T'_j. \tag{7}$$

- When the service provider confirms the content of the service contract T, the contract will be authorized by service provider. BCM sends the service contract T to IAM, and IAM uses service provider's private key K_i^{pri} for encryption operations:

$$T'_i = K_i^{pri} \xrightarrow{encrypt} T. \tag{8}$$

- When the encryption is completed, IAM will output the encrypted service contract T'_i together with the service provider's public key K_i^{pub} to the BCM. BCM generates a time-stamp S. Finally, the service requester's public key K_j^{pub}, service contract T'_j encrypted by service requester's private key, public key K_i^{pub} of service provider, service contract T'_i encrypted by service provider's private key, and the generated S are encapsulated by the BCM into an identity authorization contract, which will be broadcast to the BPC:

$$C' = K_i^{pub} \cup K_j^{pub} \cup T'_i \cup T'_j \cup S. \tag{9}$$

Note that if the service provider does not confirm the authorization of the identity authorization contract request C, the request is invalid and will be discarded. Service requester needs to re-initiate the authorization contract request.

3) Verify Contract: The notaries need to verify both of the identity authorizations from the service requester and the service provider. The verification process is as follows. After that one notary receives the contract C', the notary needs to decrypt the contracts T'_j and T'_i using the public keys K_j^{pub} and K_i^{pub} attached in the contract C', respectively. The verification process can be expressed as

$$\begin{aligned} T_1 &= K_i^{pub} \xrightarrow{decrypt} T'_i, \\ T_2 &= K_j^{pub} \xrightarrow{decrypt} T'_j. \end{aligned} \tag{10}$$

If the decrypted authorized contract content T_1 and T_2 are completely consistent, it ensures that the current identity authorization contract is valid. Then, notaries who participate the consensus proof will store the new identity authorization contract into the local contract pool and waiting it to be packed into the following data block.

V. PERFORMANCE EVALUATION

In this section, the performance of the proposed BIA is evaluated based on a developed prototype.

A. Prototype of BIA

To implement the BIA, a prototype system is developed in this paper, which is shown in Fig. 4.

1) Terminal of IAM: To implement IAM, this paper uses Xinzhongxin identifier (an off-the-shelf product) as the identity certificate reader and Orange Pi PC with ARM Cortex A7 as the identity encryptor, as shown in Fig. 4. The identity certificate reader is mainly used to read the identity certificate. Only the officially issued identity certificate can be successfully read. The identity encryptor has several functions such as identity authentication and encryption, key generation and

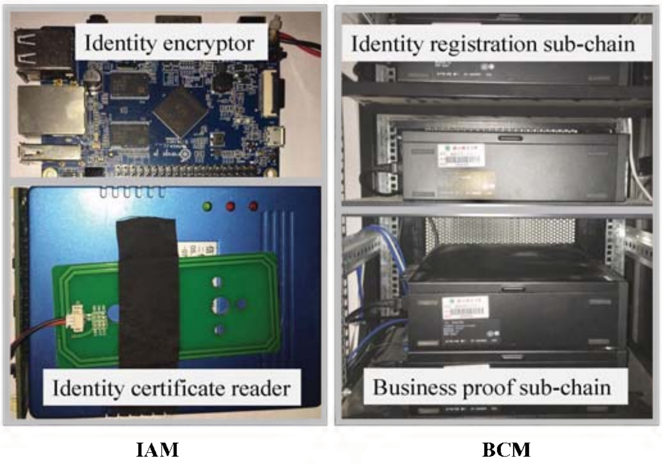

Fig. 4. The prototype of BIA.

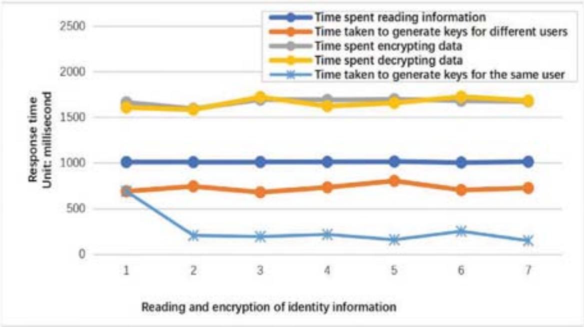

Fig. 5. Response time when the user performs authentication operation multiple times

identity authorization. They will automatically perform the corresponding function according to the designed algorithm and the received data.

2) Double-chain infrastructure: The double-chain infrastructure is constructed based on Ubuntu 16.04 LTS, 8 GB of memory and kernel of Intel i7-6700 3.40 GHz. The identity registration sub-chain runs on 2 nodes and the business proof sub-chain runs on 4 nodes. In the later performance test, hundreds of nodes can be simulated through software.

B. Scheme Analysis

1) Response Time: This paper tested the response time of the BIA function, and the test results are shown in the Fig. 5. It can be seen from the figure that the response time of encrypted and decrypted data is the same, at about 1.6s. The response time for identity reading by IAM is stable at about 1s. Because the time threshold is designed in this paper, when the interval between multiple key generation operations for the same user does not exceed the threshold, IAM directly reuses the previously generated key, so the response time will be reduced. If the threshold is exceeded, as with different users, the key must be produced each time. From the overall test situation, overall response time for all operations tested above can be stabilized at about 3 seconds. For BIA, the response time of the authentication operation is acceptable.

TABLE III
MESSAGE SIZE

	Public key K^{pub}	Encrypted data T'	Multiple encrypted data T''	TimeStamp S	Hash
Message Size(bytes)	216	128	256	13	64

TABLE IV
PACKET SIZE TRANSMITTED

	Registration	Authorization	Confirm
Conclude Data	u'+v+S	$C(K_j^{pub}, T''_{ij})$	$C'(K_i^{pub}, K_j^{pub}, T'_i, T'_j, S)$
Message Size(bytes)	141	485	701

2) Computing Consumption: Because BIA uses hardware devices, which have limited storage and computing capabilities, this paper analyzes the size of the data involved. The size of the data transmitted in the network will directly affect the efficiency of the network, so this paper analyzes the size of the data packets in the BIA, and compares the size of the transmitted data with [14] from the registration, authorization, and confirmation stage. The analysis results are shown in the Table III, IV, and the comparison result is shown in the Fig. 6. It can be seen that during the registration phase, BIA only needs to transmit 141 bytes of data. The packet size is lower than the [14]. In the authorization and confirmation phase, the data package contains the protocol that user needs to be authorized, so the data package is larger than the [14]. In general, for most blockchain networks, the size of the data packets transmitted in the BIA will not affect efficiency.

C. Security Analysis

The comparison on the capacities of the attack resistances is summarized in Table V. Several well-known attacks have been considered. The details are presented as follows.

Sybil Attack: In this paper, all users need to register their identity information through IAM. Therefore, each node has a unique identifier that is authenticated by identity information. When communicating with BIA, a fake node cannot complete the authentication of identity information through IAM.

Message Substitution Attack: During the identity authorization process, a user first needs to register through IAM and the registered information is hashed. If the original data is replaced, the hash value will definitely change. Hence the message substitution attack cannot occur in the registration phase. In the authorization phase, the content of the authorized contract is signed by the private key, and the private key is generated by the identity information. For an attacker, it is impossible to obtain the identity information of others. Thus, a message substitution attack is also impossible.

Denial of Service: Because the identity authorization process proposed in this paper requires two-way authentication, if an attacker maliciously performs identity authorization, the

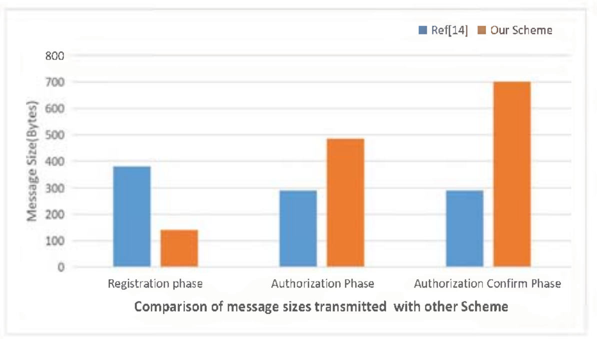

Fig. 6. Comparison of message sizes transmitted with other scheme

TABLE V
COMPARISON ON ATTACK RESISTANCES

	[16]	[17]	[18]	[14]	BIA
Sybil Attack	✓	✓	✓	✓	✓
Message Substitution	✓	✓	✓	✓	✓
DOS	✓	✓	✓	✓	✓
Man-in-the-Middle	✓	✓	✓	✓	✓
Special equipment	✓			✓	✓
Mutual Authentication	✓			✓	✓
Portability			✓		✓
Scalability	✓	✓	✓	✓	✓
Decentralization		✓	✓	✓	✓

false authorization request will be abandoned by the service provider. Hence, DOS has been effectively avoided.

Identity Information Security: Since the identity information can only be read by IAM, and the plaintext is not output to the network, only the hashed identity information is output. Since the hash algorithm cannot infer the original text, the security of the identity information can be ensured.

Authentication Information Security: Only users with an ID card issued by a credible public security agency can access the IRC, and the registration of the identity also needs to be notarized by a credible public security agency, so the security of the authentication information can be guaranteed.

Authorization Information Security: Before accessing BPC, users are required to register on IRC, thus ensuring that anonymous users cannot access BPC. The authorization information requires the service provider to perform authorization confirmation, and the notary is required for notarization, so false identity authorization operations can be avoided. So as to ensure the safety of authorization information.

In summary, this scheme can ensure identity information security and identity authorization contract security well.

VI. CONCLUSION

Considering the widespread usage of personal identity authorization in nowadays social business without effective security protection, this paper proposed a blockchain-based identity authorization mechanism (BIA). In BIA, a double-chain infrastructure was devised for on-blockchain storage of the encrypted identity certificates and on-blockchain recording of the digitally signed service contracts. To implement the BIA, the prototype has been developed and multiple smart contracts for identity authorization have been designed. In Particular, a hardware terminal named Identity Authorization Module was developed which could keep the plaintext of identity certificate off-line. The running results have demonstrated that BIA can well achieve the tamper-resistant, non-repudiable, and publicly verifiable identity authorization.

ACKNOWLEDGEMENT

This work was supported in part by NSF of China under Grants 61877055 & 61672467 and in part by the NSF of Zhejiang Province of under Grant LY18F030013.

REFERENCES

[1] R. G. Smith, "National identity security strategy estimating the cost to australian businesses of identity crime and misuse," *Australian Institute of Criminology*, 2018.

[2] CYU Internet Law Research Center, "Personal information security and privacy protection in China," 2016.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008, [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[4] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.", 2014.

[5] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," Ethereum Foundation, Technique Report, 2014, [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[6] T. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184 133–184 144, 2019.

[7] Y. Yuan and F.-Y. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[8] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, "A bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled Internet of vehicles," *IEEE Trans. Veh. Technol.*, pp. 1–1, 2020.

[9] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *Proc. ICCCNT 2018*, Bangalore, India, Jul. 10-12 2018, pp. 1–4.

[10] R. Rana, R. N. Zaeem, and K. S. Barber, "An assessment of blockchain identity solutions: Minimizing risk and liability of authentication," in *Proc. WI 2019*, Thessaloniki Greece, Oct. 13-17 2019, pp. 26–33.

[11] R. Goyat, G. Kumar, R. Saha, M. Conti, M. K. Rai, R. Thomas, M. Alazab, and T. Hoon-Kim, "Blockchain-based data storage with privacy and authentication in Internet-of-things," *IEEE Internet of Things J.*, 2020.

[12] Y. Zhang and J. Chen, "A delegation solution for universal identity management in SOA," *IEEE Trans. Ser. Comput.*, vol. 4, no. 1, pp. 70–81, 2011.

[13] I. Khalil, A. Khreisha, and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," *Comput. Netw.*, vol. 65, no. 2, pp. 99–110, 2014.

[14] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Ser. Comput.*, vol. 13, no. 2, pp. 241–251, 2020.

[15] Y. Zheng, Y. Li, Z. Wang, C. Deng, Y. Luo, Y. Li, and J. Ding, "Blockchain-based privacy protection unified identity authentication," in *Proc. CyberC 2019*, Guilin, China, Oct. 17-19 2019, pp. 42–49.

[16] Z. Bao, W. Shi, D. He, and K. R. Choo, "IoTChain: A three-tier blockchain-based IoT security architecture," *arXiv: Cryptography and Security*, 2018.

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

[18] 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 Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6688–6698, 2020.