Blockchain-based Decentralized Authentication Modeling Scheme in Edge and IoT Environment

Ma Zhaofeng, *Member, IEEE*, Meng Jialin, Wang Jihui and Shan Zhiguang

***Abstract*—Authentication is the first entrance to kinds of information systems; however, traditional centered single-side authentication is weak and fragile, which has security risk of single-side failure or breakdown caused by outside attacks or internal cheating. In the edge and IoT environment，blockchain can apply edge devices to better serve the Internet of Things and provide decentralized high security service solutions. In this paper, we proposed a blockchain-based decentralized authentication modeling scheme (named BlockAuth) in edge and IoT environment to provide a more secure, reliable and strong fault tolerance novel solution, in which each edge device is regarded as a node to form a blockchain network. We designed secure registration and authentication strategy, blockchain-based decentralized authentication protocol, and developed the blockchain consensus, smart contract, and implemented a whole blockchain-based authentication platform for the feasibility, security and performance evaluation. The analysis and evaluation show that the proposed BlockAuth scheme provides a more secure, reliable and strong fault tolerance decentralized novel authentication with high-level security driven configuration management. The proposed BlockAuth scheme is suitable for password-based, certificate-based, biotechnology-based, and token-based authentication for high level security requirement system in Edge and IoT Environment.**

***Index Terms*— Blockchain, Decentralized Authentication Modeling, Edge Computing, IoT.**

I. Introduction

As one of the most important entrances to kinds of information systems, authentication plays a prominent role in information system protection, which ensures the right user have access to the right system with the right identity[1-2]. Currently, the identity authentication technologies[3-8] are consist of 1)Password-based authentication. 2) Certificate-based authentication. 3) Biotechnology-based authentication, for instance, face, fingerprint or sound recognition.

As is known to all, the password-based authentication system stores the hash value of user's password in the database, and compares the current new password hash values with the stored hash of the original password. If they are consistent, the authentication is passed, otherwise the authentication will be rejected. Although the password-based authentication method is easy to achieve, some serious security problems are existed, such as the brute force cracking and the dictionary attack.

In order to ensure the identity information is not tampered and destroyed, Certificate-based authentication uses digital certificates in the authentication process, which is regarded as an extremely secure and reliable way. Digital certificate can effectively solve the problem of identity authentication in the network world by binding the identity information and related key of certificate holder. As the basic architecture of the digital certificate, Public Key Infrastructure(PKI) provides identity establishment and authentication mechanism in the network through digital certificates management, which allows users to use encryption, decryption technology and digital signature technology in various application scenarios easily[1-3,7-9].

And Biotechnology-based authentication collects users' biometric information, such as fingerprint, face, iris, voiceprint and so on, and compares them for identity information security. Biometric-based identification technology has many advantages over traditional identity authentication, for example, confidentiality, convenience, good anti-counterfeiting performance, not easy to forge or steal, carry around and use anytime and anywhere. However, the collection of biometric information is difficult. If the information is not encrypted, it may cause the leakage of private information[4-10].

Unfortunately, the current traditional authentication methods, such as the ones introduced above, are centralized schemes, which are weak and single-side with poor fault tolerance and reliability. Meanwhile, they have the following disadvantages[1-2,10-12]:

1) The current single authentication has the hidden danger of single point failure, which is easy to be the target of the attacker, because the attacker can easily forge identity and others to implement the invasion.

2) Blindly trust the authentication agency will bring major security problems, the authentication agency may issue the wrong type of certificate, and are vulnerable to hacking, forgery, and falsification of digital certificates.

3) It is difficult for a single organization to provide multiple types of identity data on which comprehensive multi-factor authentication depends. Moreover, when a single organization is attacked, its corresponding local multi-factor identity data can still be leaked[8-10].

Obviously, in the centralized network, all management rights are gathered in the central node, which bears a huge risk because of the significant responsibility given.

Manuscript received April 8th, 2020. Corresponding author: Ma Zhaofeng, Ph.D Degree, IEEE Member, ACM Member and CCF member. He engages in science research and education work in School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China (e-mail: mzf@bupt.edu.cn).

Since 2008, blockchain technologies[12-13] entered the public's vision with its unique characteristics of high transparency, decentralization, security and reliability. Up to now, many scholars have conducted in-depth research on the technology and security of blockchain[14-17].

As far as the technological development trend of is concerned, the integration of the Internet of things(IoT) and the blockchain is inevitable. Actually, IoT ensures that the information is accurate, real-time, transmitted, while the blockchain establishes a trust mechanism by using its asymmetric encryption algorithm and time stamp technology, which can ensure the timeliness, security, and traceability of information in the process of transmission and sharing[18-23]. Hence, in the process of merging the two technologies, IoT technology can provide more application scenarios for the blockchain, while the blockchain technology can solve the problems of information loss and privacy information security in the IoT.

At present, because of the centralized architecture, the traditional IoT system has great defects in security and robustness. Aiming at the problem, in this paper, we propose an identity authentication scheme based on blockchain, called the BlockAuth scheme, which uses edge devices to build blockchain nodes and provides a decentralized, safe and reliable solution. Compared with traditional centralized authentication scheme in edge and IoT environment, our proposed scheme possesses three characteristics:

(1) Each edge device is regarded as a node to form a blockchain network. All nodes of the decentralized network can participate in the management, and the relationship among nodes is equal. If one node fails, other nodes will replace it.

(2) The scheme can effectively avoid the traditional single-side fault. When the system authenticating a client user, the authentication unit is charged by the blockchain nodes rather than the traditional centered authentication unit, which can avoid the single-side fault risk, especially when the traditional single authentication center is attacked or clasped because of heavy load.

(3) The BlockAuth scheme is not only suitable for password-based authentication, but also suitable for certificate-based, bio-authentication, or token-based authentication, which can be used in high level security requirement, for instance, the core confidential or military system.

II. Related work

Until now, there are many solutions to the problem of identity authentication technologies such as password-based authentication, certificate-based identity management, and finger-based access control or face-recognition-based authentications, upon which certificate transparency (CT) [11] detects fraudulent certificates by forcing certificates issued by the certification center to be attached to the certificate transparency log.

Another method is public key pinning (PKP), that is, the server sends the hash value of the public key or the public key of the certificate of the certification center to the client, and the hash value is stored by the client, which can detect whether the key has changed. However, the need to configure a web server poses a risk to domain name holders. If the domain name holder loses access to these keys, or key disclosure occurs, the browser will reject the link, and the customer will not be able to access the website[10-11].

For the research of edge computing, many scholars also put forward different solutions. To address the complex and dynamic control issues, Xiaofei Wang et al[24]. proposed a FederAted Deep reinforcement learning-based cooperative Edge caching (FADE) framework.

In 2008, blockchain[12-13] came into the public's view. Blockchain is a combination of encryption algorithm, consensus mechanism, distributed data storage and point-to-point transmission, which has the characteristics of transparency, immutability, anonymity and high security[24].

With the implementation of blockchain, scholars realized that blockchain technology can be used not only in the field of economics and currency, but also in the field of security control. Identity authentication and access control based on blockchain have been widely concerned and studied. Research on blockchain-based schemes improved authentication methods much more[14-23].

Duard A et al.[19] proposed a blockchain-based decentralized network trust and IoT authentication protocol under the public key encryption system. Sanda, Tomoyuki. et al.[20] proposed a new authentication method in Wi-Fi access using Bitcoin 2.0. Puthal D et al.[22] presented a novel consensus algorithm called Proof-of-Authentication (PoAh) to replace Proof-of-Work and introduce authentication. H. Es-Samaali et al.[23] contributed to reinforcing the security of Big Data platforms by proposing a blockchain-based access control framework.

The existing blockchain-based authentication scheme has the following shortcomings[21-23]. First, most of the existing schemes are built on the public chain, therefore, its reading and storage performance is low, the transaction time is long, its nodes are difficult to add or cancel flexibly, and the schemes are difficult to upgrade. Second, the existing scheme lacks the combination with the existing traditional PKI technology, so it is difficult to adapt to a variety of application scenarios. Third, some identity authentication schemes simply use the key technology, which is difficult to develop into the international standard general identity authentication schemes.

Edge computing has important applications in distributed systems. In order to further optimize the edge system, Xiaofei Wang et al [25]. designed the “In-Edge AI” framework, proposed to integrate the Deep Reinforcement Learning techniques and Federated Learning framework with the mobile edge systems.

In the Internet of things environment, each edge device can be regarded as a node to form a complete blockchain network, which realizes the integration of blockchain and Internet of things technology. This paper proposed the BlockAuth scheme combines the advantages of the above research ideas, and improves the shortcomings of the existing authentication schemes. It makes full use of the blockchain characteristics to

ensure the privacy of identity information and the high transparency of authentication process, so that the authentication technology of this design scheme is credible and reliable in edge and IoT environment.

III. THE BLOCKAUTH SCHEME

A. The BlockAuth Scheme Model

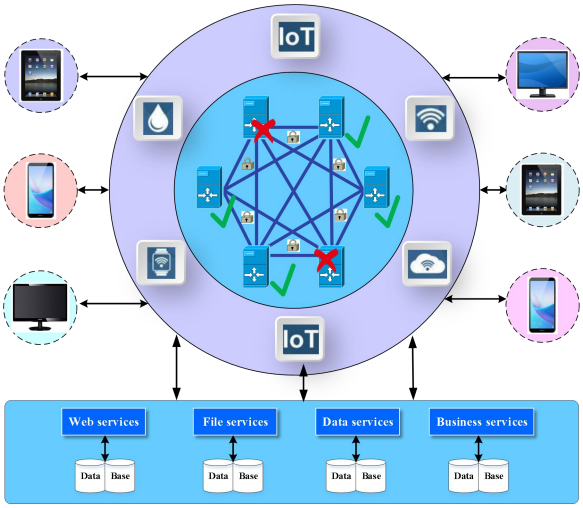

Fig. 1. The architecture of the BlockAuth Scheme

In view of the problems existing in the current identity authentication protocol, a BlockAuth Scheme is proposed. In the proposed BlockAuth Scheme, the registration protocol, consensus mechanism of security enhancement and the authentication protocol are studied in detail. The secure architecture of the BlockAuth scheme is described as Fig. 1.

In the scheme, users can access data resources, service resources, business resources and management resources through the user interface, and can send user registration or authentication requests and information to the blockchain network. The blockchain network is the core of the platform, including smart contracts, node management, consensus mechanisms, cryptographic algorithms and other functions, providing secure services for all functions of the scheme.

The business process of BlockAuth Scheme is shown in Fig. 2. In the service process, user can call the interface to send the request and data to the blockchain platform. Then, in order to deal with the request and data, the blockchain platform will call the blockchain execution engine to invoke the smart contract and other functions. After verification by at least three endorser nodes, the blockchain execution engine will call the block generation module to generate a new block. Finally, the engine will write the completed transaction into the newly created block, and write the timestamp and other information additionally.

B. The BlockAuth Scheme Protocol

(1). Client initiates user registration request

When the user requests for the initialization of the authentication from the system certificate issuer, the user initiates a registration request, the user's name and password attribute values need to be entered. The request info of user certificate includes certificate type, user's public key and it's validity period, then submits certificate application request and applies for registration of certificate. After receiving the user's application, the registration center verifies the validity of the user's identity information, once finished the approval of the registration center, the user identity certificate(CertU) is generated through the certificate issuing center as follows:

$$CertU = \mathrm{Req}(UID \mid pswd) \tag{1}$$

(2). Registration Stage of the BlockAuth Scheme

During the registration stage of the BlockAuth scheme, the user signs the user's index and hash of the password attribute values to generate signature information, and then commits the information in the blockchain by calling the smart contract of the blockchain and creates the blockchain and transaction information. The registration procedure is described as follows:

$$\mathrm{Sig} = UID \mid h(pswd) \mid \mathrm{Sig}_{\mathrm{prk}_u}(UID \mid h(pswd)) \tag{2}$$

(3). Authentication Stage of the BlockAuth Scheme

The blockchain verifies the identity of the transaction initiator by verifying the transaction signature, and confirms that the certificate is issued by verifying the signature in the certificate. In details, when the authentication nodes receive the authentication request from the client user, the peers in the AuthNode authenticate the client request as follows:

$$\begin{cases} V_1 = \mathrm{V}_{\mathrm{p}_1,\ pk_u}(UID \mid h(pswd) \mid Sig_{\mathrm{prk}_u}(UID \mid h(pswd))) \\ V_2 = \mathrm{V}_{\mathrm{p}_2,\ pk_u}(UID \mid h(pswd) \mid Sig_{\mathrm{prk}_u}(UID \mid h(pswd))) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ V_n = \mathrm{V}_{\mathrm{p}_n,\ pk_u}(UID \mid h(pswd) \mid \mathrm{Sig}_{\mathrm{prk}_u}(UID \mid h(pswd))) \end{cases} \tag{3}$$

A request of authentication passes the verification if and only if the following conditions are satisfied: Where f is the fault nodes, and n is the total nodes in a specific blockchain system.

As we know, the relationship of n and f in RAFT and Practical Byzantine Fault tolerance (PBFT) [28-29] consensus is as follows:

$$n \geq \begin{cases} 2f+1, & RAFT \\ 3f+1, & BPFT \end{cases} \tag{4}$$

Thus, we have the following relationship between f and T_0:

$$T_0 = n - f = \begin{cases} (2f+1) - f = f+1, & RAFT \\ (3f+1) - f = 2f+1, & BPFT \end{cases} \tag{5}$$

That is to say, the authentication condition in the RAFT or PBFT consensus should at least exist f+1 or 2f+1 confirmation that can confirmed the authentications as follows:

$$T \geq \begin{cases} f+1, & RAFT \\ 2f+1, & BPFT \end{cases} \tag{6}$$

(4) Security Enhanced Consensus of the BlockAuth Scheme

PBFT is a set of algorithms based on state machine copy replication, which is proposed by Miguel Castro and Barbara Liskov and others. The security of PBFT algorithm is jointly

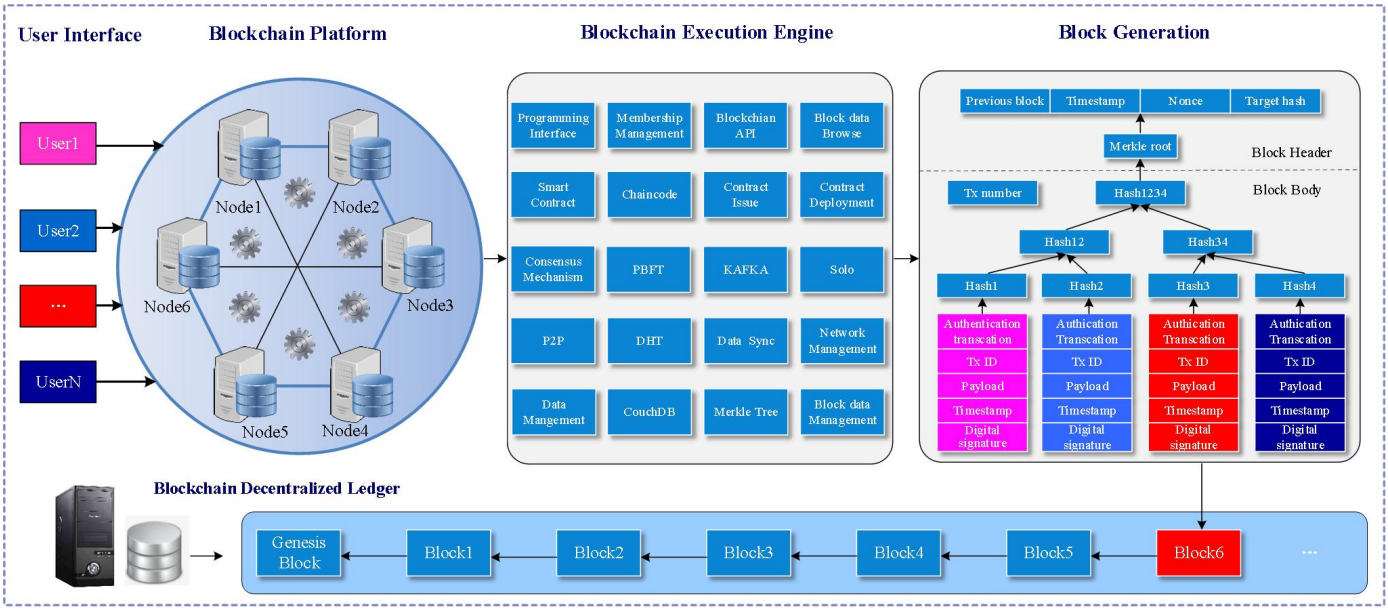

Fig. 2. The service process of BlockAuth Scheme

guaranteed by each node of blockchain network. Meanwhile, PBFT algorithm is mainly determined by three votes among nodes, and is achieved by the way that the minority is subject to the absolute majority[26-27]. The consensus process of PBFT is as follows[27]:

(1) Propose. The client sends the request message *m* to the nodes in the network, including the leader node and other endorser nodes

(2) Pre-prepare. The leader node receives the request message *m* sent by the client, assigns the *m* serial number *s*, and calculates the pre-prepare message (*pre-prepare*, H (m), *s*, *v*), where H() is a one-way hash function, and *v* represents the view at this time. Before sending a message, the node needs to digitally sign *m* with its private key. Then the leader node sends the prepared message to other endorser nodes in the organization.

(3) Prepare. After receiving the pre-prepare message from the leader node, the endorser node verifies the validity of H(m). If the verification passes, the endorser node calculates the preparation message (*prepare*, H (m), *s*, *v*) and broadcasts it throughout the entire network. At the same time, all nodes collect the preparation message. If the number of the collected legal preparation message is more than or equal to 2*f*+1(including itself).

(4) Commit. When the prepared certificate is composed, the node will calculate the commitment message (*commit*, *s*, *v*) and broadcast it, and put the message *m* into the local log. At the same time, the node collects the commitment message in the network. If the number of legal commitment messages collected is more than or equal to 2*f*+1(including itself), then the committed certificates are composed of these commitment messages, which proves that the message *m* completes the final commitment.

(5) Reply. The endorser nodes return the committed certificate to the client as the reply to message *m* and the client confirms the final commitment of message *m*.

In the PBFT consensus, there is a node set R with N nodes, whose node number is i ($i \in \{0,1,2\ldots\ldots,\ N\text{-}1\}$). Among them, the set of nodes participating in consensus is R^c and the number of nodes is M; the set of nodes not participating in consensus is R^N (the number of nodes is N-M), which satisfies:

$$R^C \cup R^N \ \&\& R^C \cap R^N = \Theta \tag{7}$$

and satisfies:

$$\begin{cases} R_i \in R^C, & i \in [0,\ M) \\ R_i \in R^N, & i \in [M, N) \end{cases} \tag{8}$$

Among them, there may be k error nodes in the consensus node set R^C. If the error node set is R^K, there are:

$$R^C \supseteq R^K \tag{9}$$

According to the voting characteristics of Byzantine Fault Tolerance(BFT)[28], in order to meet the consensus needs, there are:

$$3f + 1 \le n \tag{10}$$

The main contribution of PBFT is the system can still operate when it exists $(n-1)/3$ malefactor, where n is the maximum participants in the system[26-27].

(5) The BlockAuth verification protocol

Elliptic curve digital signature algorithm (ECDSA)[28] is a digital signature method using elliptic curve encryption technology. Suppose the sender needs to send the message signed by the elliptic curve to the receiver. First, we need to define a set of parameters which are accepted by both sides, and express these parameters as $(CURVE, G, n)$. Where *curve* is the point domain and geometric equation of the elliptic curve, G is the base point for all dot product operations, n is the multiplicative order of the elliptic curve, and $nG = 0$.

Second, the sender will create a private key and a public key. Where the private key is a random number in the range of $[1, n-1]$:

$$d_A = rand(1, n-1)$$

The public key is the elliptic curve dot product of the private key and the base point:

$$Q_A = d_A \times G \tag{11}$$

1) Signature algorithm

The signer signs the message *m*. In this scheme, message *m* includes user name and user attribute information.

The specific steps are as follows:

Step1: Calculate e=h(m)， where $m = (UID \,|\, \mathrm{h}(pswd))$;

Step2: And calculate z, from the highest L bit (leftmost) of binary e, and L is the binary length of n in the above parameters;

Step3: Choose a random integer k from $[1, n-1]$;

Step4: Calculate a point on the elliptic curve:

$$(x_1, y_1) = k \times G \tag{12}$$

Step5: Calculate the value of r, if $r == 0$, return to step3 for recalculation;

$$r = x_1 \bmod n \tag{13}$$

Step6: Calculate the value of s，if $s == 0$，return to step3 for recalculation

$$s = k^{-1}(z + rd_A) \bmod n \tag{14}$$

Step7: The digital signature is the generated (r, s).

2) Verification algorithm

In addition to receiving signature documents, the receiver will also have a public key. Therefore, the authentication has two parts: first, authenticate the public key, and then authenticate the signature (r, s).

a) Verification of public key

Step1: The coordinates of public key Q_A should be valid and not equal to a limit value of null point O;

Step2: The coordinates of public key Q_A are used to authenticate that they are points on the elliptic curve;

Step3: The formula (15) must be workable, that is, the point product of the multiplicative order n and the public key doesn't exist;

$$n \times Q_A = \mathrm{O} \tag{15}$$

b) Verification of signature files

Step1: Authenticate r and s are integers in the range of $[1, n-1]$; otherwise, the authentication fails;

Step2: Calculate e = h(m);

Step3: Then calculate z， from the highest L bit of e;

Step4: Next, calculate w *with*

$$w = s^{-1} \bmod n \tag{16}$$

Step5: And u_1 and u_2

$$u_1 = zw \bmod n \quad , \quad u_2 = rw \bmod n \tag{17}$$

Step6: Then calculate (x_1,y_1) the (x_1,y_1) should be a point on the elliptic curve; otherwise, the authentication fails;

$$(x_1, y_1) = u_1 \times G + u_2 \times Q_A \tag{18}$$

Step7: The following formula should hold; otherwise, the authentication fails.

$$r \equiv (x_1 \bmod n) \tag{19}$$

There are two conditions that can pass the verification: the one is that the verification information is correct, and the other is that the correct threshold of the consensus node must reach the minimum number of verifications，that is,

$$t \geq t_0, \quad t_0 = 2f + 1 \leq n \tag{20}$$

In the PBFT $t_0 = n - f \geqslant 2f + 1$， such as, if $f = 1$， the condition for reaching consensus is that the number of correct nodes(t_0) is at least 3.

If the authentication is successful, the success information will be sent to the endorser node, and then be returned to the client through the channel; otherwise, the authentication fails, and the failure information will be returned.

C. The BlockAuth Network Topology

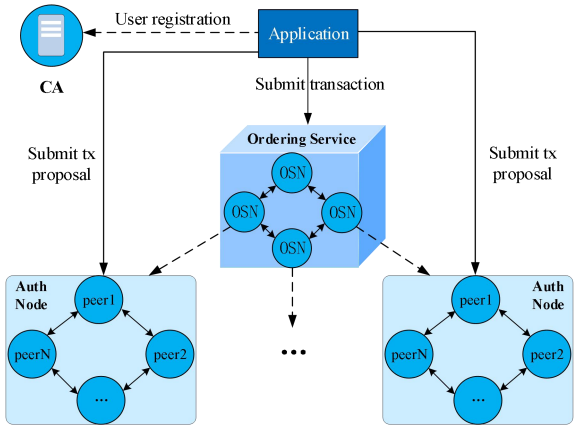

Fig. 3. The topology of BlockAuth Scheme

In the BlockAuth Scheme, the actual authentication system deployment includes the independent deployment of multiple role servers, including the deployment of blockchain network, the deployment of identity authentication service. Blockchain network deployment includes the deployment of endorser node and peer node. The authentication service deploys the registration server and the certificate issuing server.

The whole topology of BlockAuth Scheme can be shown in Fig.3. The blockchain network established in the BlockAuth Scheme has one order node and two orgs. Each org includes one CA and two peer nodes. All nodes in the blockchain are committer nodes. Before submitting a registration request, the system enrolls an administrator, who is registered with other tools for each CA of the org in advance, and then, use the administrator to register, enroll, and deregister users and other transactions of the org.

In the BlockAuth Scheme, there is a client and a server, the client provides the user interface, which is responsible for collecting user requests and data. The server adopts the stand-alone deployment, the consensus mechanism is Solo. Meanwhile, the Hyperledger Fabric1.4 is deployed in the server, which is responsible for processing requests and data, writing transaction into block and so on.

IV. Implementation of The BlockAuth Scheme

For the design of the BlockAuth Scheme, we implemented the decentralized authentication platform based on Hyperledger Fabric1.4, with the functions of identity registration, enrollment and authentication. In the scheme, a

specific smart contract for identity authentication is put forward, and all kinds of parameters for implementing and developing the decentralized authentication platform are listed in Table 1.

Table 1 The parameters of developing BlockAuth platform

Name	Data
CPU	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz 2.40Ghz
Memory	8.00 GB
Hard disk	256 GB
Client	OS :Windows 10 Pro
Virtual machine	Virtualbox 5.2.8
Server (Virtual machine)	Memory: 2GB , Harddisk: 22GB, OS: Ubuntu16.04, Docker 17.03e,
Blockchain	Hyperledger Fabric 1.4

Table 2 Critical chaincode of BlockAuth platform

```
func (t *SimpleChaincode) checkCons(stub
shim.ChaincodeStubInterface, args []string) pb.Response{
    pubKey := hexToPublicKey(args[2], args[3])
    sigR, _ := new(big.Int).SetString(args[0],10)
    sigS, _ := new(big.Int).SetString(args[1],10)
    msg := []byte(args[4])
    hash := sha256.New()
    hash.Write(msg)
    bytes := hash.Sum(nil)
    ok := ecdsa.Verify(pubKey, bytes, sigR, sigS)
    if ok == true {
        return shim.Success([]byte("Authentication passed"))
    } else {
        return shim.Success([]byte("Authentication failed")) }}
```

The BlockAuth scheme proposed designs a corresponding chaincode to authenticate the accuracy of the signed information. The critical chaincode for authentication are shown in Table2.

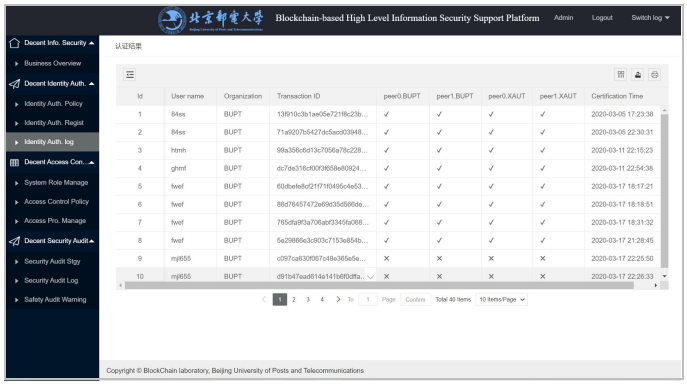

Fig. 4. The authentication log interface of BlockAuth Scheme

The identity authentication log interface of the BlockAuth platform is shown in Fig. 4, which shows the on-chain data of identity authentication of all users on the platform.

After the blockchain network was created, transactions, initiated by users through the client, will be written into the newly generated block of the blockchain. In the BlockAuth Scheme, we set up two orgs in the server, where each org adds two peers and each peer node can store block data independently. Table 3 lists one of the block data in detail.

Table 3 The block data of BlockAuth platform

Name	Data
BlockNumber	54
CurrentHash	086a2258c82385e53ec7bc03cc33b8e04a3dacaaa7aeead80505043e2ca810d8
PreviousHash	175bedeaf81c3628bed909add1985a5a1bac29fea4094a78cdae2c50aa026156
Datahash	7469b2924f77b9cc33b9ead1bf14a0554af7d7ad38e7b12a8f350e14f706e6fa
Number of tx	1
tx_id	6214d992b9b1d5497157c3b5b92ea4868a440ce5c71e4ad46fdee5500160ec12

Next, we test the function of registration and user enrollment in the scheme. The client initiates the user registration request to the preset endorser node. And the endorser nodes verify the identity of the CA administrator who applies to register the user. After the verification, the generated certificate is returned to the client.

Table 4 The registration and enrollment user process of BlockAuth platform

1 Fabric1.4 register and enroll user
2 CA -http://192.168.188.1:7054 Enrolled Admin.
3 CA -http://192.168.188.1:7054 Registered User - org1User15802
4 CA -http://192.168.188.1:7054 Enrolled User - org1User15802

Then, the newly registered user is used for authentication. The endorser nodes will verify the identity submitted by the client, as well as authenticate its additional attribute information signed by the ECDSA with the user public key. When the chaincode and endorsement strategy are deployed and added respectively, the transaction will be verified by at least three of the four peers. The endorser nodes invoke the precompiled chaincode to authenticate after verifying the identity of the initiator of the request.

Table 5 The authentication passed and failed process of BlockAuth platform

1 ----------User Identify Authentication----------
2 peer1.org1.BlockAuth.com: Authentication passed
3 peer1.org2.BlockAuth.com: Authentication passed
4 peer0.org2.BlockAuth.com: Authentication passed
5 peer0.org1.BlockAuth.com: Authentication passed
1 ----------User Identify Authentication----------
2 peer1.org1.BlockAuth.com: Authentication failed
3 peer1.org2.BlockAuth.com: Authentication failed
4 peer0.org2.BlockAuth.com: Authentication failed
5 peer0.org1.BlockAuth.com: Authentication failed

After using the user public key sent by the client to authenticate the identity information, the chaincode will return the verification result to the client. Table 4 lists the process of user registration and enrollment in the platform. Before registering a user, a registered admin must be enrolled to the CA of the org, and perform the operations of registering and enrolling users. Table 5 lists the process of the BlockAuth platform of user authentication passed or failed.

V. Evaluation of The BlockAuth Scheme.

The evaluation of the BlockAuth Scheme is based on the authentication time from initiate the request to receive the result. Generally, this time is related to the network speed of

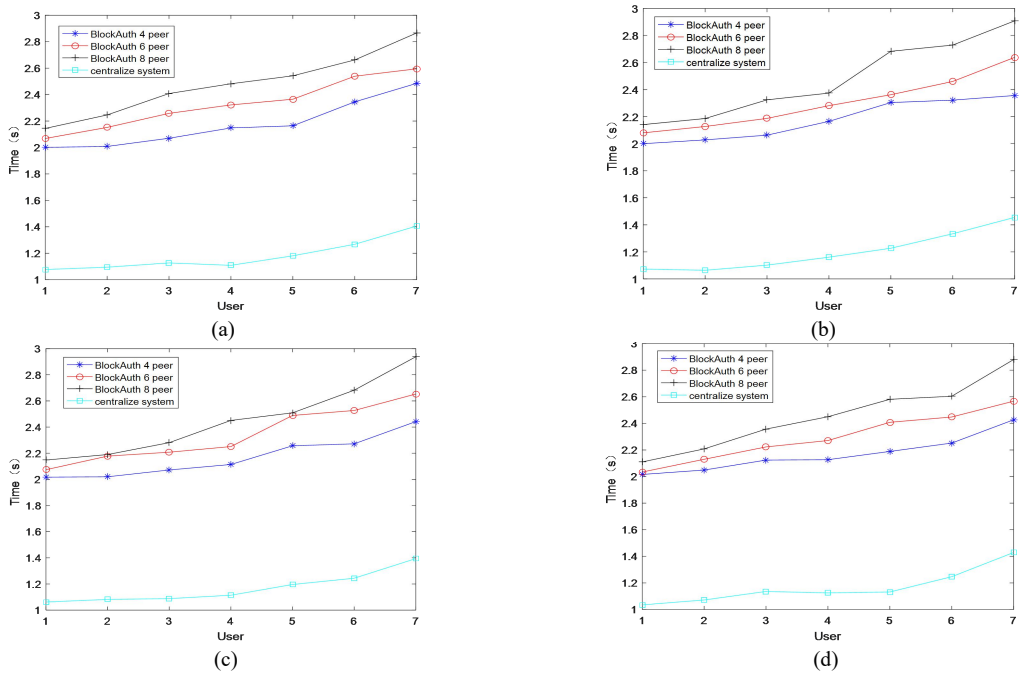

Fig. 5. The performance evaluation results of BlockAuth platform

the test environment. The slower the network speed is, the longer the time will be.

We evaluate the scheme according to the different results of identity authentication, passed or failed. In this scheme, we test the response time of centralized network and 4-peer, 6-peer and 8-peer in the decentralized network respectively. The response time test is divided into 2 groups, where each group tests 7 groups of data. The test result is shown in Fig.5, where figure a and b are the response time of authentication failed, others are the response time of authentication passed.

It can be seen that, in the 'passed' scene of the BlockAuth scheme, the average response time of 4-peer, 6-peer and 8-peer in two groups test is about 2.24s, 2.31s and 2.40s respectively. And in the 'failed' scene, the average response time of 4-peer, 6-peer and 8-peer in two groups test is 2.22s, 2.30s and 2.40s respectively. Moreover, it is note that the fluctuation of response time may be related to the speed of the network.The average value of the two scenes is not much different, and the data fluctuation of each scene is within the normal range. Therefore, the system performance is relatively stable. The average response time of the centralized authentication scheme is about 1.13s. Although the centralized authentication response time is very short, it does not mean that its security is highly reliable, because it is easy to be attacked and invaded.

Compared with the existing related scheme, although the time complexity of the proposed BlockAuth scheme is high, its security, robustness and fault tolerance are strong, and is more suitable for application scenarios with higher security requirements. The detailed results are shown in Table 6.

The analysis proves that the proposed BlockAuth scheme has following advantages: collaborative authentication, strong fault tolerance, decentralization, stability and high-level security. In addition, this scheme can meet the authentication requirements of multiple scenarios and development demand of the international standard authentication scheme.

Table 6 BlockAuth scheme comparison with related work

Scheme	Centralization/ Decentralization	Multi-signature identity data	Award	Decision Strategy/ Consensus	Fault Tolerance	Time complexity	Security & Reliability
PKP[10]	Centralization	NO	NO	Single/Centralized	1	O(1)	Poor
CT [11]	Centralization	NO	NO	Single/Centralized	1	O(1)	Poor
Duard A et al. [19]	Decentralization	NO	YES	POW	2f+1≤n	O(n)	Median
Sanda T et al. [20]	Decentralization	NO	YES	POW	2f+1≤n	O(n)	Median
BlockAuth	Decentralization	YES	NO	PBFT	3f+1≤n	$O(n^2)$	Strong

VI. CONCLUSION

In order to solve the security and reliability of traditional authentication in the edge and IoT environment, we proposed a BlockAuth Scheme, which can provide a more secure, reliable and strong fault tolerance decentralized novel authentication solution with high-level security. In this scheme, each edge device is regarded as a node to form blockchain network. Specially, we designed the secure registration and authentication strategy and the blockchain-based decentralized authentication protocol, improved the blockchain consensus, developed smart contract, and finally implemented the whole blockchain-based authentication platform for the feasibility, security and performance evaluation. According to Evaluations and Comparison with the existing related scheme, our scheme enhances security and stability on the basis of

sacrificing a certain degree of time complexity, and meets the high security and fault tolerance requirements of identity authentication in edge and IoT environment. Furthermore, this scheme proposed by us can meet the authentication requirements of multiple scenarios and development demand of the international standard authentication scheme.

REFERENCES

[1] Proc. Roy. Soc. A Math. Phys. Eng. Sci., vol. 426, no. 1871, pp. 233-271, 1989.

[2] M. Abadi and M. R. Tuttle, "A semantics for a logic of authentication", Proc. 10th Annu. ACM Symp. Princ. Distrib. Comput., pp. 201-216, 1991.

[3] Hung-Yu Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Transactions on Dependable and Secure Computing, vol.4, pp.227-340, 2007.

[4] Jia-Lun Tsai ; Nai-Wei Lo. A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services. IEEE Systems Journal, vol.9, pp.805-815, 2015.

[5] Muhammad Ajmal Azad; Samiran Bag; Charith Perera; Mahmoud Barhamgi; Feng Hao. Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network. IEEE Transactions on Industrial Informatics, vol.16, pp.3606-3615,2020.

[6] Libor Dostálek. Multi-Factor Authentication Modeling. 2019 9th International Conference on Advanced Computer Information Technologies (ACIT).

[7] K. M. Renuka ; Saru Kumari ; Dongning Zhao ; Li Li. Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems. IEEE Access, vol.7, pp. 51014 – 51027, 2019.

[8] T.-D. Nguyen, A. Al-Saffar and E.-N. Huh, "A dynamic id-based authentication scheme", Proc. 6th Int. Conf. Netw. Comput. Adv. Inf. Manage. (NCM), pp. 248-253, Aug. 2010.

[9] S. Chen, M. Ma and Z. Luo, "An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems", Secur. Commun. Netw., vol. 9, pp. 1146-1157, 2016.

[10] X. Sun, S. Men, C. Zhao and Z. Zhou, "A security authentication scheme in machine-to-machine home network service", Secur. Commun. Netw., vol. 8, no. 16, pp. 2678-2686, 2015.

[11] Arno Fiedler, Christoph Thiel. Certificate Transparency. Datenschutz und Datensicherheit - DuD, 2014, Vol.38 (10), pp.679-683.

[12] Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.

[13] Ryan Henry; Amir Herzberg; Aniket Kate, "Blockchain Access Privacy: Challenges and Directions", IEEE Security & Privacy, vol.16, no.4, pp.38-45,2018.

[14] Tomaso Aste; Paolo Tasca; Tiziana Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry", Computer, vol.50, no.9, pp.18-28,2017.

[15] Tien Tuan Anh Dinh; Rui Liu; Meihui Zhang. "Untangling Blockchain: A Data Processing View of Blockchain Systems", IEEE Transactions on Knowledge and Data Engineering, vol.30, no.7, pp.1366-1385,2018.

[16] H. G. Do, W. K. Ng, "Blockchain-based system for secure data storage with private keyword search", 2017 IEEE World Congress on Services (SERVICES), pp. 90-93, 2017.

[17] Y Zhe, Y Kan, et.al. Blockchain-based Decentralized Trust Management in Vehicular Networks，IEEE Internet of Things Journal , Vol.6, No.2, pp.1495-1505,2019.

[18] Xu Q, Jin C, Rasid M F B M, et al. Blockchain-based decentralized content trust for docker images. Multimedia Tools and Applications, Vol.77, No.14, pp.18223–18248,2018.

[19] Duard A, Gremaud P, Pasquier J. Decentralized web of trust and authentication for the internet of things. Proceedings of the Seventh International Conference on the Internet of Things. ACM, 2017: 27.

[20] Sanda T, Inaba H. Proposal of new authentication method in Wi-Fi access using bitcoin 2.0. Consumer Electronics, 2016 IEEE 5th Global Conference on. IEEE, 2016:1-5.

[21] S. Khan and R. Khan, "Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions,"Energies, vol. 11, no. 5, p. 1154, 2018.

[22] Puthal D, Mohanty SP, Nanda P, Kougianos E, Das G. Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In: Proceedings of the 2019 IEEE international conference on consumer electronics (ICCE). IEEE; 2019. p. 1–5.

[23] H. Es-Samaali, A. Outchakoucht, and J. P. Leroy, A blockchain-based access control for big data, Int. J. Comput. Netw. Commun. Secur., vol. 5, no. 7, pp. 137–147, 2017.

[24] Xiaofei Wang, Chenyang Wang, Xiuhua Li, Victor C. M. Leung, Tarik Taleb: Federated Deep Reinforcement Learning for Internet of Things with Decentralized Cooperative Edge Caching. IEEE IoT Journal, DOI: 10.1109/JIOT.2020.2986803

[25] Xiaofei Wang, Yiwen Han, Chenyang Wang, Qiyang Zhao, Xu Chen, Min Chen: In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning. IEEE Network 33(5): 156-165 (2019)

[26] Lamport L, Shostak RE, Pease MC. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems, vol.4, no.3. 1982.

[27] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems, vol.20, no.4, 2002, 398–461.

[28] Don Johnson, Alfred Menezes, Scott Vanstone. "The Elliptic Curve Digital Signature Algorithm (ECDSA)", International Journal of Information Security, vol.1, No.1, pp.36-63, 2001.

Ma Zhaofeng is IEEE member, CCF member and ACM member with Ph.D. Degree. He engages in science research and education work in School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include blockchain, mobile Internet security, digital rights management (Email: mzf@bupt.edu.cn).

Meng Jialin is a master student School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. She had finished the blockchain-based digital asset management system, blockchain-based decentralized authentication system. Her research interests include blockchain, network security& cryptography (Email: mengjialin655@163.com).

Wang jihui is a master graduated engineer of Puhua Group Co.Ltd. Haidan, Beijing He finished 5 important blockchain projects management and development work, and finished the projects performance evaluations. His research interests include blockchain, network security and cryptography(Email: wangjh@hotmail.com).

Shan Zhiguang is Ph.D and the dean of the national information center, Beijing, China. He Finished more than 18 Projects of intelligent city, blockchain and IoT, he published 10 high quality papers in IEEE Transactions on Automatic Control, IEEE Transactions on Systems, Man and Cybernetic, Computer Networks (Email:shanzg@scdr.sic.gov.cn) .