Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Research on Digital Identity Authentication Technology Based On Block Chain

To cite this article: Zaixing Chen and Shaofei Wu 2021 *J. Phys.: Conf. Ser.* **1802** 032091

PRIME
PACIFIC RIM MEETING ON ELECTROCHEMICAL AND SOLID STATE SCIENCE
HONOLULU, HI
Oct 6–11, 2024
Abstract submission deadline:
April 12, 2024
Learn more and submit!
Joint Meeting of
The Electrochemical Society
•
The Electrochemical Society of Japan
•
Korea Electrochemical Society

Research on Digital Identity Authentication Technology Based On Block Chain

Zaixing Chen[1, 2], Shaofei Wu[1, 2, *]

[1]Hubei Province Key Laboratory of Intelligent Robots, Wuhan Institute of Technology, Wuhan, P.R.China
[2]School of Computer Science and Engineering, Wuhan Institute of Technology, Wuhan, P.R.China

*Corresponding author: 04005047@wit.edu.cn

Abstract. In the traditional digital identity authentication, there are potential security threats caused by the user's personal privacy data being too centralized and vulnerable to attack, and data centralization will lead to data redundancy, poor permeability, user's lack of master control, high overall cost, and potential threats of abuse of central rights. The digital identity authentication technology based on block chain can perfectly solve the problem of appeal. The main innovative work includes the design of a new digital identity ID and a new asynchronous Byzantine fault-tolerant algorithm dsbft using cryptography, computer network, asynchronous Byzantine fault-tolerant algorithm and other technologies, Block chain is designed based on ID and dsbft, and a decentralized identity authentication system is designed based on block chain. Hash algorithm is used for signature and acceptance to improve authentication efficiency and scalability. In order to solve the dust attack and quantum computation, the elliptic curve digital signature algorithm (ECDSA) encryption algorithm can be combined with other cryptography. The results show that the appeal identity authentication scheme can resist a variety of attacks and has high efficiency and security.

Keywords: Block chain,Authentication; Decentralization; ECDSA; Hash algorithm.

1. Introduction

In the era of rapid development of the Internet, in order to more convenient and efficient use of networking equipment, it is necessary to verify the network digital identity authentication, China has basically realized the network real name system. How to effectively authenticate legal and trusted digital identity, establish secure and reliable communication, and avoid the hidden danger and risk of information security is very important to the safe operation of mobile Internet Society [1]. The current network identity authentication system basically adopts the centralized design method, which has the problem of information leakage or tampering caused by the authority control error or the intrusion of the central organization [2]. In view of the frequent occurrence of network fraud, infringement and other identity related illegal acts, we need a more secure and reliable encryption and decryption technology and digital signature technology [3] to protect the user's information and property security.

However, the use of certification authority introduces the hidden danger of single point of failure, and excessive trust of certification authority will bring significant security problems [4]. For example, the certification authority may mistakenly issue an intermediate certification center certificate [5]. Network trusted identity authentication technology is one of the core technologies of information security, and its task is to identify and verify the legitimacy and authenticity of user identity in the network business system and the consistency of online and offline identities [6]. In view of the channel between the server and the user no longer has highly reliable security, and the centralized network is difficult to bear the increasing network burden, some researchers proposed to use block lattice in the Internet of things identity authentication protocol. Due to the existence of consensus mechanism, the throughput of block lattice can not meet the requirements of the protocol. Therefore, a bifurcated block lattice structure is proposed to deal with the double flower attack [7].Some researchers have also designed a block chain based security authentication and key agreement scheme for the Internet of things, which mainly aims at the end-to-end two-way identity authentication between devices and devices, and between devices and users. The public identity information of devices and users is stored in the block chain, To ensure that the key information will not be stolen and changed, the existing authentication schemes can solve the problems of certificate management, over centralization of authentication and public key replacement [8]

In recent years, block chain technology with its distributed, security, reliability and data integrity features, has been widely concerned by practitioners and researchers. In view of the disadvantages of the traditional centralized identity authentication method, although some scholars have proposed some identity authentication schemes based on block chain, there are still some shortcomings, such as weak resistance to attacks, non repudiation, non bidirectional authentication, and low authentication efficiency. Therefore, in order to solve the above problems, an identity authentication mechanism based on block chain technology is proposed and implemented. The main research contents are as follows:

This paper studies the technology and principle of block chain, understands the application of block chain in data protection, access control, trust management, device identification, privacy and security mechanism, and designs a new digital identity ID and a new asynchronous Byzantine fault-tolerant algorithm dsbtf by using cryptography, computer network, asynchronous Byzantine fault-tolerant algorithm and so on. The mechanism constructs a block chain transaction transaction and a trust certificate ticket to verify the identity of the device. At the same time, keccak hash algorithm and ECDSA digital signature algorithm are used to ensure the integrity and non repudiation of interactive messages between devices and block chain nodes.

Aiming at the problems and shortcomings of the traditional authentication scheme based on centralization and the existing authentication scheme based on block chain, this paper designs a federated block chain based on ID and dsbtf, designs a decentralized identity authentication system with the block chain as the bottom layer, and compiles the corresponding intelligent contract algorithm and code implementation in each stage of the proposed scheme, With the help of open source hash algorithm and ECDSA digital signature algorithm, the key modules of the system are implemented. Finally, from the perspective of system function test, the validity of the phase of creating trust domain, associated trust domain and authentication is verified.

2. Research and implementation of identity authentication technology based on block chain

Applying public key technology to block chain, this paper proposes an identity authentication system based on block chain. Through the improvement of consensus mechanism, encryption algorithm, and the design of a suitable smart contract to complete the system. The system has the advantages of security, irreversibility, unforgeability, undeniability and transparency. Effectively enhance the credibility of identity authentication. Through the block chain technology, we can effectively complete the digital certificate issuance, update, revocation and other functions, reduce the dependence on the traditional authentication technology on a single certification authority, which is more efficient, more reliable trust relationship, and more secure identity authentication.

2.1. Design objectives

This paper designs an identity authentication system based on block chain, The main functions include issuing certificate, revoking certificate, updating certificate, downloading certificate, querying status, revoking list, changing key of certification authority, and auditing operation of authentication authority identity authentication.

The system has the following characteristics:

First of all, the security of the whole system is high. Each network node of the block chain, registration center, certificate issuing center and public server are all two-way authentication to ensure mutual trust. The internal communication of the system is closed, so it is not easy to be attacked. The design of smart contract can also reflect the security. For example, in the design of rights management, the administrator can do the write operation, while the ordinary user can only do the query operation.

The credibility of the whole system is high. As a third party, the public service organization can monitor the real-time status of the block chain at any time, and improve the credibility of the consistency of each node in the block chain. The nodes of the block chain exist distributed and each node is maintained separately. The public server can establish a trusted site through the system's pre issued certificate to increase the credibility of the query results.

The system is easy to audit. Because the operation of digital certificate is open, transparent and credible, it can easily query all operation records by consensus service, and query by page or by time.

The system has high generality. When designing the smart contract interface, it is consistent with the interface of traditional public key technology infrastructure system to a great extent, which provides convenience for docking with existing public key infrastructure and meets the needs of scenarios.

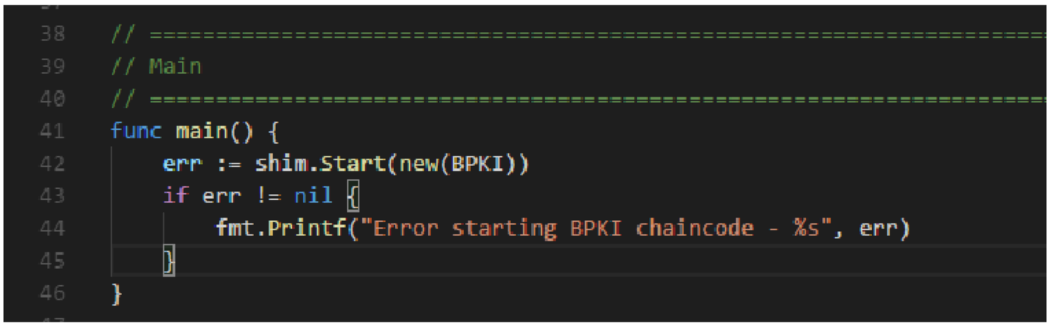
2.2. Smart contract design

A smart contract is a piece of code that can be executed automatically and deployed in a distributed ledger. Smart contract has the characteristics of self consistency, self-sufficiency and distribution. It is defined by code and executed independently [9].

2.2.1. Data structure design. The data structure of the system includes CA certificate linked list, CA operation record table, certificate life cycle table to cooperate with identity authentication, certificate verification and other functions.

2.2.2. Contract function design. Hyperledger fabirc's smart contract is a set of callback functions [10], also known as chain code. These implementations are called back at the appropriate time when the block chain is running.

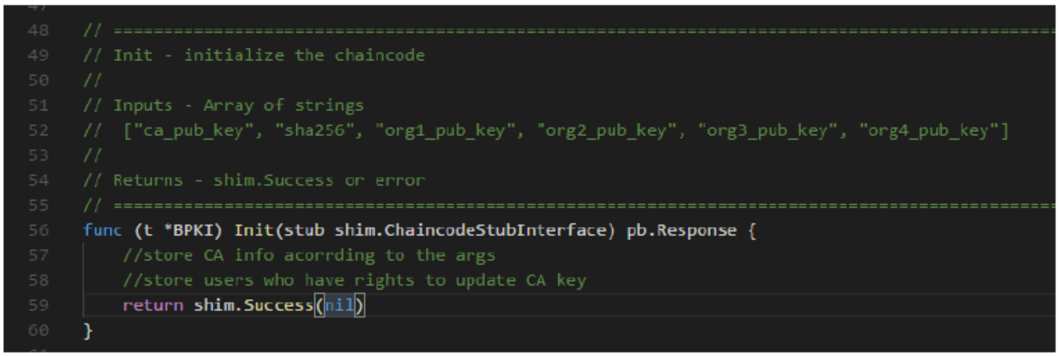
The main function is main. When the smart contract is installed, the block chain will create a container to run the smart contract process, and use the main function as the process entry. The main function can refer to figure 1



```
// ===============================================================
// Main
// ===============================================================
func main() {
    err := shim.Start(new(BPKI))
    if err != nil {
        fmt.Printf("Error starting BPKI chaincode - %s", err)
    }
}
```

Figure 1. Principal function diagram.

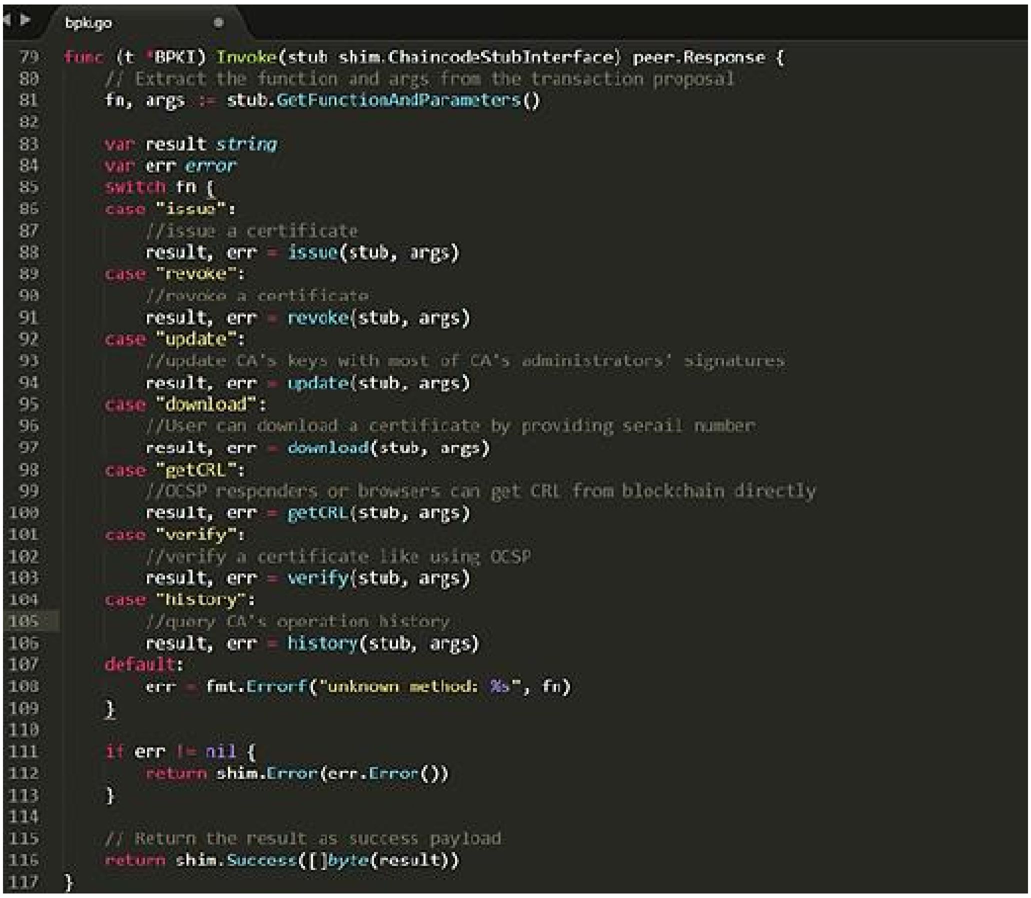
Initialization function init, which will be called by block chain to complete initial configuration when chain code is instantiated. The initialization function is implemented with reference to figure 2.



```go
// =========================================================================================
// Init - initialize the chaincode
//
// Inputs - Array of strings
//  ["ca_pub_key", "sha256", "org1_pub_key", "org2_pub_key", "org3_pub_key", "org4_pub_key"]
//
// Returns - shim.Success or error
// =========================================================================================
func (t *BPKI) Init(stub shim.ChaincodeStubInterface) pb.Response {
    //store CA info acorrding to the args
    //store users who have rights to update CA key
    return shim.Success(nil)
}
```

Figure 2. Initialization function diagram

Call the function invoke, which will be called back when the block link is traded. Refer to figure 3 for calling function implementation.



```go
func (t *BPKI) Invoke(stub shim.ChaincodeStubInterface) peer.Response {
    // Extract the function and args from the transaction proposal
    fn, args := stub.GetFunctionAndParameters()

    var result string
    var err error
    switch fn {
    case "issue":
        //issue a certificate
        result, err = issue(stub, args)
    case "revoke":
        //revoke a certificate
        result, err = revoke(stub, args)
    case "update":
        //update CA's keys with most of CA's administrators' signatures
        result, err = update(stub, args)
    case "download":
        //User can download a certificate by providing serail number
        result, err = download(stub, args)
    case "getCRL":
        //OCSP responders or browsers can get CRL from blockchain directly
        result, err = getCRL(stub, args)
    case "verify":
        //verify a certificate like using OCSP
        result, err = verify(stub, args)
    case "history":
        //query CA's operation history
        result, err = history(stub, args)
    default:
        err = fmt.Errorf("unknown method: %s", fn)
    }

    if err != nil {
        return shim.Error(err.Error())
    }

    // Return the result as success payload
    return shim.Success([]byte(result))
}
```

Figure 3. Call function graph

2.3. *Certificate management*

2.3.1. Issue of certificates. In the process of user authentication, the most important step is to issue the certificate to the user authentication system. The issued certificates and operation records will be written into the block chain to ensure that the data is transparent and can not be tampered with.

2.3.2. Renewal certificate. In the identity authentication system based on block chain, when the user needs to change the domain name or the certificate extension, the user has no right to update the certificate by himself. He can pass the audit of the registration center and call the update interface of the smart contract to update the user's certificate, only the content of the certificate is updated, and the user's public and private keys are not changed.

2.3.3. Revocation of certificate. In the identity authentication system based on block chain, when the user needs to revoke the certificate, the revoke interface of the smart contract is called to revoke the user's certificate after passing the audit. Users can take the initiative to revoke the certificate, or the administrator can revoke the certificate for other reasons, such as certificate expiration or key leakage.

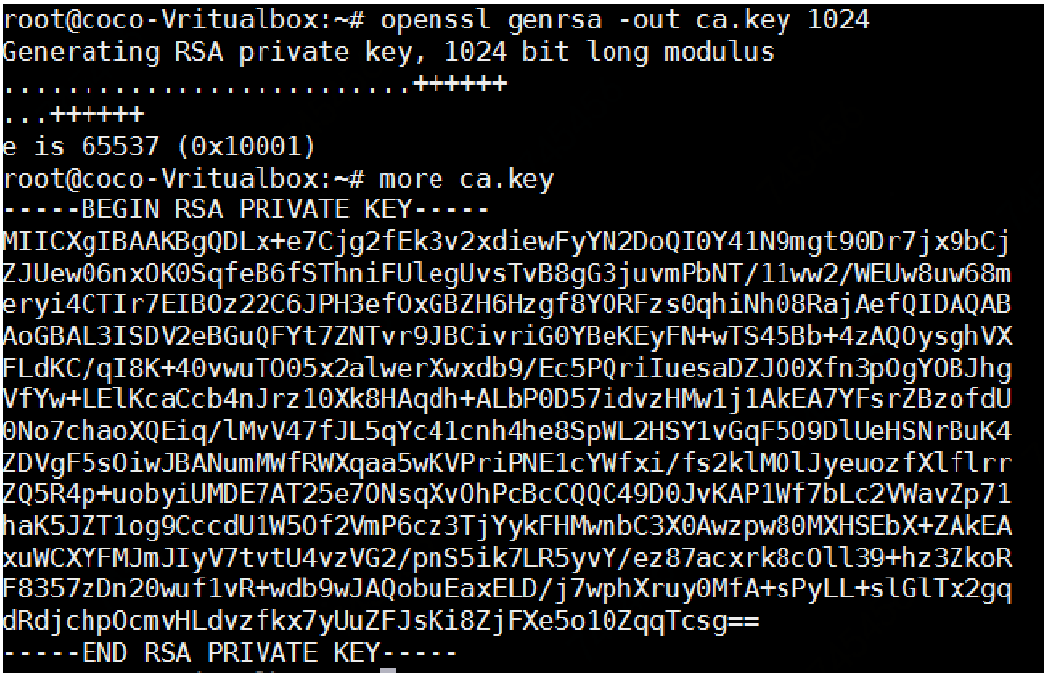
3. Test and verification of identity authentication technology based on block chain

3.1. *Experimental environment*

Vm1 installs registration service, signing and issuing service, publicity service and block chain SDK. Vm2 installs hyperledger fabric network through docker. The network structure of 4per and 1orderer is adopted. The certificates used by all nodes are manually generated offline by the issuing system. To verify the implementation, a browser is used to access the web server in Vm1 on the host.

3.2. *Function test*

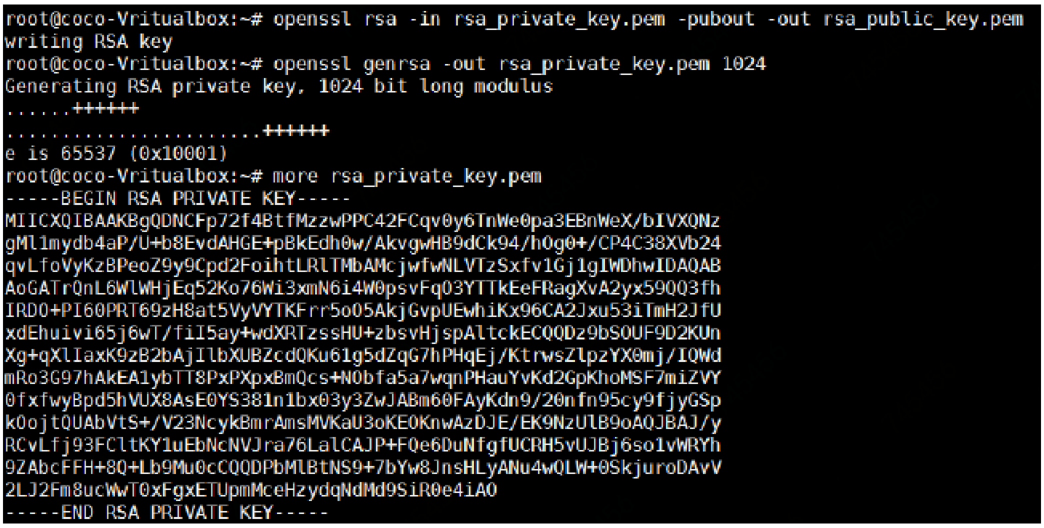
3.2.1. Generate self signed root certificate. The private key generation result of the issuing center is shown in Figure 4.



```
root@coco-Vritualbox:~# openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
...........................++++++
...++++++
e is 65537 (0x10001)
root@coco-Vritualbox:~# more ca.key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDLx+e7Cjg2fEk3v2xdiewFyYN2DoQI0Y41N9mgt90Dr7jx9bCj
ZJUew06nxOK0SqfeB6fSThniFUlegUvsTvB8gG3juvmPbNT/11ww2/WEUw8uw68m
eryi4CTIr7EIBOz22C6JPH3efOxGBZH6Hzgf8Y0RFzs0qhiNh08RajAefQIDAQAB
AoGBAL3ISDV2eBGuQFYt7ZNTvr9JBCivriG0YBeKEyFN+wTS45Bb+4zAQOysghVX
FLdKC/qI8K+40vwuTO05x2alwerXwxdb9/Ec5PQriIuesaDZJ00Xfn3pOgYOBJhg
VfYw+LElKcaCcb4nJrz10Xk8HAqdh+ALbP0D57idvzHMw1j1AkEA7YFsrZBzofdU
0No7chaoXQEiq/lMvV47fJL5qYc41cnh4he8SpWL2HSY1vGqF5O9DlUeHSNrBuK4
ZDVgF5sOiwJBANumMWfRWXqaa5wKVPriPNE1cYWfxi/fs2klM0lJyeuozfXlflrr
ZQ5R4p+uobyiUMDE7AT25e7ONsqXvOhPcBcCQQC49D0JvKAP1Wf7bLc2VWavZp71
haK5JZT1og9CccdU1W5Of2VmP6cz3TjYykFHMwnbC3X0Awzpw80MXHSEbX+ZAkEA
xuWCXYFMJmJIyV7tvtU4vzVG2/pnS5ik7LR5yvY/ez87acxrk8cOll39+hz3ZkoR
F8357zDn20wuf1vR+wdb9wJAQobuEaxELD/j7wphXruy0MfA+sPyLL+slGlTx2gq
dRdjchpOcmvHLdvzfkx7yUuZFJsKi8ZjFXe5o10ZqqTcsg==
-----END RSA PRIVATE KEY-----
```

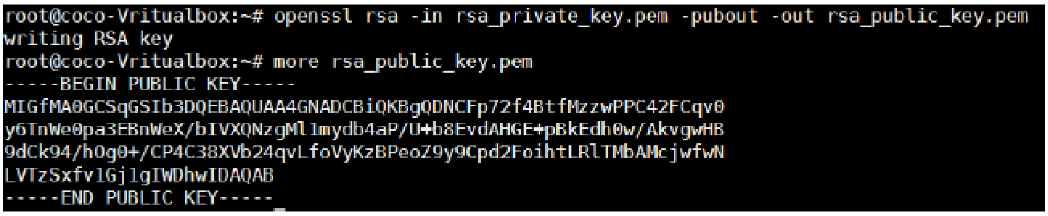
Figure 4. Generate issuing center private key

3.2.2. Certificate issuing process. The user private key generation result is shown in Figure 5.The user public key is generated according to the user private key, as shown in Figure 6.



```
root@coco-Vritualbox:~# openssl rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
writing RSA key
root@coco-Vritualbox:~# openssl genrsa -out rsa_private_key.pem 1024
Generating RSA private key, 1024 bit long modulus
......++++++
.......................++++++
e is 65537 (0x10001)
root@coco-Vritualbox:~# more rsa_private_key.pem
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDNCFp72f4BtfMzzwPPC42FCqv0y6TnWe0pa3EBnWeX/bIVXQNz
gMl1mydb4aP/U+b8EvdAHGE+pBkEdh0w/AkvgwHB9dCk94/h0g0+/CP4C38XVb24
qvLfoVyKzBPeoZ9y9Cpd2FoihtLRlTMbAMcjwfwNLVTzSxfv1Gj1gIWDhwIDAQAB
AoGATrQnL6WlWHjEq52Ko76Wi3xmN6i4W0psvFq03YTTkEeFRagXvA2yx59Q03fh
IRD0+PI60PRT69zH8at5VyVYTKFrr5o05AkjGvpUEwhiKx96CA2Jxu53iTmH2JfU
xdEhuivi65j6wT/fil5ay+wdXRTzssHU+zbsvHjspAltckECQQDz9bS0UF9D2KUn
Xg+qXlIaxK9zB2bAjIlbXUBZcdQKu61g5dZqG7hPHqEj/KtrwsZlpzYX0mj/IQWd
mRo3G97hAkEA1ybTT8PxPXpxBmQcs+N0bfa5a7wqnPHauYvKd2GpKhoMSF7miZVY
0fxfwyBpd5hVUX8AsE0YS381n1bx03y3ZwJABm60FAyKdn9/20nfn95cy9fjyGSp
k0ojtQUAbVtS+/V23NcykBmrAmsMVKaU3oKE0KnwAzDJE/EK9NzUlB9oAQJBAJ/y
RCvLfj93FCltKY1uEbNcNVJra76LalCAJP+FQe6DuNfgfUCRH5vUJBj6so1vWRYh
9ZAbcFFH+8Q+Lb9Mu0cCQQDPbMlBtNS9+7bYw8JnsHLyANu4wQLW+0SkjuroDAvV
2LJ2Fm8ucWwT0xFgxETUpmMceHzydqNdMd9SiR0e4iA0
-----END RSA PRIVATE KEY-----
```

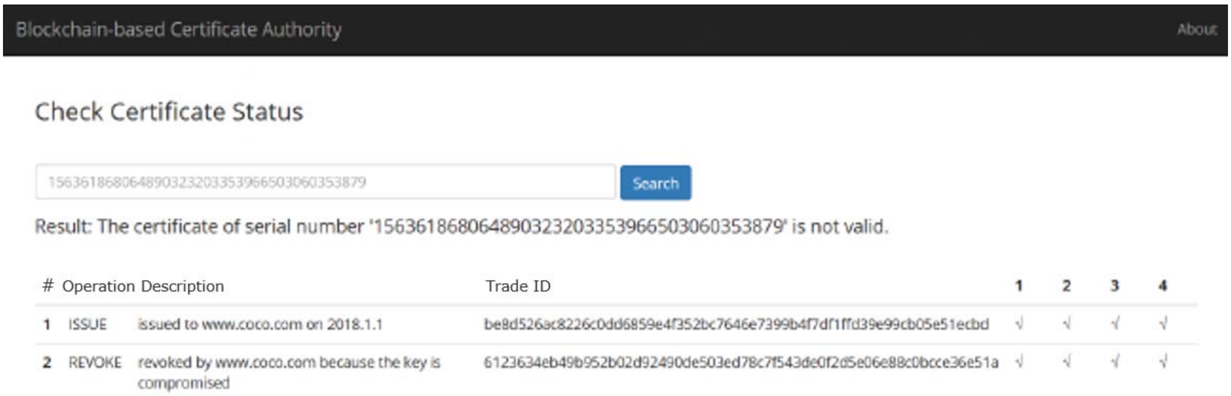
Figure 5. Generate user private key



```
root@coco-Vritualbox:~# openssl rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
writing RSA key
root@coco-Vritualbox:~# more rsa_public_key.pem
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDNCFp72f4BtfMzzwPPC42FCqv0
y6TnWe0pa3EBnWeX/bIVXQNzgMl1mydb4aP/U+b8EvdAHGE+pBkEdh0w/AkvgwHB
9dCk94/h0g0+/CP4C38XVb24qvLfoVyKzBPeoZ9y9Cpd2FoihtLRlTMbAMcjwfwN
LVTzSxfv1Gj1gIWDhwIDAQAB
-----END PUBLIC KEY-----
```

Figure 6. Generate user public key

3.2.3. View Certificate Status. Through the block chain SDK, query requests are sent to four nodes at the same time. As shown in Figure 7, when querying the certificates issued by the system, the nodes 1, 2, 3 and 4 on the right confirm the query certificate data, and show the symbol "√". When the certificate is revoked, the status of the certificate can also be queried. The graph shows that the user revoked the certificate by himself because of the key leakage.



Check Certificate Status

156361868064890323203353966503060353879

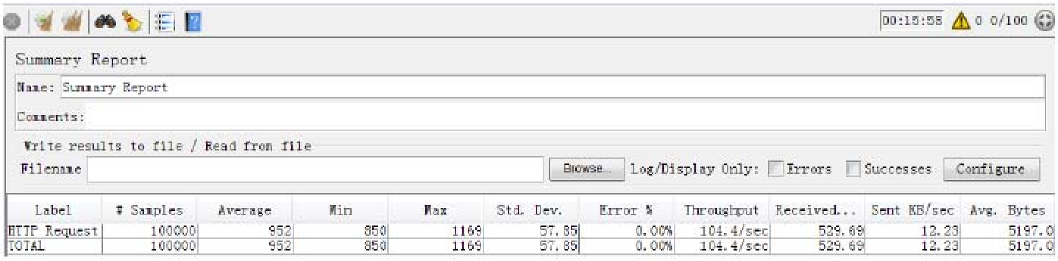
Result: The certificate of serial number '156361868064890323203353966503060353879' is not valid.

#	Operation	Description	Trade ID	1	2	3	4
1	ISSUE	issued to www.coco.com on 2018.1.1	be8d526ac8226c0dd6859e4f352bc7646e7399b4f7df1ffd39e99cb05e51ecbd	√	√	√	√
2	REVOKE	revoked by www.coco.com because the key is compromised	6123634eb49b952b02d92490de503ed78c7f543de0f2d5e06e88c0bcce36e51a	√	√	√	√

Figure 7. Query result graph of digital certificate

3.3. Performance test

Because performance depends on hardware and network and many other factors, this paper tests the most commonly used query function. The specific steps are to set up the experimental environment first, then apply and issue the certificate through the page, and then use the test tool to launch HTTP request to query the certificate. Set 100 threads concurrency, query each thread 1000 times, and then query the next time immediately after returning. The experimental results are shown in Fig. 8.



Summary Report

Name: Summary Report

Comments:

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received...	Sent KB/sec	Avg. Bytes
HTTP Request	100000	952	850	1169	57.85	0.00%	104.4/sec	529.69	12.23	5197.0
TOTAL	100000	952	850	1169	57.85	0.00%	104.4/sec	529.69	12.23	5197.0

Figure 8. Query function test chart

The results were analyzed:

100000 query requests took 15 minutes and 16 seconds, no errors. It can be seen from the results that it is normal for a node to initiate a query and wait for all returned data before returning the final query result. In the actual use environment, the physical delay cost is ignored, and the key is to call the underlying nodes in turn. Therefore, in the actual use environment, the prediction delay is about 1 second. It is acceptable for users to browse the web page. For users who want to improve query performance, there are many methods. For example, OCSP service is one of them [11].

4. Summary and Prospect

4.1. Work summary

This paper first analyzes the disadvantages and shortcomings of traditional authentication technology and existing identity authentication technology, and introduces the new identity authentication technology proposed in this paper to build a better identity authentication system. The main work of this paper is as follows

In this paper, the traditional public key infrastructure technology and the existing identity authentication technology are deeply analyzed, and the improvement strategy of the previous scheme is proposed, and the system security stability is analyzed.

The working principle of block chain is deeply studied, and an improved scheme of identity authentication technology based on block chain is proposed, which makes the system more efficient, more secure and reliable, greatly reduces the dependence of the identity authentication system on the original authentication center, and realizes the open and transparent identity authentication.

The functions of certificate issuing, certificate updating, certificate revocation, user key updating and authentication authority updating are realized. The performance of the system is tested, and the results show that the technology performs well.

Aiming at the problems of key loss and disclosure in traditional certification authority, a suitable smart contract is designed to avoid the security risks caused by certificate expiration and invalidation, user key loss and disclosure or key leakage and expiration of certification authority. It can reduce the possibility of security loopholes in the system and improve the efficiency and security performance of system authentication.

4.2. Research prospect

Although this paper puts forward an improved scheme for the current technology, it has many excellent characteristics compared with the previous system. However, due to the difficulties in the research and application of the technology, there are still some areas for further improvement. This study can be further studied in the following directions.

It is suitable for complex authentication architecture. It makes the research adapt to larger scale and more complex application scenarios.

Optimize the underlying consensus algorithm of block chain to improve the business processing capacity of the system. A better consensus algorithm is designed for different scenarios.

A new compound cipher algorithm is designed to improve the system security against new quantum computing attacks.

Improve the adaptability and scalability of the system. Provide more detailed interface design for a variety of traditional identity authentication, and enhance system compatibility.

References

[1] Cheng Nuo. Research and implementation of identity authentication technology based on block chain in centreless network [D]. Xi'an University of Electronic Science and technology, 2018

[2] Wang naizhou, Jin Lianwen, Gao Bing, Jin Xiaofeng. Research on identity authentication and storage method based on blockchain technology [J]. Modern information technology, 2020,4 (08): 164-167Pilkington. M, Blockchain Technology: Principles and Applications, J. Social Science Electronic Publishing, 2016.

[3] Nash A, Duane W, Joseph C. PKI: Implementing and Managing E-security[M]. McGraw-Hill, Inc., 2001.

[4] Ellison C, Schneier B. Ten risks of PKI: What you're not being told about public key infrastructure[J]. Comput Secur J, 2000, 16(1): 1-7

[5] Ducklin P. The TURKTRUST SSL certificate fiasco-what really happened, and what happens next[J]. Naked Security. SOPHOS, 2013, 8.

[6] Song Xianrong, Zhang Meng. Research on network trusted identity authentication technology [J]. Cyberspace Security, 2018,9 (03): 69-77

[7] Zhang Xiaohan. Research on identity authentication protocol of Internet of things based on blockchain [D]. University of science and technology of China, 2019

[8] Zhang Xiaowei. Design and implementation of Internet of things security authentication system based on blockchain [D]. Southwest Jiaotong University, 2019

[9] Magazzeni D, McBurney P, Nash W. Validation and Verification of Smart Contracts: A Research Agenda[J]. Computer, 2017, 50(9): 50-57.

[10] Cachin C. Architecture of the Hyperledger blockchain fabric[C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.

[11] Myers M, Ankney R, Malpani A, et al. X. 509 Internet public key infrastructure online certificate status protocol-OCSP[R]. 1999.