SCTIM: A Trusted Identity Model Based On Smart Contract

Junze Xu* and Danwei Chen
School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu Province, China

*Corresponding author e-mail: xunjze_nj@keyaninfo.com

Abstract. The anonymity of blockchain identities brings security risks to transactions. To solve this problem, this paper proposes a trusted identity model based on smart contracts and introduces the CA certificate of the PKI system to endorse the authenticity of the user’s identity. The model structure is designed, the blockchain digital certificate format is given, the cross-domain authentication scheme based on smart contracts is described, and the security and efficiency of the model are analyzed. In terms of security, the model meets the needs of entity verification; in terms of efficiency, the use of a hash algorithm to construct a complete certificate chain, compared with existing solutions, significantly improves the efficiency of cross-domain authentication.

Keywords: Blockchain, Smart Contracts, Public Key Infrastructure, Cross-Domain Authentication

1. Introduction
In recent years, with the development of computer technology, blockchain technology has received more attention and applications due to its many excellent characteristics. With its advantages in common maintenance, traceability, and non-tamperability, blockchain technology has played an important value in applications in many fields[1]. With these advantages, it helps to solve the trust problem between different institutions, different systems, and different regions. As a computer transaction protocol[2], smart contracts have attracted much attention in recent years with the popularity of blockchain technology, and related research and applications continue to increase. Its features of decentralization, self-verification, and automatic execution of contract terms significantly improve the level of transaction automation.

The anonymity of blockchain identity[3] hides the real identity of actual users and brings certain risks to real business transactions. In order to ensure the security of transactions and solve this hidden risk, it is necessary to introduce a trusted identity system. One of the strategies is to introduce PKI identities and use CA-certified digital certificates to ensure the credibility of blockchain account identities. However, the traditional PKI is complicated to construct a certificate chain. How to realize cross-domain authentication on the blockchain is the current research point.

2. Related Work
The core of the application of PKI technology to identity authentication is public key cryptography. To build a trust system between different PKI trust domains. Traditional schemes such as reference[4] summarized structures including hierarchical model, mesh model, bridge CA model and so on. Reference[5] uses the elliptic curve algorithm to complete the signature, which improves the cross-domain efficiency compared with the traditional bilinear pairing operation. Reference[6] creates a virtual bridge CA through the elliptic curve threshold signature, which reduces the cost of using bridge CA in the traditional scheme and meets the mobile terminal’s cross-domain requirements.

In the process of continuous development of blockchain technology, blockchain technology has been applied to a certain extent in the field of identity authentication, and has gradually achieved a large number of application results. Reference[7] uses Bitcoin to design a decentralized PKI certification system that uses Certcoin to replace CA; reference[8] addresses the above-mentioned solution information leakage problem and designs a privacy-protected Certcoin scheme, which integrates authentication with privacy protection Function to avoid leakage or loss of user information. Reference[9] designed a new PKI authentication system based on the Ethereum platform. Reference[10] designed a cross-domain scheme of consortium chain using blockchain root certificates to share applications in distributed systems.

3. SCTIM Architecture

In order to solve the problem of blockchain identity credibility, it solves the complex construction of certificate chain authentication of digital certificates in the traditional PKI/CA model, and the cumbersome cross-domain authentication. This paper proposes a Smart Contract based Trusted Identity Model (SCTIM) based on blockchain smart contracts to solve these problems. Utilizing the decentralized and non-tamperable characteristics of smart contracts, the model is designed with a blockchain architecture, and a blockchain digital certificate management method is proposed. On this basis, a new trusted identity registration on-chain scheme and a cross-domain identity authentication scheme are proposed.

3.1 Model Design

3.1.1 SCTIM Model. The SCTIM model is shown in the figure 1. The root CA transfers the trust relationship layer by layer in the trust domain. Different from the traditional PKI system that constructs a certificate chain through certificate signatures, the SCTIM model uses the certificate hash value list published by each layer of issuers to implement the certificate chain construction. When a user performs identity authentication, he obtains the hash list of the CA issuing the blockchain certificate and compares it with the current certificate hash value to verify the validity and authenticity of the certificate (See Figure 2). When performing cross-domain authentication, the authentication can be completed by obtaining the trusted root CA blockchain certificate hash value list published by the central node, and comparing and obtaining the root CA certificate hash value of the opposite user.

![Figure 1. SCTIM model](image1.png)

![Figure 2. Blockchain digital certificate](image2.png)
3.1.2 Model participation role. (1) Central node: The central node is the node with the highest authority in the identity authentication system, responsible for the authentication of the root CA account. Due to the consensus mechanism in blockchain public chain transactions, it is difficult to ensure absolute security. The introduction of a central node can ensure the authenticity of the root CA account.

(2) CA users: According to the trust level in the PKI domain, CA users are divided into root CA, ordinary CA and so on. The root CA verified by the central node is responsible for managing the blockchain digital certificate of the lower CA. Ordinary CAs that have successfully registered manage the blockchain digital certificates of ordinary users.

(3) Ordinary users: Compared with CA users, ordinary users do not have the authority to issue certificates, who are the actual users of blockchain digital certificates in the system.

3.2 Blockchain Digital Certificate

In the traditional PKI/CA system, in order to ensure that the digital certificate is not tampered with, it is necessary to digitally sign the certificate through a higher-level CA to ensure that the identity information of the certificate holder corresponds to the public key one-to-one. As a trusted machine, the blockchain has the characteristics of security and cannot be tampered with. Therefore, compared with the conventional X.509 certificate, the blockchain digital certificate in the model changes the signature verification function to compare hash value, and forms a certification chain by calculating the hash value of the blockchain certification. Hash value forms a verification chain. This model uses the decentralization feature of the blockchain to publish the hash value of the digital certificate under the issuer’s blockchain account, and the security and anti-counterfeiting of the certificate can be determined by calculating the hash value of the certificate and simply comparing the published number. So this model does not need digital signature and signature algorithm module.

The URL module of the revocation check service is also cancelled in the blockchain digital certificate of this model. For certificate revocation, as the blockchain is time-sequential and can never be tampered with, the issuer only needs to update the hash value of the certificate published by himself in this model, and can carry out full life cycle management of the blockchain digital certificate by using the characteristics of the blockchain.

4. SCTIM Cross-domain Identity Authentication Mechanism

4.1 Trusted Identity On-Chain Design

Trusted identity on-chain means that a user builds a virtual digital identity in the blockchain to realize the association and binding of offline identities and on-chain identities. On-chain identity is a prerequisite for user identity management and identity authentication. The scheme of this article is divided into three parts: identity registration contract release, identity information registration, identity information inquiry and authentication. The issuance of the identity registration contract is a process in which the central node deploys or updates the identity registration contract based on the information of the registered domain CA account. Identity information registration is a process in which system users register their identity information on the blockchain through the CA account or central node of the registered domain and obtain a blockchain certificate. Identity information query authentication refers to the process in which the service provider will obtain the blockchain digital certificate account and query it on the chain based on the account address information, and compare the query result with the hash value information published by the issuing CA. Among them, cross-domain authentication includes an authentication protocol for users in a trusted domain. Using the central node to obtain a list of trusted root CA certificate hash values, cross-domain authentication between different root CAs has been achieved.

4.2 Contract Deployment and Identity Registration
The system is initialized, the central node registers account information, and the smart contract for identity registration is deployed. System user registration identity, where the root CA first registers the identity, the root CA is responsible for the identity registration of the lower-level sub-CAs, and finally each sub-CA is responsible for managing the life cycle of ordinary users’ blockchain digital certificates.

(A) Root CA registration

(1) The root CA registers a blockchain account and obtains the public key EPKCA and private key ESKCA of the blockchain account. Provide its own Base64 standard encoded digital certificate and Ethereum account address, and apply to the central node to become a registered node. The central node will be responsible for recording all successfully registered root CA accounts.

(2) The central node uses the provided digital certificate to verify the qualification of the CA center. After passing, add the legal root CA account address to the system registered account list VaildCA, and mark the mapping result as true. Issue a blockchain digital certificate for the account, including the certificate serial number, user account, user blockchain public key, user CA public key, central node address and other information. Calculate the hash value of the blockchain digital certificate, and update the hash value to the CertList of the issued certificate list of its own account.

(B) System user registration

(1) System users include sub-CA users and ordinary users. First register a blockchain account and obtain the public key EPKU and private key ESKU of the blockchain account. If you have ever obtained a certificate, submit your own Base64 standard-encoded digital certificate to the registered domain trusted CA user (the account address marked as true in the VaildCA list). Individual users who register for the first time, submit identity information, including personal information, ID number and other information.

(2) The CA node accepts the verification information and confirms that it is true and valid. Issuing blockchain digital certificates, including the certificate serial number, user account, user blockchain public key, user CA public key, verification CA node address and other information. Calculate the hash value of the blockchain certificate and update the hash value to the CertList of the issued certificate list of its own account.

4.3 Cross-domain Authentication Scheme

Cross-domain identity authentication refers to the authentication process in which users request to obtain blockchain digital certificates from other domains (See Figure 3). This model takes B domain user UB to perform cross-domain authentication for A domain user UA as an example. In order to simplify the process, take the user certificate issued by the root CA user as an example to introduce the cross-domain authentication protocol of the model. The protocol process mainly includes user UA request service , The user UB verifies the UA blockchain digital certificate certificate, and UB verifies the issuance of the CA certificate in three stages.
Figure 3. Cross-domain authentication agreement

The specific agreement is as follows:

The first step request access stage
1) M1: UA→UB: request service
A domain user UA sends a service request, requesting the B domain user UB service.
2) M2: UB→UA: {R1}
   After receiving the request from the user UA, the user UB in the B domain responds to the request and sends the random number R1 to the user UA in the A domain.

The second step is to verify the user’s UA blockchain digital certificate
1) M3: UA→UB: {Sign(R1)}
   (i) A domain user UA receives a response from a B domain user UB, and the user UA uses the CA private key skUA to sign the random number R1 to generate Sign(R1), and sends the signature to the B domain user UB;
   (ii) The B domain user receives the message and confirms whether the random number R1 is valid;
2) M4: UB→SC: {addressUA}
3) M5: SC→UB: {CertUA}
   (i) The B domain user retrieves the blockchain certificate information from the smart contract according to the user UA’s blockchain user address.
   (ii) B domain users use the obtained UA blockchain certificate CA public key and random number to verify whether the signature is valid. Parse the CA user address information issued in the blockchain digital certificate.
4) M6: UB→SC: {addressCA}
5) M7: SC→UB: {CertCA, CertList}
   (i) The B domain user retrieves the CA user’s blockchain digital certificate and the published certificate hash value list from the smart contract according to the obtained CA user address. Check whether the calculated user UA certificate hash value is in the list.
   a. If there is no consistent result, the blockchain certificate provided by the user is abnormal and the authentication fails.
   b. If the comparison is consistent, confirm that the current certificate is indeed issued by the CA user, and continue to request verification of the trustworthiness of the CA user’s blockchain digital certificate.

The third step is to verify the CA certificate
1) M8: UB→SC: {addressCenter}
M9: SC→UB: {CertList}
   (i) The B domain server retrieves the certificate hash value list of the central node from the smart contract. Compare and calculate whether the hash value of the CA user’s blockchain certificate is in the list.
      a. If there is no consistent result, the blockchain certificate provided by the current CA user is abnormal. The CA user is not a system trusted CA, and the authentication fails.
      b. If the comparison is consistent, the verification is passed, the A domain user UA passes the cross-domain authentication of the B domain user UB, and the B domain user provides services for the A domain user.
   Similarly, the above scheme can be used to complete the cross-domain authentication of the user UA to the user UB. Achieve two-way authentication.

5. Scheme Analysis

5.1 Safety Analysis
(1) Prevent replay attacks
   When the external account of Ethereum transmits messages through smart contracts, a nonce will be added to prevent replay attacks.
(2) Certificate ownership and authenticity
   The blockchain certificate designed by this model is different from the traditional certificate signature design. It uses each issuer to hash the certificate and publish it in the certificate list issued by the smart contract to realize the establishment of the certificate chain. Blockchain uses consensus algorithms to build a trust system through different nodes, instead of third-party trust reliability. Blockchain storage ensures that the digital certificate is real, and the certificate ownership can be determined through the issuer’s published certificate hash list.
(3) Two-way authentication
   Based on the digital certificate model of the smart contract, during cross-domain authentication, both parties use the smart contract to query the hash value to construct a certificate chain and establish a trust relationship. Due to the immutable nature of the blockchain, both parties can trust the existence of the digital certificate published by the blockchain. Using smart contracts, mutual trust transactions between users of two domains can achieve mutual verification.
(4) Prevent single point of failure
   The distributed and decentralized characteristics of blockchain technology ensure that the failure of a single node will not affect the security of the entire storage. Compared with traditional servers, it avoids the problem of single points of failure. Anyway, because of a single node failure, the system cannot provide services normally, which greatly ensures the security of the system’s identity.

5.2 Performance Analysis

| Scheme            | Public key encryption and decryption | Digital signature and verification | Hashing |
|-------------------|-------------------------------------|-----------------------------------|---------|
| Reference Error!  | 2                                   | 4                                 | 10      |
| Reference source not found. |                    |                                   |         |
| Reference Error!  | 0                                   | 4                                 | 2       |
| Reference source not found. |                        |                                   |         |
| This paper SCTIM   | 0                                   | 2                                 | 6       |

Table 1. Computation overhead

Compared with the traditional PKI cross-domain reference[5], this model has a significant reduction in public key encryption and decryption and digital signature (See Table 1). Under the premise of the same password protection capability, using the same machine for testing, the SM2 algorithm runs more efficiently than the traditional RSA algorithm. The hash algorithm SHA-256 used
is also much higher than the asymmetric encryption RSA algorithm, and the speed is even dozens of times faster. Therefore, the execution performance of the scheme in this paper is much better than that in the reference[5], and as the number of trust domains increases, the cross-domain authentication efficiency of this model will significantly lead the reference [5].

Compared with the blockchain alliance chain reference[10], this model updates all digital certificates to the blockchain, changing the authentication method between the user and the CA. The model introduced the domestic SM2 algorithm in the signature encryption performance is far better than the ECDSA-192 algorithm, and the model compared to the reference[10] reduced the number of signature algorithms. Due to the high execution efficiency of the hash algorithm, although the number of times of the hash algorithm is increased in the digital certificate verification process, the overall efficiency of the system still exceeds that of the reference[10]. Due to the limited performance of the blockchain itself, it is necessary to use hash algorithms in the authentication process of digital certificates, which also makes it feasible to use blockchain technology to build the entire PKI system. Therefore, the cross-domain authentication of this scheme has strong practical significance.

6. Summary
This paper proposes a blockchain-based trusted identity on-chain scheme. Use smart contracts to implement a cross-domain authentication model. This model does not change the PKI system architecture in the original domain, and realizes the construction of trust relationships between domains through the blockchain smart contract platform. Introduce the digital certificate certified by the CA based on the national secret algorithm into the blockchain transaction to ensure the legal compliance of the public chain transaction. Compared with existing cross-domain authentication schemes, this scheme uses smart contracts on the basis of ensuring security, instead of the mutual issuance of certificates and verification signatures in the traditional PKI, and improves the efficiency of cross-domain authentication. The model level is clear and the scalability is strong.

References
[1] China Blockchain Technology and Industrial Development Forum. China Blockchain Technology and Application Development White Paper, 2018
[2] Liwei Ouyang, Shuai Wang, Yong Yuan, Xiaochun Ni, Feiyue Wang. SmartContracts: Architecture and Research Progresses, Acta Automatica Sinica, Vol.45, No.03, PP.445-457, 2019.
[3] Liehuang Zhu, Feng Gao, Meng Shen, Yandong Li, Baokun Zheng, Hongliang Mao, Zhen Wu. Survey on Privacy Preserving Techniques for Blockchain Technology, Journal of Computer Research and Development, Vol.54, No.10, PP.2170-2186, 2017.
[4] Linn J . Trust Models and Management in Public-key Infrastructures. RSA laboratories, December, 2000.
[5] Changyuan Luo, Shiwai Huo, Hangzhi Xing. Identity-based Cross-domain Authentication Scheme in Pervasive Computing Environments, Journal on Communications, Vol.32, No.9, PP.111-115, 2011.
[6] Wenfang Zhang, Xiaomin Wang, Wei Guo. An Efficient Inter-Enterprise Authentication Scheme for VE Based on the Elliptic Curve Cryptosystem, Acta Electronica Sinica, Vol.42, No.6, PP.1095-1102, 2014.
[7] Fromknecht C, Velicanu D, Yakoubov S. Certcoin: A namecoin based decentralized authentication system[EB/OL]. 2014[2018-04-10]. [online] Available: http://courses.csail.mit.edu /6.857 /2014 /files/19-fromknecht-velican-yakoubo-certcoin. pdf
[8] Axon L M, Goldsmith M. PB-PKI: a privacy-aware blockchain-based PKI. 2016.
[9] Lewison K, Corella F. Backing Rich Credentials with a Blockchain PKI. Technical Report, Pomcor, 2016. [online] Available: https://pomcor.com/techreports/BlockchainPKI. pdf, 2018.
[10] Zhicheng Zhou, Lixin Li, Zuohui Li. Efficient Cross-domain Authentication Scheme Based on
Blockchain Technology, Journal of Computer Applications, Vol.38, No.02, PP316-320+326, 2018.