A Privacy-Aware PKI System Based on Permissioned Blockchains

Rong Wang
Digital Society & Blockchain Laboratory
Beihang University, Beijing, P. R. China
wangrong@buaa.edu.cn

Juan He, Can Liu and Qi Li
Digital Society & Blockchain Laboratory
Beihang University, Beijing, P. R. China
{xiongbao_hj, liucan & liqi7}@buaa.edu.cn

Wei-Tek Tsai
Digital Society & Blockchain Laboratory
Beihang University, Beijing, P. R. China
Beijing Tiande Technologies
No.l S Suzhou Street, Haidian District, Beijing, China
tsai7@yahoo.com

EnyanDeng
Beijing Tiande Technologies
No.l S Suzhou Street, Haidian District, Beijing, China
deng@tiandetech.com

Abstract-Public key infrastructure (PKI) is the foundation and core of network security construction. Blockchain (Be) has many technical characteristics, such as decentralization, impossibility of being tampered with and forged, which makes it have incomparable advantages in ensuring information credibility, security, traceability and other aspects of traditional technology. In this paper, a method of constructing PKI certificate system based on permissioned BC is proposed. The problems of multi-CA mutual trust, poor certificate configuration efficiency and single point failure in digital certificate system are solved by using the characteristics of BC **distribution** and non-tampering. At the same time, in order to solve the problem of identity privacy on BC, this paper proposes a privacy-aware PKI system based on permissioned BCs. This system is an anonymous digital certificate publishing scheme, which achieves the separation of user **registration** and authorization, and has the characteristics of anonymity and conditional traceability, so as to realize to protect user's identity privacy. The system meets the requirements of certificate security and anonymity, reduces the cost of CA **construction,** operation and maintenance in traditional PKI technology, and improves the efficiency of certificate application and configuration.

Keywords-component; public-key infrastructure; permissioned blockchains; privacy-awareness; security; digital certificate

I. INTRODUCTION

Public key infrastructure (PKI) is the foundation and core of network security construction, which is the basic guarantee of the implementation of e-commerce security [1]. PKI technology is used in many fields such as secure email, virtual private network, e-commerce, e-govemrnent, and etc. PKI technology uses certificate management public key, binds the user's public key with other user identification information (such as name, e-mail, identity card number, etc.) through the third party's trusted authentication certificate authority (CA), verifies the user's identity on the Internet, and transmits the user's identity through CA Digital information is encrypted to ensure the confidentiality and integrity of information transmission, and the authenticity and denial of identity are guaranteed by signature, A complete PKI system consists of certification authority, registration authority (RA), digital certificate library, certificate revocation system, application interface (API) and so on [2]. As shown in Figure 1.

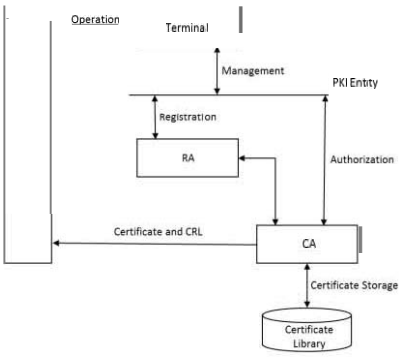

Figure 1. PKI architecture

In PKI technology, the certificate authority (CA) is the starting point of trust. Only by trusting a CA, can we trust the digital certificate issued by the CA to users. However, in specific applications, PKI technology has the following problems.

(1) Single point failure. The core CA is vulnerable to attack Once controlled, the CA root certificate and the certificate issued by the CA are no longer trusted [1].

(2) Poor efficiency of certificate deployed. When users configure and use certificates, they need to first apply for certificates from CA After the certificates are issued by CA, users need to configure or install the certificates to the target device or server. In some occasions where batch operation is required, the efficiency of batch configuration equipment certificate is low due to the individual difference between private key and certificate, and the security and confidentiality

978-1-5386-6565-7/18/$31.00

requirements in the configuration process introduce management overhead and cost [3].

(3) Multi CA mutual trust problem. User certificates can only be validated by the root certificate of the CA to which they belong. Different CAs cannot verify each other. The applicability of existing CA mutual trust solutions are limited. In PKI system, the methods to solve the problem of mutual trust in CA include authoritative CA list, CA cross-certification, bridge CA, etc. In addition, when users configure and use certificates, they need to apply for certificates from CA first. After the certificates are issued by CA, users need to configure or install the certificates to the target device or server [4].

The BC is a new technology system derived from the underlying technology of Bitcoin. The earliest definition comes from the paper published by Satoshi Takemoto in 2009 [5]. BC has many technical characteristics, such as decentralization, impossibility of being tampered with and forged, which makes it have incomparable advantages in ensuring information credibility, security, traceability and other aspects of traditional technology [6]. ABC-based PKI system ensures that certificates on the write BC are trusted. It can be used for the issuance and management of self-signed digital certificates across multiple organizations, and can also be used to replace multiple instances of bridge CA connections that use different CAs to issue certificates.

The content of this paper is organized as follows: Section 2 introduces the relevant technical background; Section 3 presents a privacy-aware PKI system based on permissioned BCs; Section 4 discussion and analysis; Section 5 The work was summarized.

II. BACKGROUND

A. Permissioned BCs

Permissioned BCs refers to a BC that is managed by several organizations, each of which runs one or more nodes [7]. Only nodes are permitted to voting, accounting, and building blocks. Each node in the BC usually has a corresponding entity or organization, participants join the network by authorization and form a stakeholder alliance to jointly maintain the operation of the BC The data only allows different organizations in the system to read, write and send transactions, and jointly record transaction data. It has the advantages of high transaction speed, no need for mining, low transaction cost, and support for supervision.

The permissioned BC can use the Concurrent Byzantine Fault Tolerance (CBFT) algorithm, which is a Byzantine fault-tolerant algorithm with four communication faces for block building [8]. In the case of hacker attacks, it can guarantee data is difficult to be tampered with to ensure data security.

The permissioned BC can use dual-chain architecture, which has good scalability. The dual-chain architecture of the BC system is composed of Account BC (ABC) and transaction BC (TBC). ABC is used to store user data hash after encryption and TBC is used to process transactions [9].

B. Multi-signature

Multi-signature is a digital signature scheme which allows a group of users to sign a single document [10]. Usually, a multi-signature algorithm produces a joint signature that is more compact than a collection of distinct signatures from all users.

In the multi-signature, the signer is composed of a plurality of the same plaintext as a part of the signature, then the signature will be integrated into a multi-part signature. If an address can only be signed and paid by one private key, the form is 1/1 and the form of multiple signatures is *min*, that is to say, a total of n private keys can sign an account, and when m addresses are signed, a transaction can be paid. In some specific scenarios, some important documents need to be confirmed by multiple signers before they can take effect. Each signature group member use their own key to confirm the transaction information, and then the system synthesizes the processing results as the signature information of the whole signature group. The verification in the network only needs to know. Any public key in the signature group can verify the validity of the signature.

III. A PRIVACY-AWARE PKI SYSTEM BASED ON PERMISSIONED BLOCKCHAINS

A. System Architecture

Different CA organizations form a BC to create and maintain a unified certificate that is recognized by authorization, and to ensure real and effective data sharing, to ensure that the real data cannot be tampered with. Distributed nodes are constructed by BC technology, which will allow CA organizations in different regions to join the BC network. CAs provide certificate issuance and validation through consensus mechanism. Consensus certificates will be recorded in the BC These certificates are all CA-approved certificates in the BC, and the whole BC will become. A joint certificate verification alliance across CA can replace point-to-point CA bridges to establish secure communication channels between different CA systems, which simplifies management and implementation costs.

However when all organizations are on a BC, the privacy of user is hard to guarantee. The real name of the certificate holder will be marked in the BC When the certificate holder presents the certificate to the service provider or site, the real identity information of the user will be disclosed. So it is difficult to use anonymous services to protect user's privacy, such as online trading or electronic voting.

We propose a privacy-aware PKI system based on permissioned BCs. As shown in Figure 2, the system consists of registration BC (RBC), certificate BC (CBC) and user. The RBC node is responsible for user identification, encrypting user identity information and storing authenticated user data after encryption. The CBC node is responsible for user legality authentication, and then certificates with authentication information and service information to users and stores anonymous digital certificates, and stores anonymous digital certificate data. And store anonymous digital certificate data.

Identify applicable sponsorls here. Ifno sponsors, delete this text box. (sponsors)

The CBFT consensus is adopted in each BC to ensure the consistency and difficult modification of information between the nodes, and to ensure the consistency of the BC itself [11]. Each BC has its own consensus mechanism, each maintaining its own consistency [12].

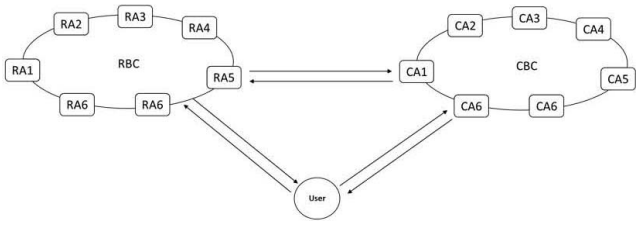

Figure 2. System architecture

The BC system is consists of four parts: storage layer, BC core layer, BC service layer and BC interface layer. As shown in Figure 3.

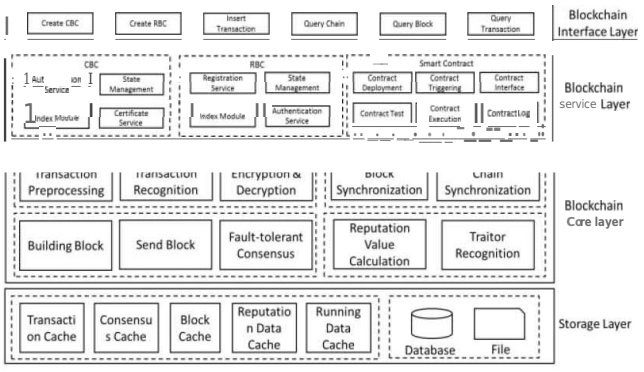

Figure 3. Be architecture

The storage layer is responsible for various cache data storage and persistent storage of BC data. The data storage layer supports multiple databases, such as Redis, MySQL, HBase, and LevelDB. The BC core layer is responsible for the core functions of the BC such as consensus mechanism, reputation mechanism, transaction preprocessing, encryption and decryption, signature verification, authentication management, and etc. The service layer includes CBC, RBC, and smart contract. The RBC node is responsible for user identification, encrypting user identity information and storing authenticated user data after encryption. The CBC node is responsible for user legality authentication, and then certificates with authentication information and service information to users and stores anonymous digital certificates, and stores anonymous digital certificate data. The smart contract provides functions such as contract deployment, contract execution, contract triggering and contract testing. The interface layer is responsible for providing the BC platform service interface to the application layer, providing various services for the application layer.

B. System Work Flows

1) *Application for Digital Certificate*

(a) The user fills in the relevant certificate application information through the client, generates the signature key pair after completion, and signs the filled data, and authenticates the identity to RBC. The client sends the authentication request to the consensus nodes of RBC.

(b) Each consensus node of RBC receives the user's identity verification request and verifies the signature. Each consensus node verifies the user's identity and sends the verification results to other nodes.

(c) Every consensus node of RBC votes after receiving the results of other nodes. If the number of nodes passing the verification result is larger than 2/3 of the total node, the verification is passed, and the user information is encrypted multiple times. The encrypted data is stored on RBC and the successful anonymous user identity is sent to the client. . If the node passing the verification result is less than 2/3 of the total node, the verification fails and the failed message is returned.

(d) The client receives RBC information. If the identity registration is successful, the client signs the anonymous user identity information and sends certificate application requests to the consensus nodes of CBC.

(e) Each consensus node of CBC receives a certificate request to verify the user's signature. Each consensus node searches the user's identity in RBC according to the user's public key, verifies the user's anonymous identity, and sends the results of authentication to other nodes.

(f) The consensus nodes of CBC vote after receiving the results of other nodes. If the number of nodes passing the verification results is larger than 2/3 of the total nodes, the verification is passed. The anonymous CA is sent to the user and the anonymous CA is recorded on CBC.

(g)The user downloads and installs the certificate.

2) Revoke Digital Certificate

Anonymous certificates need to be revoked when anonymous certificates are found to be abused, private key leaks or certificates expire. The steps to revoke anonymous certificates are as follows:

(a) User send anonymous requests to the CBC consensus nodes through the client.

(b) Each consensus node of CBC receives the user's request to revoke anonymous certificate and verifies the signature. Each consensus node traces the user's identity through the anonymous certificate tracing function, verifies the identity and sends the results of identity verification to other nodes.

(c) Each consensus node of CBC receives certificate application request to verify the user's signature. Each consensus node searches the user's identity in RBC according to the user's public key, verifies the user's anonymous identity, and sends the verification results to other nodes.

(d) The consensus nodes of CBC vote after receiving the results of other nodes. If the number of nodes passing the verification results is larger than 2/3 of the total nodes, the verification will pass. The user's anonymous CA is revoked and recorded on CBC.

(e) Return the execution result to the user.

3) Tracking Digital Certificates

When an anonymous certificate is found to be abused, the service provider can request the CBC consensus node to track

the anonymous certificate. The tracking steps for anonymous certificates are as follows:

(a) When an anonymous certificate issued by the CBC is obtained, the user can use this traceable anonymous certificate to register or verify with the service provider.

(b) If abuse of anonymous certificates is detected, service providers send requests for revocation of users' anonymous certificates to all CBC nodes.

(c) Each node of CBC receives the request from the service provider, and each node of CBC will track and review the anonymous certificate of the user. And the results of the review are sent to other nodes.

(d) The consensus nodes of CBC vote after receiving the results of other nodes. If the result of revocation of certificate is larger than 2/3 of the total node, the verification is passed. The user's anonymous CA is revoked and recorded on CBC

(e) Return the execution result to the service providers and users.

IV. SYSTEM ANALYSIS

A. Anonymity

REC node is responsible for user identification, encrypting user identity information and storing authenticated user data after encryption. CBC node is responsible for user legitimacy authentication. Then, it issues certificates with authentication information and service information to users and stores anonymous digital certificates, and stores anonymous digital certificate data. User identity authentication and legitimate authorization are realized by using different license chains, thus the separation of user identity authentication and legitimate authorization is realized.

B. Safety

Traditional CA is vulnerable to attack. Once controlled, the CA root certificate and the certificate that the CA has issued are no longer trusted. The license chain is used to construct the storage digital certificate system. Certificates and states exist on the BC after verification and consensus of the nodes, and are collectively maintained by the consensus nodes to ensure the uniqueness, validity and non-tampering of the certificates, thus avoiding the single point failure of traditional CA.

C. Traceability

The user identity authentication is separated from the legality authorization. The user's real information is encrypted by the multi-signature and stored on the REC The user information needs to be approved by most REC nodes. The user information operation record is recorded on the REC. Tracking to real users is only possible when licensed by most nodes of the REC

V. SUMMARY

This system is a publishing scheme of anonymous digital certificate, which realizes the separation of user identity authentication and legitimate authorization, and has the characteristics of anonymity and conditional traceability, so as to realize the protection of user identity privacy. The system meets the requirements of certificate security and anonymity, reduces the cost of CA center construction, operation and maintenance in traditional PKI technology, and improves the efficiency of certificate application and configuration.

ACKNOWLEDGMENT

This work is supported by National Key Laboratory of Software Environment at Beihang University, National 973 Program (Grant No. 2013CB329601) and National Natural Science Foundation of China (Grant No. 61472032) , (Grant No. 61672075) and (Grant No. 61690202).

REFERENCES

[I] Adams, C., & Lloyd, S. (2003). Understanding PKI: concepts, standards, and deployment considerations. Addison-Wesley Professional.

[2] Khosrow-Pour, Mehdi, ed. Encyclopedia of e-commerce, e-government, and mobile commerce. IGI Global, 2006.

[3] Lioy, Antonio, et al. PKI past, present and future. International Journal ofinfonnation Security 5.1 (2006): 18-29.

[4] Li, Mingchu, et al. A new modified bridge certification authority PKI trust model. Pervasive Computing and Applications, 2006 1st International Symposium on. IEEE, 2006.

[5] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system.(2008).

[6] Li, Xiaoqi, et al. A survey on the security of blockchain systems.Future Generation Computer Systems (2017).

[7] Tsai, Wei-Tek, Xiaoying Bai, and Lian Yu. Design Issues in Permissioned Blockchains for Trusted Computing. Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on. IEEE, 2017.

[8] Tsai, Wei-Tek, and Lian Yu. Lessons Learned from Developing Pennissioned Blockchains. 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2018.

[9] Tsai, Wei-Tek, et al. A system view of financial blockchains. Service-Oriented System Engineering (SOSE), 2016 IEEE Symposium on. IEEE, 2016.

[10] Bellare, Mihir, and Gregory Neven. Identity-based multi-signatures from RSA. Cryptographers' Track at the RSA Conference. Springer, Berlin, Heidelberg, 2007.

[II] Tsai, Wei-Tek, et al. Blockchain systems for trade clearing. The Journal of Risk Finance just-accepted (2017): 00-00.

[12] Tsai, Wei-Tek, et 31. Intellectual-Property Blockchain-Based Protection Model for Microfilms. Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on. IEEE, 2017.