基于区块链的数字证书及电子印章系统架构

张 芬 李腾跃

摘要：通过利用区块链的不可篡改、去中心化等特性，结合CA原有的优势，提出一款基于区块链的数字证书及电子印章系统架构。架构中每一个加入链的CA都作为一个节点，可以发布、更新本CA的数字证书和电子印章，以及通过区块链验证其他CA发布的数字证书及电子印章，打破了原来PKI中心化模式下的跨CA间不能互通互验的瓶颈。

关键词：区块链；数字证书；电子印章

一、前言

PKI（Public Key Infrastructure）是一种使用公钥密码技术支持认证、加密、完整性和不可否认服务的安全基础设施[1]。PKI技术采用数字证书管理用户的公钥，通过CA认证中心对用户的身份信息进行校验，然后签发公钥，并将公钥与其实名信息进行绑定，以达到在网络中上验证用户信息的目的。

PKI–CA的工作原理是通过签发和维护数字证书来建立一套信任体系，在该信任体系中，用户可以通过签发拿到的数字证书来实现身份验证和安全处理。但是在传统的PKI技术中，CA中心是信任的源头，也就是说当信任了某个CA机构，才会信任该CA签发的数字证书，可是很难找到一个绝对安全的通信信道，所以信息有被截获和篡改的风险。另一方面，如果信任的起点受到恶意攻击被控制后，那么便会发生一系列的连锁反应，即在这种环境下的CA根证书、该根下签发的数字证书以及与证书绑定的电子印章都不再可信。现实中不乏这种事例：事件发生在2016年，StartCom作为一家CA认证服务机构，在未经客户授权的情况下，错误签发了大量SSL证书，此外，签发虚假信息证书的TurkTrustCA公司、被攻击的DigiNotarCA公司等一系列事件，均说明了CA作为信任的起点，一旦被攻破后就有发生安全事件的风险[2]。

与CA中心化概念相对的区块链，是一种可以在去中心化网络环境中，以顺序相连的方式，按照时间顺序，以链式数据结构方式组合数据区块。区块链的安全机制在于区块链是以密码学方式，确保分布式账本的不可篡改和不可伪造性。鉴于这种使用共识机制、分布式数据存储、防篡改等区块链技术，提供了以去中心化方式建立信任关系的思路与落地方案，引起了很多行业的关注。目前，基于区块链的PKI技术的代表应用，已有EMCSSL、CertCoin，实现了去中心化的认证方式。美国科技公司Pomcor同样提出了基于区块链的PKI系统，但该系统仅适用区块链存储已发布或撤销证书的散列值[3]。

鉴于以上，为了解决由于过度依赖中心化服务器而产生的安全风险，本文提出了一种基于区块链的数字证书及电子印章系统架构。电子印章作为PKI技术的重要应用，在无纸化办公领域均得到了广泛的使用，架构中利用区块链技术构建了一种PKI公钥基础设施，区块链用于存储CA操作数字证书的记录以及电子印章信息，并由CA通过共识机制进行维护，以区块链的方式进行数字证书、电子印章的发布、存储、更新、验证，PKI体系中各个节点均可对以上操作记录进行安全审计，从而实现PKI去中心化，最终有效解决CA证书分发过于中心化的问题，避免单点失败和多CA间交叉认证互信的问题，有效防御CA被恶意攻击所带来的连锁反应。

二、相关技术概述

（一）区块链技术

区块：区块是一种记录交易的数据结构。每个区块均是由区块头和区块主体组成，区块主体只负责记录前一段时间内的所有交易信息[4]，而且区块头几乎实现了区块链的大部分功能，详见下图1。

哈希值：使用SHA256加密算法计算得出的一串定长且不可逆的字符串，即将任何篇幅的字符通过SHA256加密算法运算后，都将得到一个定长为256位的Hash值（散列值）。该算法的特点一是相同的数据通过SHA256算法加密后都将会得到相同的结果；二是输入数据哪怕有一点微小变化（比如文章中某个逗号改为句号）则将

得到一个千差万别的结果值，且该结果值无法预先知道；三是无法通过加密转化后的结果逆向转发，即正向计算即由数据计算其对应的 Hash 值十分容易，但是逆向计算则极其困难，在当前科技条件下被视作不可能。

时间戳：可信时间戳服务是基于 PKI 技术，采用精确的时间源，利用签名和加密等技术保证用户电子文件的准确性、完整性、抗抵赖性。以数字签名技术为核心，提供生成、验证权威时间凭证的服务。通过签发权威的电子凭证，用于证明电子数据文件自申请可信时间戳后，数据文件内容的完整性与不可抵赖性，可广泛的应用在电子公文、电子商务、电子政务、电子交易等领域。

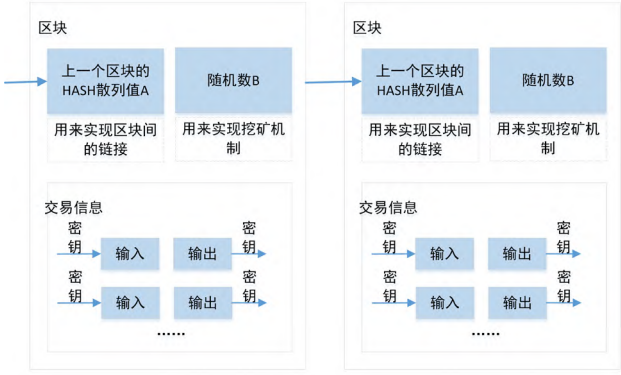

图 1 区块链区块示意图

区块链中的每个区块储存着一系列的信息，主要包含了以下内容：

（1）每个区块都有一个唯一标识，即该区块储存的哈希值；

（2）最近的加有时间戳的交易信息；

（3）以及上一个区块的哈希值。

交易系统中的所有区块依次前后相连从而形成一个链条。即使其中某一个区块被破坏，仍然可以根据它前后两个区块的交易信息，从而补全缺失的交易信息[5]。以上每个区块的交易信息包括：

（1）交易的时间戳；

（2）交易者的公钥信息；

（3）由前一交易信息和当前交易者的公钥，一起生成的哈希值；

（4）前一区块的数字签名值。

不同的交易信息之间通过如下机制来验证：一旦有新的交易信息上链时，即利用当前交易者的公钥和上一条交易信息，生成一个唯一的哈希值，首位相连作为此条交易信息的唯一标识。同时，上一条交易的所有者使用自己的私钥，需要对此条交易的哈希值进行签名，并且签名值作为标记储存在交易的区块中。

（二）电子印章技术

电子印章是将电子文件内容的数字签名通过数字水印、加密等技术，使电子文件内容和电子印章图像进行有效的绑定（如利用隐藏技术将数据隐藏在电子印章的图像中等）[6]，以使其加盖的电子文件具有与使用物理印章的纸质文件具有同等的法律效力。外观上电子印章保留与实体印章相同的视觉效果，符合用户物理印章的使用习惯及体验。通过验证数字签名的合法性来验证电子印章的真伪，当一份加盖电子印章的电子文件通过电子签名 / 验证技术验证通过后，才能证明与电子印章相关联的电子文件是真实的，即能确保该电子文件未被篡改，电子文件中的印章图像才被承认是有效的，否则电子印

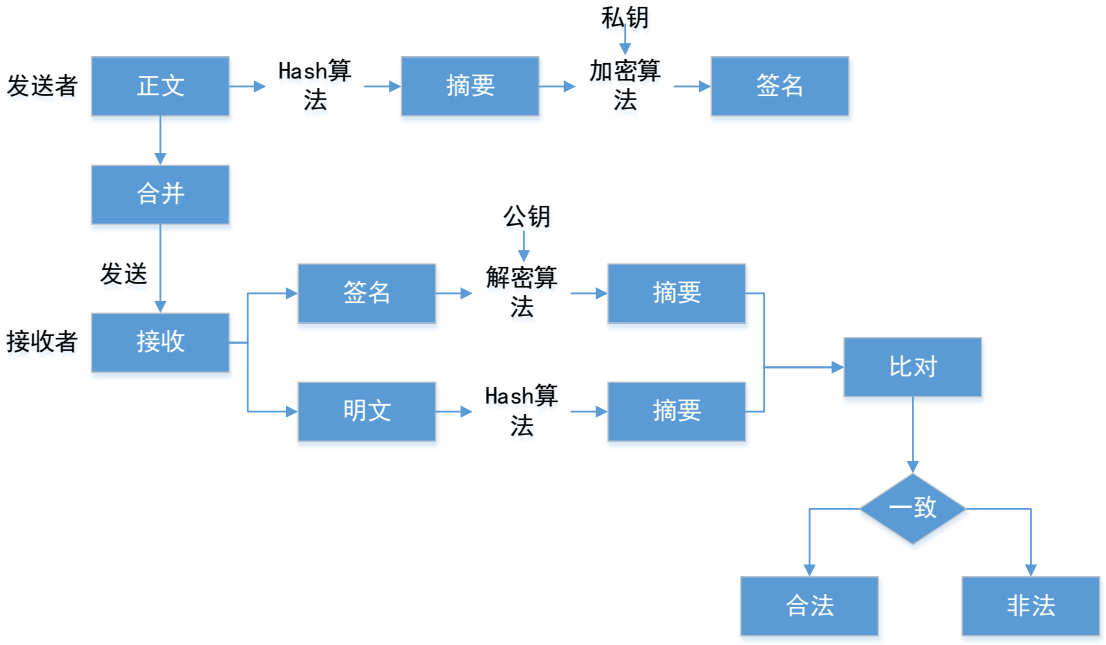

图 2 签名验证流程图

章只能是一个没有法律效力的图片而已。所以当数字证书被吊销或冻结时，那么该数字证书签发的电子印章状态应随即同步变更。

电子印章的验证包括验证数字签名的有效性和电子印章状态的有效性。

1. 数字签名有效性的验证：一是验证数字证书在有效期内；二是通过验证签名来确定信息发送方的身份信息；三是通过验证原文的哈希值来验证消息的完整性。数字签名技术是用发送者的私钥对原文的摘要信息进行加密，然后与原文一起发送给接收者。接收者用发送者的公钥对加密后的摘要进行解密，获取到明文摘要后，再用哈希算法将原文转为摘要，最后再与收到摘要明文进行比对。如果相同，则说明收到的原文是完整的，在传输过程中没有丢失或者被篡改，否则说明原文不完整或被篡改过，因此数字签名能够验证信息的完整性，验证流程图详见图 2。

2. 电子印章状态的有效性，则需要根据电子印章序列号去对应的电子印章系统进行实时查询。

三、基于区块链的数字证书及电子印章系统架构

（一）系统架构

该系统模式下，每一个加入联盟链的 CA 都作为一个节点，可以发布、更新本 CA 的数字证书和电子印章，以及通过区块链验证其他 CA 发布的数字证书及电子印章，打破了原来 PKI 中心化模式下的跨 CA 间不能互通互验的瓶颈，系统架构图详见图 3。

该系统架构充分利用了区块链的去中心化、不可篡改性等特性，将数据关键信息存储在主链上，同时控制了不同用户对电子数据的访问权限，有效解决了电子数据存储的安全问题。区块体中记录着网络中每一份数字证书和与该证书相关的操作，以及操作执行之后当前证书的状态。区块链网络去中心化的特点，使得数字证书、电子印章信息可以在每一个节点得到验证，攻击者想要篡改需要掌握全网区块链一半以上的算力才能成功。

（二）区块设计

上图中的当前区块链中的 HASH 值，是通过对上一个区块散列值 A、随机数 B、本区块的交易散列值 C 进行综合哈希计算获得。前后区块根据这个值进行首尾相连组成区块链，并且这个值对区块链的安全性起到了至关重要的作用，详见图 4。

当前时段所有交易单的 HASH 值 C 主要用于检验一笔交易是否在这个区块中存在，它是由当前区块主体中所有交易的HSAH值再前后两两哈希计算出来的一个值。

在当前区块加入区块链后，就会立即开始下一个区块的计算工作。具体包括：

（1）把在本地内存中的数字证书、电子印章操作信息记录到区块主体中。

（2）在区块主体中生成此区块中所有数字证书、电子印章操作信息的梅克尔树，且将梅克尔树值保存在区块头中。

（3）把上一个刚刚生成的区块的区块头的数据通过 SHA256 算法生成一个哈希值计入到当前区块的 HASH 值中。

（4）用时间戳对当前时间进行签名，保存在时间戳字段中。

（5）难度值不固定，该字段会根据之前一段时间区块的平均生成时间进行调整。

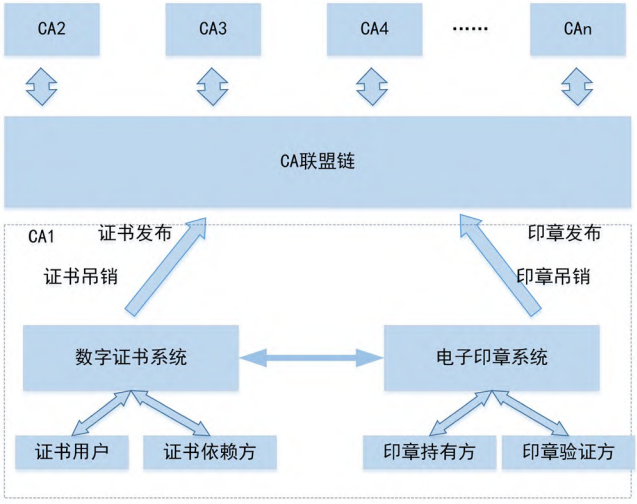

图 3 系统架构图

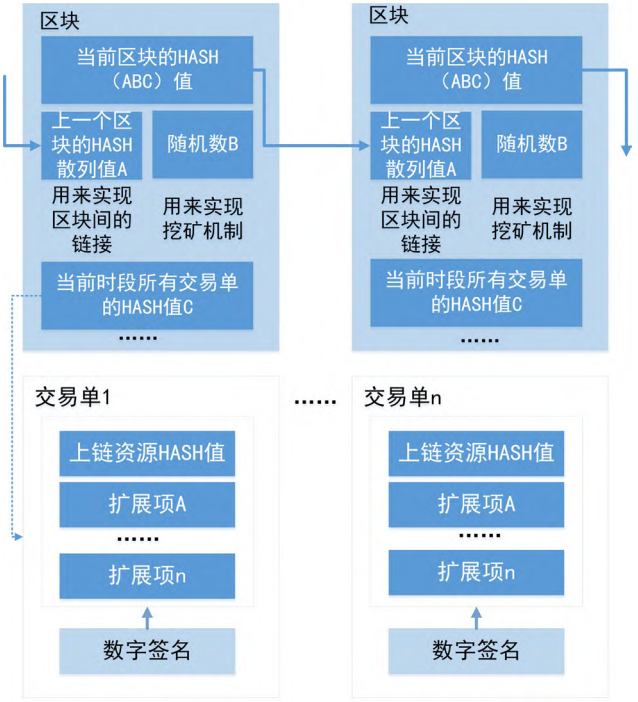

图 4 区块设计图

（三）上链流程设计

本框架中证书序列号作为上链交易的唯一标识，需要加入联盟链的 CA 间定义好证书序列号的生成规则，防止多 CA 间的证书序列号的重复。另外，增加证书主体标识、证书状态、印章序列号、印章状态这些扩展项，便于检索及查询。

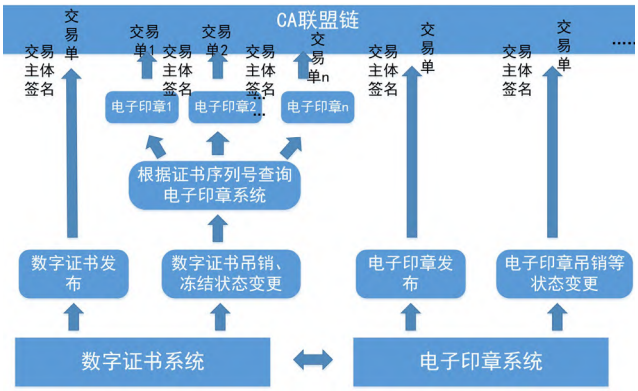

图 5 上链流程设计图

当数字证书发布时，将证书发布的操作作为一次交易信息上链，详见上图 5。具体一笔交易信息，如下表 1 数字证书发布交易表：

表 1 数字证书发布交易表

证书序列号	唯一标识	必填
证书主体标识	扩展项 A	必填
证书状态	扩展项 B	必填
企业名称	HASH 值	必填
企业统一信用代码		
其他基本信息		

当电子印章发布或电子印章状态发生变更时交易信息，见表 2 电子印章更新交易表，包括：

表 2 电子印章更新交易表

证书序列号	唯一标识	必填
证书主体标识	扩展项 A	必填
证书状态	扩展项 B	必填
印章序列号	扩展项 C	非必填
印章状态	扩展项 D	非必填
企业名称	HASH 值	必填
企业统一信用代码		
电子印章图片		
电子印章名称		
其他基本信息		

表 3 数字证书状态变更交易表

证书序列号	唯一标识	**********
证书主体标识	扩展项 A	**********
证书状态	扩展项 B	吊销
印章序列号	扩展项 C	**********
印章状态	扩展项 D	吊销
电子印章图片	HASH 值	**********
电子印章名称		
企业名称		
企业统一信用代码		
其他基本信息		

当数字证书状态发生变更时，以吊销为例，数字证书系统先根据证书序列号调用电子印章系统进行查询该数字证书签发的电子印章，然后将数字证书、电子印章等信息以一笔交易上链，此时上线信息如下表 3 数字证书状态变更交易表。

（四）实例描述

电子印章的发布：某单位向某 CA 机构申请制作一个单位电子印章，该单位实名登录该 CA 机构的电子印章系统，上传单位印章图片，电子印章系统识别该单位的 UKEY 证书或服务端数字证书，不管该数字证书是否是本 CA 机构签发，电子印章系统都可以根据证书的序列号上链查询该单位证书的状态，若证书状态是吊销状态，则系统提示停止制作电子印章；当证书状态是有效时，电子印章系统会将印章图片、数字证书按标准拼成印章结构体，且将印章序列号、印章状态作为扩展项、印章结构体信息转 HASH 值，关联证书序列号加上本 CA 机构的数字签名上链存储。

用章的业务系统在使用电子印章签章前，先根据印章序列号调用区块链系统的验证接口进行验证该电子印章的状态，电子印章状态为有效时，才继续进行后续的盖章操作。

参考文献

[1] 王勇，王佩玮，赵鹏．基于区块链的电子印章管理系统的设计 [J]. 价值工程 ,2019.

[2] 许金叶，夏凡．区块链的产生根源及其本质 [J]. 会计之友．

[3] 马昂，潘晓，吴雷，等．区块链技术基础及应用研究综述 [J]. 信息安全研究 ,2017.

[4] 林虹萍．区块链技术构筑互联网信息安全新范式 [J]. 云南警官学院学报 ,2017.

[5] 张伟，丁朝晖．基于区块链和数字签名技术的智慧电厂数据安全传输系统研究与设计 [J]. 电力信息与通信技术 ,2021.

[6] 许锋波，牛丹梅，赵治远．计算机网络安全综述 [J]. 电脑知识与技术 ,2010.

（作者单位：上海市数字证书认证中心有限公司）