文章编号：2096-1472(2020)-08-32-03
DOI:10.19644/j.cnki.issn2096-1472.2020.08.009

区块链电子认证系统的设计与实现

周 硙

(北京工业大学，北京 100022)
✉w.zhou@ieee.org

摘 要：本文提出了一种基于区块链的电子认证系统(CA/PKI)。该系统数据持久化及访问依赖于区块链的去中心化特性，相对于单点部署PKI系统具有更高的可靠性，且运维难度低于集群部署；同时系统继承了区块链不可篡改、不可伪造的特性，可以对数字证书的签发、验证、吊销关键环节实现数据存证，方便各方交换数据，并保证全程留痕。上述特性使得该系统可以便捷的实现私有部署，成本低、安全性高，在企业级应用、电子商务等领域具有潜在的应用价值。

关键词：区块链；电子认证服务；证书基础设施
中图分类号：TP311 **文献标识码**：A

Design and Implementation of Electronic Authentication System based on Blockchain

ZHOU Wei

(*Beijing University of Technology*, *Beijing* 100022, *China*)
✉w.zhou@ieee.org

Abstract: This paper proposes a digital authentication system (CA/PKI, Certificate Authority/Public Key Infrastructure) based on blockchain. The data persistence of this system depends on decentralized characteristics of blockchain. It is more reliable than single-point deployment of PKI system, and the operation and maintenance is easier than that of the cluster deployment. This system inherits the characteristics of blockchain that cannot be compromised. This solution can issue, verify, and revoke key certificates to realize data storage certificates, facilitate the exchange of data, and ensure that traces are kept throughout the process. The above features make the system easy to implement private deployment, taking into account the cost and security, and it is highly expected to be available in enterprises and e-commerce areas.

Keywords: blockchain; Certificate Authority; Public Key Infrastructure

1 引言(Introduction)

数字证书广泛的使用在金融交易、电子签名、用户鉴权等场景。即可以代替传统的用户名密码认证模式、也可以在原有系统上提供双因子认证，进一步提高系统安全性[1]。信息系统利用数字证书核实用户身份。证书包含身份信息、授权信息及第三方权威机构的数字签名。其中数字签名，由具有公信力的第三方证书颁发机构(Certificate Authority，CA)核实信息后，用密码学方法计算得到。CA同时提供了公钥基础设施(PKI)实现证书的生命周期管理。PKI需要实现证书签发、更新、作废、查询等一系列服务[2]。特定场景下有部署私有CA/PKI的需求，如企业级应用等。CA将成为整个系统安全的基石，采用中心化部署时，CA的安全将是系统安全的重中之重，需要该组织机构具有相应的技术能力、管理能力，需要有专业的团队，并投入充足的建设及后期维护费用。

区块链是一种集体维护的分布式共享加密数据库[3]，众多的项目证明它具有不可伪造、全程留痕、可以追溯的技术特性。区块链可以不依赖中心化权利机构，对现有中心部署的CA/PKI系统是一项重要的补充，能够有效降低单点风险，具有低成本、部署简单、安全性高的优势[4,5]。

2 设计概述(Design overview)

2.1 设计目标

CA系统核心功能是签发数字证书、管理数字证书。根证书、中级证书的存放及使用安全是系统安全的核心。目前主要措施有：私钥物理隔离、操作日志审计、多人共同签发、人员背景调查等。用户的证书可能会丢失或者被盗，系统需要实现证书吊销功能。该功能是PKI维护的一个在线列表，列举了所有在有效期内但是有安全风险的证书。在证书存在安全隐患时，持有人可以向PKI申请将不安全的证书加入吊销列表。其他用户可以通过在线查询协议，查询证书吊销列表，从而判断一个证书是否有效。本文用区块链技术代替部分CA/PKI流程，设计了可低成本私有化部署的方案。该方案利用多私钥共同签名颁发证书，代替传统的多人共同操作的

签发环节，通过公共账本代替传统日志系统及证书在线查询协议，通过智能合约和区块链共识协议响应重大安全事件。

2.2 系统角色

CA的根证书是一切信任的基础，仅用于生成中级证书，不用于普通证书的签发。用户证书的签发流程是首先由用户提交CSR，操作员在管理人员及审计人员见证下，用中级证书签发用户的数字证书。本文所述方案沿袭了CA的基本流程，设计了普通用户、见证人、矿工、访客四种用户角色，见图1。

普通用户对应传统CA/PKI框架下的证书持有人。在区块链系统中，普通用户自行生成私钥及公钥。公钥附加身份信息打包成证书请求文件(CSR)。CSR经私钥数字签名后发送给见证人。经过多名见证人核实信息并签发后，即得到数字证书(CRT)。

见证人是签发的负责人，具有提案权及投票权。见证人在接收到普通用户的CSR后，如果确认了用户信息正确，可以将相关信息广播给矿工，发一起个证书签发提案，即提案权。见证人同时需要监听链上数据，如果发现新的CSR上链，需要对其进行投票，即投票权。投票通过的CSR将由智能合约自动生成CRT，实现证书签发。

矿工负责区块生成及公共账本维护。矿工是唯一接触区块链的角色，矿工之间通过底层的区块链技术，如Fabric/Ethereum框架，实现区块链基本功能。每个矿工均持有一份公共账本，账本记录了证书的提案、投票、吊销的状态。矿工对其他角色暴露服务接口，负责①接收见证人的提案；②运行智能合约，处理投票，并根据结果更新公共账本的数据；③处理证书吊销请求；④响应访客的查询请求。

访客可以访问区块链数据，验证一个证书的签名是否合法，也可以在线获取证书的状态，确认证书是否被吊销。

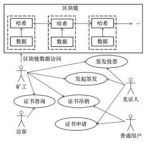

图1 系统角色及用例

Fig.1 System roles and use case

2.3 客户端

区块链不需要中心服务器，系统由若干独立客户端构成的对等网络运行。客户端可以同时具有上述四种角色中的一种或多种。客户端以Master/Slave模式工作，Master实例负责监控其他Slave，必要时对故障实例重启。矿工以网络及磁盘IO操作为主，事件驱动的单线程模式完全可以充分利用典型的硬件资源；见证人需要响应CSR操作，适当增加见证人可以谈提高系统吞吐量。因此典型情况，客户端可以包含一个矿工及多个见证人。

3 证书管理(Certificate management)

3.1 证书签发请求

普通用户需在区块链上具有合法身份，该身份是一个区块链地址及控制该地址的私钥。用户需要自行使用区块链的密钥算法，生成一对密钥。并由公钥通过哈希算法生成区块链地址。

在拥有区块链身份后，可以创建CSR文件。首先为CSR文件创建一对密钥，私钥有用户自行保管，不能公开。将证书授权的域名、主体名称、国家地区、密钥算法及其他附加信息序列化成属性集。CSR文件是比较成熟的格式，OpenSSL等工具可以非常便捷完成上述工作，但是此类工具缺少对自定义字段的处理能力，考虑到Postal Address字段通常闲置，因此用该字段存储用户区块链地址，实现CSR与用户身份在区块链的上关联。最后公钥、证书内容及数字签名重新打包生成CSR文件。

3.2 预见证过程

普通用户将CSR发送给各见证人，各见证人首先对CSR文件进行预见证。见证人之间通过Paxos/Raft等一致性算法[6]，对验证结果进行协商。如果见证人发现证书信息有错误，如身份或域名信息不符，可以直接否决该CSR。如果见证人均同意了该证书，则需要选举一位见证人负责发起CSR上链请求。由该负责人将CSR广播给各矿工，矿工通过区块链共识协议，实现CSR数据上链。

预见证阶段是必要的。见证人在预见证阶段已完成了CSR的信息核验，并在上链之前已在大多数见证人间达成一致，CSR上链后，见证人只需要对文件内容进行复核，不需要对CSR内容进行实质性核验，因此加快了区块链上的多签名程序。预见证算法效率高于区块链共识协议，预先在见证人间取得一致，避免了CSR上链后在最终签署阶段产生分歧的可能性，节约了处置分歧的区块链资源。见证人的选举程序可以避免同一CSR，被不同见证人重复提交。最后预见证过程可以避免无效CSR直接上链，在上链前就否决掉无效的CSR，减少链上空间的浪费。图2给出了预见证过程的时序图。

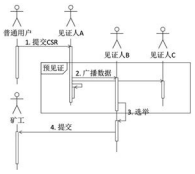

图2 预见证过程的时序图

Fig.2 The sequence diagram of the witness process

3.3 证书签发

各见证人需要监听区块数据更新。发现新的CSR上链后，独立核实CSR请求信息，并独立决定同意或否决该CSR。同意或者否决意见均需要提交到区块链上。见证人把自己的决定和签名结果发布给矿工。矿工负责验证CSR文件自身的合法性及各见证人的投票意见，当投票数满足既定规则时，将会自动触发CSR对应的签发或否决逻辑。该逻辑在区块链上表现为多签名智能合约[5]，以下代码展示了其核心逻辑，当同意的见证人数量超过常量MIN_SIGNATURES时，该合约发布一个CRT事件，代表签发一个数字证书：

```
function sign(uint csrId) public isWitness {
CSR storage csr = csrs[csrId];
...
csr.count++;
if( csr.count >= MIN_SIGNATURES ) {
...
emit CRT(csrId);
deleteCsrs(csrId);
}
}
```

因为矿工负责提供证书查询服务，为了提高查询性能，需要采用Redis等KeyValue数据库，加速查询的效率[7]。当矿

工发现证书更新时，需要及时更新缓存，保证数据一致性。图3下图给出了证书签发的时序图。

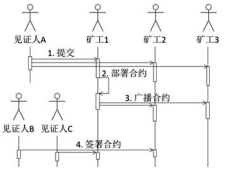

图3 证书签发的时序图

Fig.3 The sequence diagram of the certificate issuance

3.4 证书吊销

证书吊销，由证书私钥持有人向矿工节点发起吊销申请。用证书私钥及用户私钥分别对吊销申请签名，最后将吊销申请及签名发给矿工，矿工验证后将申请发布于区块链上，实现证书吊销。该吊销方法适用于普通用户的证书，也适用于见证人的中级证书吊销。矿工需提供相应的数据访问API供访客查询。吊销申请一经确认，不可撤销。

4 实现(Implementation)

4.1 账本

区块链数据主要有UTXO和账户两种模式。CA/PKI系统需要存储CSR、CRT及签名历史，UTXO无法满足要求，因此本系统考虑账户模式。为了完成证书的生命周期管理，需要存储证书管理规则和状态信息。证书的管理规则以智能合约的形式存储于区块链中，一个CSR对应一个智能合约的实例。实例的状态描述了证书的签署状态以和吊销状态。证书的管理规则对应了区块链智能合约的事件处理；证书的状态对应了区块链智能合约的状态机。

4.2 节点与角色

区块链系统通常是若干个节点构成的分布式系统。一个节点可以具有一种角色，也可以同时具有多种角色。区块链技术诞生的初期，网络各个节点是完全对等的，一个节点要与其他所有节点具有相同的功能，持有所有历史区块的数据。该数据模型对于矿工的任务是必要的，但是不利于其他角色使用区块链功能。后续发展出了多种节点类型，大体分成全节点和轻节点两类。全节点具有完整的数据，有能力对所有业务进行验证，可以执行智能合约；轻节点只保存了有限数据，仅可以验证事件是否发生。在本系统中，少部分矿工节点负责维持整个区块链的运行，需要以全节点方式工作。见证人可以通过矿工获取区块链数据，投票过程是构造投票请求附加数字签名，由矿工节点完成后续操作，见证人不需要完整的区块数据，可以采用轻节点方式运行。

4.3 区块链浏览代理

相对于全节点，轻节点只需保留有限的数据，以便查询证书的状态，典型情况下轻节点数据量约为全节点的10%到25%。但是对于用户而言依然需要保存相当的数据。传统的Web系统中，浏览器只需要信任少数CA的根证书。以对根证书的信任为基础，通过证书链，将信任延伸到SSL服务器，浏览器只需要几百KB的存储即可以完成证书链校验。本文方案沿用证书链传递信任的设计，以减轻终端用户的成本。访客可以信任一部分见证人，根据证书链追溯计算一个证书是否由可信的见证人签发。其次可以在线请求证书状态。矿工提供区块链数据的代理访问服务。普通用户和访客可以不运行客户端实例，不需要直接读取、校验区块链数据，只需要通过矿工代理数据请求，询问一个证书是否被签发、证书过期时间以及是否被吊销。该代理服务称为区块链浏览代理，对内负责与各个矿工沟通，及时更新数据，更新缓存；对外提供Rest接口方便用户查询数据。该服务有可能成为系统瓶颈，需要合理设计缓存系统。

5 讨论(Discussion)

5.1 共识协议的选择

共识协议是区块链节点实现数据一致的算法。常见的共识协议为PoW、DPoS及PBFT。DPoS及PBFT均适合本系统方案[8]。DPoS优势在于对投票权的精细控制，不同节点可以拥有不同权重的投票权，安全性较好的节点可以分配较高的投票权。因为投票权可以与身份无关，所以DPoS不要求所有节点实名，只需要持有投票权超过一定比例的节点实名。投票权的分配是公开的，因此伪造身份的虚假节点很难获得足够的投票权，即无法威胁到系统安全。PBFT不需要管理投票权，在实现方面成本相对较低。PBFT可以容忍不超过1/3的节点恶意篡改数据。为了控制该风险，通常需要对矿工节点实名管理，并及时将恶意节点除名。

5.2 安全性

系统安全性取决于区块链安全、见证人根证书及中级证书的安全。区块链系统对数据安全有天然优势，如果想篡改数据，DPoS协议要求具有50%以上的投票权，PBFT协议要求1/3以上的节点合谋[9]，以上两点均很难实现。见证人的根证书中级证书的私钥如果泄露或者被不当使用，可能会签发出假证书。相对于传统CA，区块链系统可以通过多签名智能合约，强制要求多名见证人共同签名才能签发证书，因此个别见证人的安全事件不影响系统的安全性。同时矿工可以通过投票的方式，决定吊销见证人的见证资格，保证系统的安全性。

5.3 成本优势

私有部署CA/PKI系统，主要成本用于维护系统安全。基于区块链的系统，可以有效减少系统在安全方面的成本支出。区块链通过多个独立节点的一致决议，代替了单点系统签发证书的程序，系统不受个别节点的影响。可以节约部署单独的高防服务器及保管私钥的专用物理空间的相关成本。系统核心业务逻辑以区块链智能合约为基础，由多个矿工共同执行，可以有效避免人为错误及人员舞弊，有效降低管理成本。

6 结论(Conclusion)

本文提出了一种基于区块链的电子认证系统改进方案。该系统具有见证人、普通用户、访客、矿工四种角色。矿工角色负责区块链数据的访问，实现了数据的持久化；见证人系统利用多签名智能合约实现数字证书的签发、查询、吊销关键流程，其中签发过程通过预见证及链上签署两步完成，可以提高签发效率，降低区块链数据存储压力。本文所述方案中数据持久化依赖于区块链的中心化特性，具有天然的高可靠性；证书签发流程依赖于智能合约，避免了人为因素；数字签名需要有多位见证人联署，增加了系统安全性。上述安全特性使得该系统可以减少在硬件、场地方面的成本投入。相对于CA/PKI系统具有明显的成本优势，广泛适用于CA/PKI私有部署需求。

参考文献(References)

[1] Brecht B, Therriault D, Andr é Weimerskirch, et al. A Security Credential Management System for V2X Communications[J].

(下转第19页)

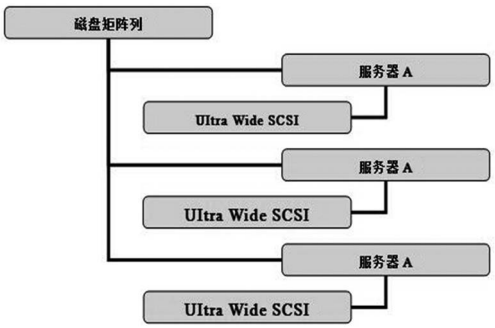

图1 网络系统集群管理结构

Fig.1 Cluster management structure of the network system

7 结论(Conclusion)

网络系统可靠性测试需要在整网虚拟环境下测试运行，网络系统可靠性测试通常情况下采用黑盒测试，不仅需进行端到端的测试，同步监测各个关键模块的实际运行情况，流量和协议控制层面的运行状态，做好各类异常情况以及故障分类分析报告，总结解决问题的方式、方法，全面分析网路系统实际运行环境的行业性、特殊性、复杂性，对网络系统的相关特性进行深入分析，在模拟测试网络系统运行环境中不断优化配置各类参数，得到最优最可靠的网络系统，提升计算机网络系统运行的可靠性。

参考文献(References)

[1] 詹亚平.计算机通信及网络远程控制技术的应用与可靠性提升[J].科技创新与应用,2020(08):174-175.

[2] 廖骏杰.计算机通信网络可靠性设计技术[J].电子技术与软件工程,2019(6):6-7.

[3] 徐蕾.计算机网络可靠性优化设计分析[J].信息与电脑(理论版),2018(04):136-137;142.

[4] 王喜来.计算机网络可靠性优化设计[J].计算机与网络,2020(04):44-45.

[5] 刘文辉,曾斌.基于计算机网络信息和网络安全及其防护策略研究[J].电子元器件与信息技术,2018(04):9-11.

[6] 刘振亮,马小琴.计算机网络可靠性优化设计问题研究[J].信息通信,2015(04):99-105.

[7] 陈刚,李璐,陈泽.计算机网络可靠性优化设计问题的研究[J].计算机产品与流通,2019(09):148-149;171.

[8] 赵鹤群.计算机网络可靠性提升要点分析[J].科技传播,2018(1):117-118.

[9] 鲁梁梁,周小健.计算机网络安全的可靠性及优化设计问题的探讨解析[J].网络安全技术与应用,2017(4):40;46.

作者简介：

黄小兰(1977-)，女，硕士，讲师.研究领域：信息系统，计算机应用技术.

(上接第34页)

Intelligent Transportation Systems, IEEE Transactions on, 2018, 19(12):3850-3871.

[2] Patsonakis C, Samari K, Kiayias A, et al. Implementing a Smart Contract PKI[J]. IEEE Transactions on Engineering Management, 2020(99):1-19.

[3] Ahmed M, Pathan A S K. Blockchain: Can It Be Trusted?[J]. Computer, 2020, 53(4): 31-35.

[4] Yeh K H, Su C, Deng R H, et al. Special issue on security and privacy of blockchain technologies[J]. International Journal of Information Security, 2020, 19(3): 243-244.

[5] 邵奇峰,金澈清,张召,等.区块链技术:架构及进展[J].计算机学报,2018,041(005):969-988.

[6] 李东辉,吴小志,朱广新,等.分布式数据库协调技术-Zookeeper[J].科技展望,2016,026(001):7-8;10.

[7] 曾超宇,李金香.Redis在高速缓存系统中的应用[J].微型机与应用,2013, 032(012):11-13.

[8] 王晓光.区块链技术共识算法综述[J].信息与电脑(理论版),2017,379(09):78-80.

[9] 黄秋波,安庆文,苏厚勤.一种改进PBFT算法作为以太坊共识机制的研究与实现[J].计算机应用与软件,2017(10):294-299;303.

作者简介：

周 硙(1983-)，男，博士，博士后.研究领域：大数据及区块链.

(上接第37页)

问题。

参考文献(References)

[1] Tasseron G, Martens K. Urban parking space reservation through bottom-up information provision: An agent-based analysis[J]. Computers, Environment and Urban Systems, 2017 (64): 30-41.

[2] Cui Q, Ning J, Yin X. Design and Implementation of a new type of Intelligent Automatic Parking Lock[C]. 2018 Chinese Automation Congress (CAC). IEEE, 2018: 1466-1470.

[3] Huang K Y, Chang S B, Tsai P R. The advantage of the arduino sensing system on parking guidance information systems[C]. 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE, 2017: 2078-2082.

[4] 陈宝远,褚庆文,孙忠祥,等.一种基于OneNet设备云的智能硬件组网方法[J].哈尔滨理工大学学报,2017,22(05):76-80.

[5] 陈姝瑾.基于微信小程序的智能停车场管理系统的研究与设计[J].信息系统工程,2019(03):67-68.

[6] 张瑞增.基于智能车位锁的共享停车位管理系统研究与设计[D].山东大学,2017.

作者简介：

赵世民(1999-)，男，本科生.研究领域：数字水印.
刘奇锋(1998-)，男，本科生.研究领域：数字水印.
李淑芝(1964-)，女，硕士，教授.研究领域：数字水印.