计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(11):161−167 [doi: 10.15888/j.cnki.csa.007138]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链和 DNSSEC 的身份认证模型①

左　鹏[1], 孙云刚[1], 袁　梦[1], 张海阔[1], 杨卫平[1], 陈连栋[2], 王　珏[3]

[1](中国互联网络信息中心, 北京 100190)
[2](国家电网河北省电力公司, 石家庄 050022)
[3](中国科学院 计算机网络信息中心, 北京 100190)
通讯作者: 陈连栋, E-mail: chenliandong1@126.com

摘　要: 身份认证是网络安全的重要组成部分, 当前身份认证技术通过 PKI 体系为服务端颁发证书实现, 应用广泛, 但存在对 CA 依赖较强、存在密钥泄露和单点失败等风险. 本文基于区块链和 DNSSEC 技术, 提出了一种新的身份认证模型, 支持不依赖 CA 的服务端和用户端的双向身份认证, 同时改进了用户证书, 实现了对用户设备的授权管理, 在安全性和灵活性方面具有一定优势. 本文首先简要介绍了身份认证技术研究现状, 随后详细描述了身份认证模型整体架构、工作流程和主要功能, 最后对该模型进行了分析并提出了应用实例.

关键词: 区块链; DNS 安全扩展; 身份认证

引用格式: 左鹏,孙云刚,袁梦,张海阔,杨卫平,陈连栋,王珏.基于区块链和 DNSSEC 的身份认证模型.计算机系统应用,2019,28(11):161–167. http://www.c-s-a.org.cn/1003-3254/7138.html

Identity Authentication Model Based on Blockchain and DNSSEC

ZUO Peng[1], SUN Yun-Gang[1], YUAN Meng[1], ZHANG Hai-Kuo[1], YANG Wei-Ping[1], CHEN Lian-Dong[2], WANG Jue[3]

[1](China Internet Network Information Center, Beijing 100190, China)
[2](State Grid Hebei Electric Power Company, Shijiazhuang 050022, China)
[3](Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Identity authentication is crucial for internet security, the widely adopted authentication technology relies on PKI system to issue certificates for servers, thus strongly depend on CA, which may face problems including key leakage and single point failure. Based on Blockchain and DNSSEC technology, this study puts forward a new model for identity authentication which can perform two-way authentication between server and client. In the mean time, improvements are made to user certificate for the management of trustable device of users thus enhance security and flexibility. This paper briefly summaries recent research in identity authentication technology at the beginning. Then it provides a thoroughly description of the new model, including the structure, work flow, and main functionality. At last, the paper analyzes the model and provides an example case.

Key words: blockchain; DNSSEC; identity authentication

随着互联网快速发展, 越来越多的网络应用需要在客户端和服务端之间建立安全、可信的传输通道, 保护敏感的个人信息不被泄露、个人资产不受损失. 在客户端和服务端进行安全有效的身份认证是确保信道安全、保密的重要手段. 当前广泛使用公钥基础设施 (Public Key Infrastructure, PKI)[1]技术在一定程度上解决了身份认证的问题, 但该技术对证书认证中心 (Certificate of Authority, CA) 可靠性依赖较大. 一方面,

① 收稿时间: 2019-04-03; 修改时间: 2019-05-08; 采用时间: 2019-05-13; csa 在线出版时间: 2019-11-06

在 PKI/CA 体系中, CA 必须确保自身私钥不被泄露. 私钥一旦泄露, 那么用此私钥签发的证书和该 CA 的下级 CA 签发的证书都将是不可信任的[2]. 另一方面, CA 必须对颁发的证书进行严格的审核. 在 PKI/CA 体系中, 任何 CA 可以为任何域名签发证书, 任何一个 CA 签发审核不严格的证书, 都会对整个 PKI/CA 系统安全性造成潜在的威胁. 此外, 中心化的 CA 在面对强大的 DDoS 攻击时, 可能出现系统瘫痪的情况[3], 存在单点失败的风险. 在实际应用中, PKI/CA 技术主要用于对服务端的身份认证. 虽然技术上可支持对客户端的认证, 但由于客户端私钥和证书的个体差异, 对于批量操作的场景, 服务端需要配置为每个个体签发证书的 CA 证书, 管理复杂、效率较低, 并且对个人用户成本较高, 因此在实际中应用较少, 难以满足对安全性要求高、需要双向身份认证的应用需求.

为解决上述问题, 本文通过充分调研国内外研究现状, 设计提出了一种新的身份认证模型, 支持不依赖 CA、安全可靠的双向身份验证. 本文同时改进了用户证书格式, 实现了对接入设备的可信认证, 进一步提高了模型的安全性. 本文的组织结构如下: 第 1 节介绍国内外研究现状, 第 2 节详细介绍基于区块链和 DNSSEC 技术的身份认证模型设计和功能, 第 3 节分析了模型优势和具体应用实例, 第 4 节总结和展望.

1 国内外研究现状

身份认证的核心问题是建立信任关系, 传统 PKI 技术中, CA 中心是信任的起点, 由于全球 CA 众多且资质不齐, 引起的证书滥发等问题日趋严重. 基于去中心化和共识机制的区块链技术以及为全球互联网提供基础服务的分布式 DNS 系统为建立信任关系提供了新的思路和方案.

1.1 区块链技术在身份认证中的应用

2008 年, 中本聪在论文《Bitcoin: A peer-to-peer electronic cash system》中, 对区块链技术进行了初步的描述. 区块链技术是对 P2P 网络技术、非对称加密技术、共识机制、链上脚本等技术的深度融合[4,5]. 区块链将所有被确认和验证的交易按照时间顺序以数据区块链条的形式记录下来, 其中的区块由区块头和区块体组成. 区块头中主要存放保障区块链正常运行的数据, 主要包括版本号、时间戳、前一区块的哈希值和当前所有交易 Merkle 树根值等. 区块结构如图 1 所示.

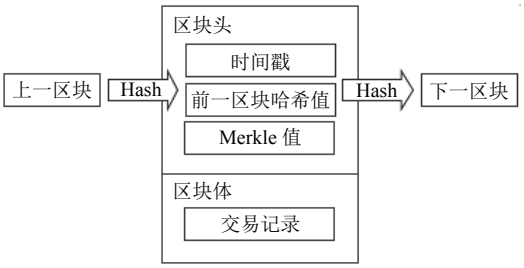

图 1 区块结构示意图

区块链系统基于 P2P 网络实现节点间的通信和协作. P2P 网络中的每个节点地位对等且以扁平式拓扑结构相互连通和交互, 不存在任何中心化的特殊节点和层级结构, 每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点等功能[6]. 共识机制[7]是区块链确定记账权归属的规则. 基于事先协商好的共识机制, 各节点可以独立自主地完成数据验证, 实现了区块链技术去中心化, 同时也确保了区块链中数据的一致性和真实性.

当前区块链主要分为 3 类: 公有链、联盟链和私有链, 三者的主要差异在于共识算法和应用场景. 公有链是面向大众的区块链, 是三者当中最为开放的, 任何人都可以自由地创建节点加入公有链, 因此去中心化的程度也最高. 联盟链一般由多个机构共同创建和维护, 会对新加入的节点进行审核和验证, 开放程度不如公有链, 属于多中心化的区块链. 由于联盟链通常被大型机构采用, 对数据的安全性和一致性要求较高, 在保证最终一致性的基础上还要保证强一致性. 私有链通常由单一个体创建和维护, 属于封闭的分布式系统.

根据区块链去中心化、去信任化、可追溯、不可篡改等技术特点, 国内外已展开相关研究, 并部分应用于实现互联网应用中的身份认证. 文献[8]提出了一种基于区块链技术构建 PKI 数字证书系统的方法, 该系统作为安全基础设施可以应用于多个领域, 如 4G 小基站设备认证、网络切片认证、多 CA 互信等. 文献[9]设计了开放式数据索引命名结构, 基于 ODIN (OPEN DATA index naming, 开放数据索引命名) 技术, 设计了基于 ODIN 的去中心化 DNS 域名协议模块, 为实现企业内部及企业间的数据安全共享构建了一种可信网络环境. 文献[10]提出基于区块链的高效跨域认证方案并设计了区块链证书授权中心的信任模型和系统架构, 利用区块链去中心化、不可篡改等特性, 解决现有 PKI 跨域认证方案的效率问题.

1.2 基于 DNS 的证书保护机制

域名系统 (Domain Name System, 简称 DNS) 作为重要的互联网基础设施, 本质上是一个全球部署的分布式数据库. 自 DNSSEC (DNS Security Extension, 即 DNS 安全扩展) 协议引入之后, DNS 数据的安全性和可靠性得到了显著提高. DNSSEC 的核心思想是通过公共密钥加密技术使区管理员对其区数据进行数字签名并由域名递归服务器验证 DNS 数据的正确性和完整性[11−13]. DNSSEC 协议引入了四种新的资源记录: RRSIG、DNSKEY、DS 和 NSEC. 其中, RRSIG 是对资源记录集合 (RRSets)[14]的数字签名, DNSKEY 用于存储 DNS 区的公钥, DS 用于建立 DNSSEC 信任链 (chain of trust)[15], NSEC 用于验证否定应答的真实性. 图 2 是 DNS 递归服务器对一条 RRset 的验证过程.

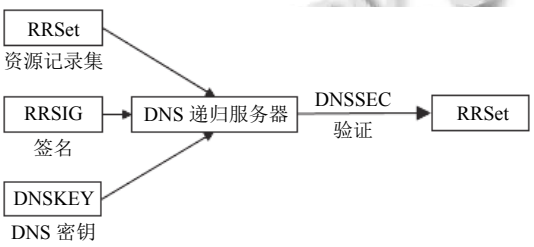

图 2 DNSSEC 验证流程图

当前基于 DNS 的证书保护机制主要有两种: 基于 DNS 的域名实体认证协议 (the DNS-based Authentication of Named Entities, DANE)[16]和基于 DNS 的 CA 授权记录协议 (DNS Certification Authority Authorization resource record, CAA)[17].

DANE 提供了一种利用 DNSSEC 基础设施对密钥和证书进行存储和发布的方法. 证书通过 TLSA 资源记录发布到 DNS 系统, 并由 DNSSEC 实现来源验证和完整性保护. 基于 DANE 的证书发布, 可解决传统 PKI/CA 体系的诸多问题: 如 PKI 技术复杂、系统维护和建设费用高昂、身份确认周期长、互操作问题突出、各地区和国家对 PKI 技术和法律问题缺乏策略和指导等[18], 其在实际场景中的应用逐渐得到关注. 文献[19]提出了一种基于 DNSSEC 的公钥分发方法, 利用 DNSSEC 为用户提供可信的公钥管理服务器定位服务, 并结合方便快捷的身份认证方法, 应用在中国科学院文档库应用中. 文献[20]针对近年来 CA 机构有意无意的证书误签发、邮件中间人降级攻击等问题, 提出了基于 DANE 的安全邮件系统架构, 改进了当前邮件协议安全方面的不足.

IETF 于 2013 年 1 月发布 RFC6844, 提出了一种 DANE 协议的替代方案, 即基于 DNS 的 CA 授权记录. 该记录可以指定一个或多个授权的 CA 为指定的域名生成证书, 从而解决 CA 滥发证书的问题. 根据 Farsight 公司的 DNSDB 数据统计[21], 截至 2017 年 6 月, 超过 400 个域名配置了一个或多个 CAA 记录. 可以看出, 目前该协议的应用仍不普及.

2 基于区块链和 DNSSEC 的身份认证模型

本文结合基于区块链的用户证书管理系统和基于 DNSSEC 的证书发布技术, 提出了一种新的双向身份认证模型. 一方面, 通过建立区块链用户证书管理子系统, 服务端实现对用户证书的签发、更新和认证. 同时创新性地在用户证书中引入了设备授权序列号, 实现了用户密钥和用户设备的双重认证, 进一步提高了安全性, 并通过区块链证书管理系统, 统一了用户证书类型, 降低服务端的管理复杂度. 另一方面, 考虑到服务端通常通过域名发布服务地址的特性, 复用 DANE 技术, 将其证书通过 TLSA 记录关联, 发布在 DNS 系统上, 客户端利用 DNSSEC 机制实现对服务端身份的验证, 降低了服务器证书签发成本, 并简化了客户端验证流程, 从而实现不依赖 CA、安全可靠的双向身份认证.

2.1 模型总体架构

本文所设计的身份认证模型总体架构如图 3 所示.

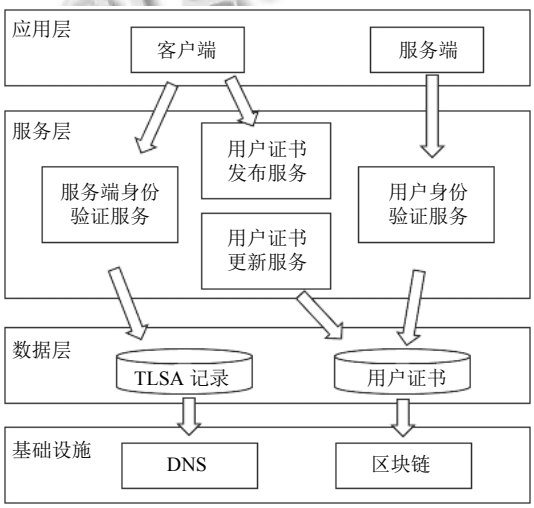

图 3 模型总体架构

图中 DNS 和区块链作为基础设施, 用于存储 TLSA 记录和用户证书等进行身份认证必须的数据. 数

据层中的 TLSA 记录用于对服务端身份的验证, 用户证书用于对用户身份的验证. 服务层基于数据层和基础设施, 可以供服务端身份验证服务、用户证书发布服务、用户证书更新服务和用户验证等服务. 通过将基于区块链的用户证书系统和基于 DNSSEC 的证书发布技术相结合, 应用层可以实现客户端和服务端的双向验证.

2.2 基于区块链的用户证书管理

2.2.1 区块链证书子系统架构

基于区块链的用户证书子系统负责对用户证书进行认证和管理. 区块链中的节点由服务端所属机构提供, 共识机制采用私有链和联盟链常用的 PBFT 机制. PBFT 机制可以保证强一致性且效率较高, 可以较好地满足本文所述模型的需求. 该子系统实现的主要功能包括用户证书的发布、存储、更新和注销以及对用户身份的验证. 用户证书子系统与客户端和服务端的交互方式如图 4 所示.

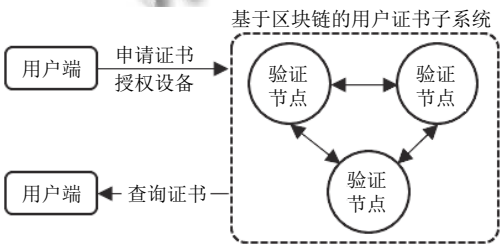

图 4 基于区块链的用户证书子系统

2.2.2 区块链用户证书

为进一步提高认证模型的安全性和易用性, 设计了改进的区块链用户证书, 如图 5 所示.

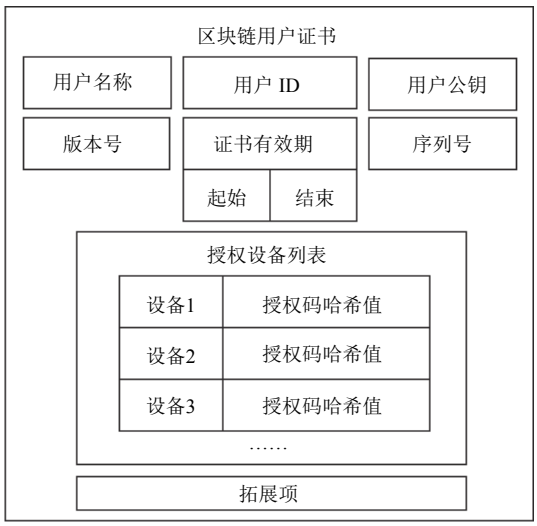

图 5 区块链用户证书

与传统的 X.509 证书相比, 主要有以下不同: 首先, 本文在证书中加入了授权设备列表部分, 用于记录和验证被授权登录的设备, 实现了对同一用户的不同设备进行授权管理. 传统 PKI 体系下, 攻击者一旦获取了用户证书对应的私钥, 即可在任何设备上冒充用户进行身份验证. 本模型在用户证书中加入了设备授权列表, 攻击者必须同时获取到用户私钥和已授权的设备才可冒充用户身份, 进一步提高了模型的安全性, 2.2.3 节将对设备授权的流程进行详细的描述. 其次, 本模型中用户证书的真实性由区块链保证, 略去了传统证书中签名算法和签名相关数据, 一方面显著降低了证书大小, 提高了证书的易用性, 另一方面服务端不需要通过证书中的签名数据进行验证, 降低了服务端的处理压力.

2.2.3 区块链证书子系统功能

基于区块链的用户证书子系统的主要功能包括证书申请、设备授权和登录验证. 与传统 PKI 技术不同, 上述功能均由区块链中的验证节点通过共识机制实现, 免去了对 CA 中心的依赖.

新用户注册时需要申请新的用户证书, 具体流程为: 用户首先申请生成一份数字证书, 与证书相对应的私钥存储于用户侧. 随后用户将证书内容和相关身份信息作为请求内容发送给验证节点, 等待证书签发. 验证节点收到用户请求后通过用户提供的信息判断是否保存用户的证书, 随后, 通过验证的证书通过共识机制被保存到区块链中.

用户申请证书时使用的设备可以对其他设备进行授权. 授权时, 初始设备向区块链发送授权请求, 区块链系统将一个随机生成的序列号和请求发出的时间拼接成字符串, 随后将字符串原文发送回初始设备, 并将字符串的哈希值存入区块链证书中的授权设备列表中. 最后, 用户将得到的字符串输入到待授权的设备中, 完成设备授权过程.

图 6 是用户端登录和验证流程. 登录请求由客户端发起, 服务端收到用户的证书后, 向区块链用户证书管理系统发起验证请求, 区块链证书系统根据用户提交的证书信息和设备授权状况, 对登录的合法性进行验证.

2.3 基于 DNSSEC 的证书发布

2.2.1 TLSA 记录

TLSA 资源记录用于关联域名和 TLS 证书或其公

钥部分. 考虑到服务端通常通过域名发布服务地址, 复用 DNS 系统, 通过 TLSA 记录发布证书可进一步提高易用性和实施成本. 客户端通过 DNS 查询获取服务端域名的 TLSA 记录并对该记录实施 DNSSEC 验证, 实现服务端的身份验证.

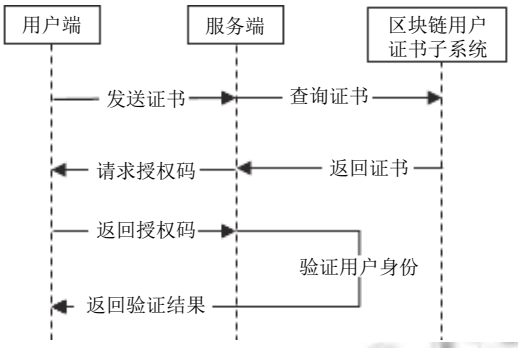

图 6 登录验证流程

如图 7 所示, 在 TLSA 记录中, Certificate Usage 字段、Selector 字段和 Matching Type 字段用于指定证书的属性, Certificate Association Data 字段用于存储记录的具体内容. Certificate Usage 字段用于指定 TLSA 记录中的证书的类型和使用方式. 当该字段值为 0 时, 记录用于指定域名信任的 CA. 值为 1 时, 记录限制主机上的服务可以使用的终端证书. 值为 2 时, 记录可用于指定域名的信任锚点. 值为 3 时, 记录中与域名绑定的证书或公钥是由域名自行签发. Selector 字段用于指定 TLSA 记录中的证书与服务端提供的证书进行比较的部分, 值为 0 时对证书全文进行比较, 值为 1 时仅对公钥部分进行比较. Matching Type 用于指定 TLSA 记录中证书的加密类型, 值为 0 时不使用加密算法, 值为 1 时使用 SHA-256 算法, 值为 2 时使用 SHA-512 算法.

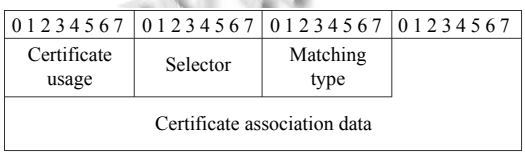

图 7 TLSA 记录格式

2.3.2 证书验证流程

客户端对服务端的身份认证基于 DNSSEC 实现, 如图 8 所示. 服务端向 DNS 服务器中添加自己的 TLSA 记录, 记录内容为服务端自行签发的证书. 客户端通过 DNS 查询的方式获取服务端的 TLSA 记录, 首先通过 DNSSEC 验证确认该 TLSA 记录的真实性, 然后, 将该 TLSA 记录与从服务端直接获取的证书进行比对, 进而验证服务端的身份.

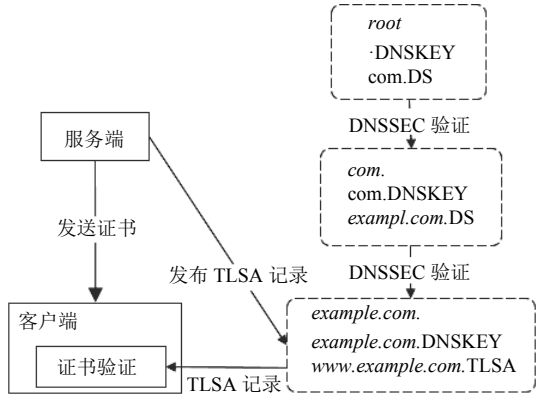

图 8 基于 DNSSEC 的证书验证流程

3 特点与应用

3.1 系统优势

本文基于区块链系统去中心化、不可篡改的特性和通过 TLSA 记录发布服务端证书并通过 DNSSEC 验证的方法, 实现了客户端和服务端双向身份认证. 相对于传统的 PKI/CA 模型, 具有以下优势:

(1) 安全性更高

本文所设计的模型基于 DNSSEC 技术完成对服务端的验证, 信任链中的各节点均为经过授权的 DNS 服务器, 可信度高、被恶意控制的概率低. 对客户端的验证由区块链证书系统完成, 相比传统 PKI/CA 体系在安全性上具有明显优势. 一方面, 区块链去中心化、不可篡改的特性解决了由于 CA 中心化导致的单点故障风险, 另一方面, 区块链的共识机制确保了证书的可靠性, 解决了 CA 信任问题. 同时, 改进了用户证书格式, 实现了对用户设备的授权认证, 进一步加强了安全性.

(2) 双向身份验证

当前, 客户端基于 PKI/CA 体系可对服务端身份进行较有效的验证, 但考虑到用户证书的个体差异、管理复杂和成本较高等因素, 实际应用中 PKI/CA 体系很少应用于客户端证书的签发和验证, 限制了应用的安全性. 本模型中, 用户的证书由区块链生成, 区块链又处在服务端的监管下, 可以随时为用户签发安全, 可靠的证书, 实现双向证书验证的可行性更高.

(3) 灵活性更高

基于 PKI/CA 体系的证书验证通常对证书的格式有严格的要求, 且 CA 签发、更新证书前会进行一定的审核. 本文所设计的模型避免了对 CA 的依赖, 服务端可以根据自己的需求设计证书的格式, 使用更加灵活.

3.2 应用实例

随着互联网的快速发展, 越来越多的银行交易通过网上银行完成. 网上银行的安全性关系到用户敏感信息和财产的安全, 传统的账号加静态口令的方式已不能满足网上银行对安全性的要求[22]. 网上银行常用的 USB KEY 技术虽然在安全性上有所保障, 但是由于这种技术需要用户携带额外设备才能进行操作, 难以满足用户需要在多个终端进行登录的需求. 当前, 网上银行经常采用短信验证码对用户身份进行验证, 但短信验证码易被病毒木马拦截, 近年来也发生了多起由于短信验证码丢失造成用户财产损失的案例.

作为对安全性要求极高的互联网应用, 网上银行可以采用本文所设计的模型来提高自身的安全性. 新用户注册时, 首先通过客户端生成密钥对和证书, 随后向区块链用户证书管理系统发送证书. 区块链中的验证节点对证书进行验证后, 将证书记录在区块中, 并向用户返回证书验证结果. 新用户的证书生成完毕后, 用户可以在其注册时使用的设备上通过密码和证书双因素验证的方式登录到银行系统中进行操作. 此时, 即使用户的密码丢失, 其他人也不能在其他设备上进行登录. 当需要在其他设备上登录或需要取消某些设备的登录权限时, 用户可以通过已有私钥的设备直接向区块链系统发送授权/取消授权的请求来对设备进行管理.

用户对服务端的验证通过 DNSSEC 机制验证其 TLSA 记录实现, 银行生成自己的证书并在 DNS 中添加 TLSA 记录将服务和证书关联起来供用户进行验证. 为了进一步提升安全性, 银行还可以对 TLSA 中的记录进行轮转, 防止私钥被暴力破解. 具体流程如图 9 所示.

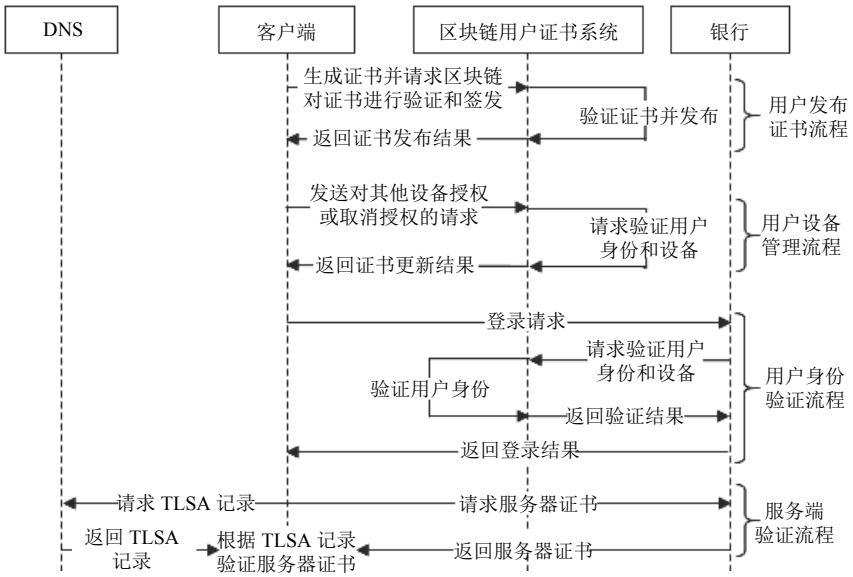

图 9 工作流程图

4 结束语

本文提出的利用区块链和 DNSSEC 技术进行双向身份验证的模型, 和现行的身份验证方法相比, 具有一些技术优势, 但也存在一些局限性. 首先, 本模型中服务端的 DNS 系统必须实施 DNSSEC, 客户端必须支持 DNSSEC 验证, 这一问题将随着 DNSSEC 更为广泛地实施而得到解决[23]; 其次, 本模型需要服务端搭建和管理区块链系统, 对于一些小型互联网应用可能存在一定难度, 该问题可以通过多家互相信任的互联网服务提供机构共同搭建和维护区块链得到解决.

互联网的快速发展使其成为了日常生活中不可或缺的一部分. 当互联网应用进入到支付、政务管理等敏感度较高的领域, 其带来巨大便利的同时, 也带来了严峻的安全挑战. 作为一项新兴技术, 区块链去中心化

和不可篡改的特性使其在安全领域的应用具有巨大的潜力. DNSSEC 对 DNS 提供的安全保障, 为 DNS 在域名解析之外的应用提供了可能性. 对这两项技术的研究和结合有望使互联网更加安全可靠.

参考文献

1 Van Droogenbroeck M. Introduction to PKI public key infrastructure. European Master in Multimedia Projects, Version, 2002, 1(1).

2 曹一生. PKI/CA 的研究与实现[硕士学位论文]. 北京: 北京工业大学, 2005.

3 毕宇. 基于区块链智能合约的 PKI-CA 体系设计. 金融科技时代, 2018, (7): 44–46. [doi: 10.3969/j.issn.2095-0799.2018.07.012]

4 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Consulted, 2008.

5 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展. 软件学报, 2018, 29(7): 2092–2115. [doi: 10.13328/j.cnki.jos.005589]

6 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494. [doi: 10.16383/j.aas.2016.c160158]

7 王李笑阳, 秦波, 乔鑫. 区块链共识机制发展与安全性. 中兴通讯技术, 2018, 24(6): 8–12, 40. [doi: 10.19729/j.cnki.1009-6868.2018.06.002]

8 阎军智, 彭晋, 左敏, 等. 基于区块链的 PKI 数字证书系统. 电信工程技术与标准化, 2017, 30(11): 16–20. [doi: 10.3969/j.issn.1008-5599.2017.11.004]

9 王继业, 高灵超, 董爱强, 等. 基于区块链的数据安全共享网络体系研究. 计算机研究与发展, 2017, 54(4): 742–749. [doi: 10.7544/issn1000-1239.2017.20160991]

10 周致成, 李立新, 李作辉. 基于区块链技术的高效跨域认证方案. 计算机应用, 2018, 38(2): 316–320, 326. [doi: 10.11772/j.issn.1001-9081.2017082170]

11 Arends R, Austein R, Larson M, *et al*. DNS security introduction and requirements, RFC4033. 2005.

12 Arends R, Austein R, Larson M, *et al*. Resource records for DNS security extensions. RFC4034. 2005.

13 Arends R, Austein R, Larson M, *et al*. Protocol Modifications for the DNS security extensions RFC4035. 2005.

14 El R, Bush B. Clarifications to the DNS specification, RFC-2181, 1997.

15 Gieben R, Labs SN. Chain of trust-the parent-child and keyholder-keysigner relations and their communication in DNSSEC. 2001.

16 Hoffman P, Schlyter J. The DNS-based Authentication of Named Entities (DANE) transport layer security (TLS) protocol: TLSA. RFC6698. 2012.

17 Hallam-Baker P, Stradling R. DNS Certification Authority Authorization (CAA) resource record. RFC6844. 2013. 1.

18 史伟奇. PKI 技术的应用缺陷研究. 中国人民公安大学学报 (自然科学版), 2007, 13(3): 53–56. [doi: 10.3969/j.issn.1007-1784.2007.03.013]

19 杨忍, 南凯. 一种基于 DNSSEC 的公钥分发方法及其应用. 科研信息化技术与应用, 2015, 6(3): 86–95. [doi: 10.11871/j.issn.1674-9480.2015.03.010]

20 柏宗超, 姚健康, 孔宁. 基于 DANE 的电子邮件安全研究. 计算机系统应用, 2018, 27(7): 71–77. [doi: 10.15888/j.cnki.csa.006427]

21 St Sauver J. CAA records: An alternative to DANE for protecting SSL/TLS certificate users. https://www.farsightsecurity.com/2017/08/25/stsauver-caa-records-farsight/. [2017-08-25/2019-03-07].

22 黄一平, 梁梓辰, 农丽萍, 等. 基于贴膜盾硬件数字证书的手机银行客户端通信安全研究与应用. 计算机应用与软件, 2018, 35(7): 313–319. [doi: 10.3969/j.issn.1000-386x.2018.07.056]

23 Lian W, Rescorla E, Shacham H, *et al*. Measuring the practical impact of DNSSEC deployment. Proceedings of the 22nd Usenix Conference on Security. Washington, WA, USA. 2013. 573–588.