(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.

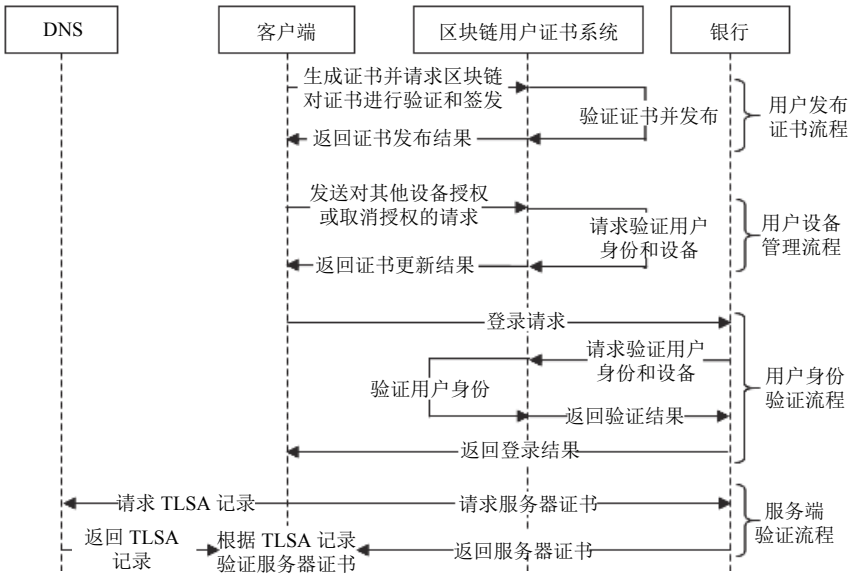

图 9 工作流程图

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.