计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(11):63−71 [doi: 10.15888/j.cnki.csa.007136]

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

基于区块链应用模式的铁路旅客身份认证系统①

郭志达, 王　鑫, 李金宇

(大连交通大学 经济管理学院, 大连 116028)
通讯作者: 郭志达, E-mail: zhidaguo@163.com

摘　要: 采用“区块链技术+不对称加密+生物识别+身份认证”应用模式, 依托智能手机客户端设计与开发一套铁路旅客身份认证系统. 基于 Ethereum 开发平台, 应用 truffle 开发框架, 实现铁路旅客身份认证系统智能合约的编写与部署. 系统针对传统铁路身份认证模式的不足, 将旅客身份数据分布式存储, 弱化中心化服务器的压力, 提升旅客身份数据的安全性和鲁棒性; 进行生物信息认证确保旅客对身份信息的所有权; 利用非对称加密技术在保护旅客隐私、实现实名制的前提下增强数据的透明性. 基于区块链应用模式的铁路旅客身份认证系统能够让用户身份实现本地存储、信息摘要链上校验, 实现铁路旅客身份信息数据访问的细粒度控制, 保障铁路旅客身份信息安全, 提升铁路旅客的乘车体验.

关键词: 铁路旅客; 区块链; 身份认证; Ethereum; 信息安全

引用格式: 郭志达,王鑫,李金宇.基于区块链应用模式的铁路旅客身份认证系统.计算机系统应用,2019,28(11):63−71. http://www.c-s-a.org.cn/1003-3254/7136.html

Railway Passenger Identity Authentication System Based on Blockchain Application Model

GUO Zhi-Da, WANG Xin, LI Jin-Yu

(School of Economics and Management, Dalian Jiaotong University, Dalian 116028, China)

Abstract: A railway passenger identity authentication system is designed and developed by using the application mode of “blockchain technology + asymmetric encryption + biometric identification + identity authentication” and relying on smart phone client. By the Ethereum development platform and truffle development framework, the intelligent contract of railway passenger identity authentication system is compiled and deployed. Aiming at the shortcomings of traditional railway identity authentication system, using distributed storage of passenger identity data to ease the pressure of centralized server, the system improves the security and robustness of passenger identity data. The system ensures the ownership of passenger’s identity information by bioinformatics authentication, and uses asymmetric encryption technology to enhance the transparency of data under the premise of protecting passenger’s privacy and realizing real-name system. The railway passenger identity authentication system based on blockchain application model can enable user identity to be stored locally and checked information abstract on the chain, realize fine-grained control of access to railway passenger identity information, guarantee the information security of railway passenger identity, and enhance the passenger experience.

Key words: railway passenger; blockchain; identity authentication; Ethereum; information security

① 基金项目: 国家自然科学基金 (7161025); 中国铁路总公司科技计划重点项目 (2017X006-C)
Foundation item: National Natural Science Foundation of China (7161025); Key Projects of Science and Technology Plan of China Railway Corporation (2017X006-C)
收稿时间: 2019-04-09; 修改时间: 2019-05-08; 采用时间: 2019-05-13; csa 在线出版时间: 2019-11-06

随着中国铁路客运进入“高速”时代, 铁路出行成为大众旅客的首选. 伴随着铁路旅客身份信息数据体量巨大、信息内容敏感、高价值等特点, 传统的身份认证模式已经不能满足“高铁时代”铁路旅客身份认证的安全需求与体验需求. 而区块链应用模式融合了P2P 网络、加密算法、分布式计算等多种技术, 将区块链应用模式应用于铁路旅客身份认证领域价值很大. 区块链应用模式广泛应用于教育就业、公民身份、电子护照等领域. Swan M 认为区块链在未来可以适用于金融服务、供应链管理、身份管理、教育就业等社会场景[1,2]. Fu DQ 利用区块链和 open badges规范设计了一套发布、显示、验证数字学位证书的系统[3]. Sullivan C 指出区块链技术的应用将会改变“电子公民”的信息存储校验方式[4]. Muzammal M 系统分析了基于区块链技术和传统分布式数据库特性的 ChainSQL 系统[5]. Zyskind G 利用区块链技术设计了一套去中心化的个人数据管理系统[6]. Paul D 对比了基于区块链技术身份认证项目的具体应用情况[7]. Faísca JG 基于 Web ID 与 JWT 实现去中心化身份管理[8]. 吕婧淑将面部识别和区块链结合, 提出一套双因子身份认证模型, 详细介绍了模型中所涉及的组件和参与方, 并阐述了模型的操作流程[9]. 国内学者对区块链应用模式也进行了大量研究, 王成提出实现精简保险业务流程的承保对账方案和实现自动化理赔的流程设计方案[10]. 周亮瑾为保障旅客的隐私安全提出利用区块链技术的数据、网络、系统和组织管理安全的管理策略与技术架构[11]. 陈宇翔分析了基于区块链的身份管理方案的优势[12]. 董贵山重点对较为成熟的 ShoCard 公司的区块链应用场景进行了分析[13]. 彭永勇在区块链上存储公钥加密的个人信息摘要, 私钥存储在客户端, 链上应用通过调用接口进行身份校验[14]. 史天运总结出适合区块链技术应用具有参与方多、交易复杂、涉及敏感信息传输等特点, 并提出铁路统一身份认证、信用管理、加密数字客票等应用的概念验证模型[15].

综上, 国内外学者基于多视角并结合多个应用领域对区块链技术进行了广泛的理论探讨与应用研究, 理论意义与现实价值很大, 但将区块链技术与零知识证明, 生物识别技术结合起来创新区块链应用模式并应用在铁路旅客身份认证领域还未涉及. 因此, 本文基于区块链应用模式, 面向智能手机客户端设计与开发一套铁路旅客身份认证系统 (简称“铁旅 ID 系统”), 以期提高铁路旅客身份认证效率, 提升铁路客运服务运作管理系统的品质.

1 铁旅 ID 系统业务

随着铁路客运运量的激增, 现有铁路旅客身份认证模式面临许多问题, 诸如中心化体系维护成本高, 易受攻击, 数据防篡改能力薄弱, 身份所有权模糊等. 利用区块链去中心化、分布式存储的特点可以弱化中心服务器的压力, 提高抗攻击能力; 其不可篡改的特点可以有效提升身份认证系统数据防篡改能力; 结合生物认证技术, 可以确保旅客对其身份拥有控制权; 借助零知识证明技术, 在旅客身份验证时, 仅需出示相关二维码即可, 校验方通过寻址对比, 就能验证信息真实性. 故本文提出“区块链技术+不对称加密技术+数字身份认证服务+生物识别技术”的技术解决方案. 基于上述分析, 基于区块链应用模式的铁路旅客身份认证系统需依托具有指纹识别、人脸识别功能的智能手机, 构建一个基于区块链应用模式的铁路旅客身份认证手机APP, 在铁路旅客进行购票、取票、进站、检票等需要验证个人身份的场景下, 利用铁旅 ID 系统进行身份授权与认证, 避免了用身份证号购票、出示身份证验证身份时可能造成的信息盗用与隐私泄露等问题, 具体用例如图 1 所示.

1.1 购票

当用户在 12306 手机客户端进行火车票购票时, 添加相应的乘车人, 此时就需要此乘车人使用铁旅 ID 系统对“用其身份进行购票”这一操作进行授权; 授权时, 铁旅 ID 系统会先对操作人进行生物识别, 确保操作人是身份所有者; 当确认操作人是身份所有者时, 系统会询问是否对“购买某车次车票”进行身份授权, 确认授权后, 12306 客户端就可以使用该乘车人身份进行购票了.

1.2 取票

当用户在自动取票机进行取票操作时, 取票机需先验证取票人身份信息, 此时, 用户需通过手机 APP 打开铁旅 ID 系统, 点击“出示身份二维码”选项; 系统会先对用户进行生物识别, 确保操作人是身份所有者; 当确认操作人是身份所有者时, 系统会显示该用户的身份二维码; 取票机扫描用户二维码, 获取用户身份信息, 打印出相应的纸质车票.

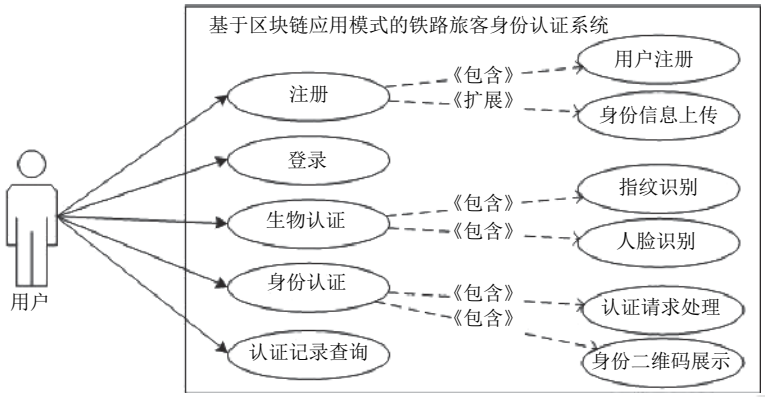

图 1 用例图

1.3 进站

当用户进站时, 车站工作人员需验证进站人身份、车次, 此时用户需打开铁旅 ID 系统, 点击“出示身份二维码”选项; 系统会先对用户进行生物识别, 确保操作人是身份所有者; 当确认操作人是身份所有者时, 系统会显示该用户的身份二维码; 车站工作人员扫描用户身份二维码, 获取用户身份信息、车次信息, 验证完毕, 用户即可进站.

1.4 检票

当用户上车检票时, 车站工作人员需验证进站人身份、车次, 此时用户需打开铁旅 ID 系统, 点击“出示身份二维码”选项; 系统会先对用户进行生物识别, 确保操作人是身份所有者; 当确认操作人是身份所有者时, 系统会显示该用户的身份二维码; 车站工作人员扫描用户身份二维码, 获取用户身份信息、车次信息, 验证完毕, 用户即可上车. 若用户购买的车次支持电子客票, 那么用户的乘车身份会与电子客票进行绑定, 用户无需取票, 出示身份二维码即可进站、检票和乘车.

2 铁旅 ID 系统设计

2.1 关键技术

(1) 开发平台的选择

选取 Ethereum[16]作为开发平台, 由于身份认证系统通常在某些特定用户间使用, 而不是 Ethereum 上所有节点, 所以为了提高效率, 系统将选用私有链. 从铁路旅客身份信息的所有权出发, 将身份信息存储在本地客户端, 身份信息经过系统验证之后将摘要数据在区块链上封存, 最终实现以 Ethereum 为原型的, 适用于铁路旅客身份认证应用场景的认证系统.

(2) 手机 App 技术选型

基于 HTML5[17]混合移动应用开发技术, 使用 React Native 作为开发框架, 采用 C/S 开发模型, 使用服务器处理客户端发出的请求.

(3) 服务器框架选型

基于 Node.js[17], 使用 Nest.js 作为服务框架可以构建一个完整的, 对 React Native 友好的服务器.

(4) 数据库选型

采用非敏感数据存储在 PostgreSQL 数据库中[18], 少量敏感数据存储在区块链中的解决方案.

2.2 整体架构

本文设计的铁旅 ID 系统将在 Ethereum 平台上开发实现, 结合 Ethereum 架构设计理念采用分层的架构设计模式. 整个铁旅 ID 系统被分为两个层次: 上层的身份认证接口层和底层的区块链服务层, 铁旅 ID 系统的整体架构如图 2 所示.

区块链服务层为整个系统搭建服务基础, 其中包括 3 个模块: 区块链服务模块, 智能合约服务模块, 成员管理模块. 铁旅 ID 系统中产生的不同事件将会触发不同的模块.

旅客身份认证接口为外部应用提供基本的区块链读写操作, 为铁旅 ID 用户和区块链之间搭建数据交换的桥梁, 铁旅 ID 系统有旅客、校验方、服务提供方、监管方等实体, 应用交互层能向外部实体提供身份认证服务、认证记录查询服务、初始身份查验服务、监管服务. 同时身份认证接口层能够响应用户对区块链上的数据查询请求, 利用认证记录查询接口获取数据, 并用更加友好的方式向用户展示身份认证记录信息.

应用交互层和区块链服务层共同组成信任服务模

型, 不但可改善传统中心化系统的不足, 而且还能满足旅客信息保护需求和监管需求.

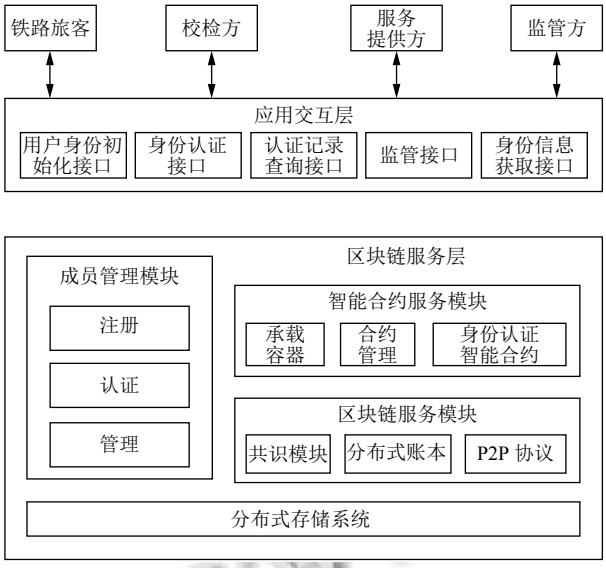

图 2 铁旅 ID 系统的整体架构

2.3 功能模块

铁旅 ID 系统有 5 个模块, 如图 3 所示, 分别是注册模块、登录模块、生物信息认证模块、身份认证模块和认证记录查询模块.

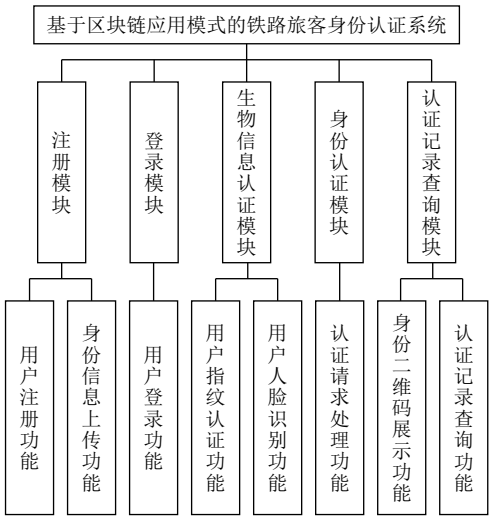

图 3 铁旅 ID 系统功能模块图

图 3 中, 注册模块包含旅客用户注册功能和旅客身份信息上传功能, 登录模块主要功能为旅客用户登录, 生物信息认证模块包含旅客指纹认证功能和人脸识别功能, 身份认证模块包含认证请求处理功能和身份二维码展示功能, 认证记录查询模块负责实现认证记录查询功能

1) 注册模块设计

注册模块流程图如图 4 所示, 首先旅客出行用户需要提供本人的手机号, 用户名, 密码等账户信息, 生成一个可登录的账户存入普通数据库内, 生成 JWT 返回至客户端, 然后客户端在本地创建非对称秘钥对, 并使用生物信息加密, 用户将其他身份信息 (手机号码, 身份证号码等) 和公钥回传至服务器, 系统将信息提交至身份审核接口; 用户身份审核通过后, 系统将存储用户公钥并用公钥将用户身份信息加密后写入区块链; 系统激活用户账户并调用智能合约将其余身份信息加密后写入区块链, 最后旅客用户注册成功.

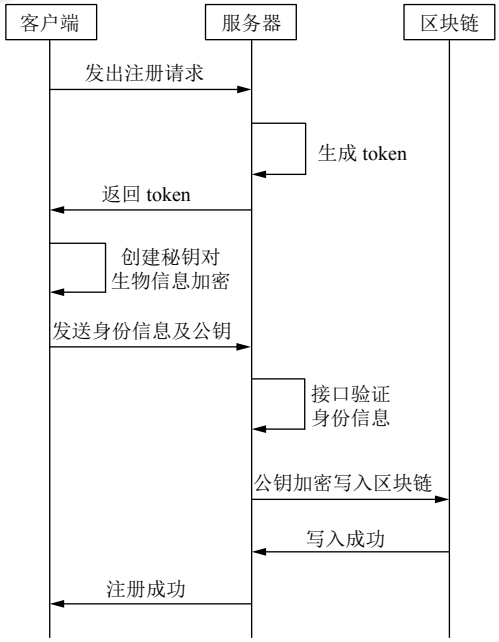

图 4 注册模块流程图

2) 登录证模块设计

登录模块流程图如图 5 所示, 客户端向服务器发起登录请求; 服务器接受请求, 从数据库请求用户账户信息摘要; 数据库返回账户信息摘要; 服务器验证账户信息并生成 token; 服务器向客户端返回 token, 用户登录成功.

3) 生物信息认证模块设计

生物信息认证模块流程图如图 6 所示, 客户端向服务器发起请求获取公钥加密的身份信息; 服务器接受请求, 并向区块链请求公钥加密的身份信息; 区块链向服务器返回公钥加密的身份信息; 服务器向客户端

返回公钥加密的身份信息; 客户端调用手机生物认证, 成功后用私钥解密身份信息.

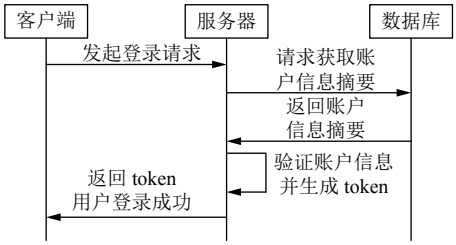

图 5 登录模块流程图

4) 身份认证模块设计

身份认证模块流程图如图 7 所示, 身份校验方向客户端发起身份认证请求; 客户端调用生物信息认证模块得到身份信息; 客户端向校验方发送私钥加密的用户信息、用户名、时间戳; 校验方向服务器请求公钥-服务器验证校验方合法性后返回用户公钥; 校验方用公钥解密信息并校验时间戳; 校验方使用用户名向区块链请求该用户加密的身份信息; 区块链向校验方返回用户加密的身份信息; 校验方用公钥加密用户身份信息并与区块链上的加密信息进行验证; 认证成功.

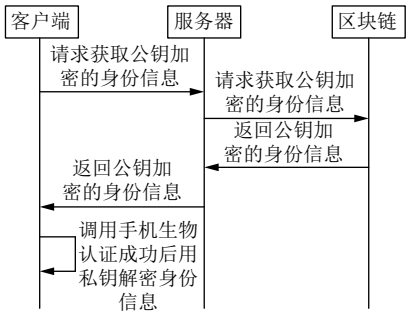

图 6 生物信息认证模块流程图

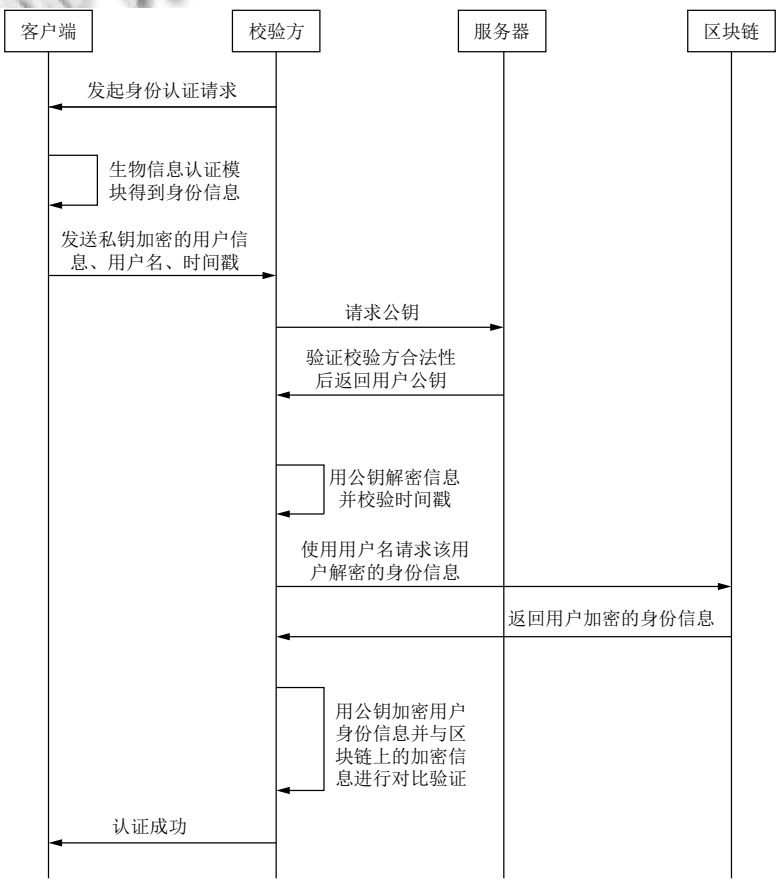

图 7 身份认证模块流程图

5) 认证记录查询模块设计

认证记录查询模块流程图如图 8 所示, 客户端调用手机生物认证核实用户身份; 生物认证成功后, 客户端向服务器发起请求获取身份认证记录; 服务器接受请求, 并向区块链请求身份认证记录; 区块链向服务器返回身份认证记录; 服务器向客户端返回身份认证记录.

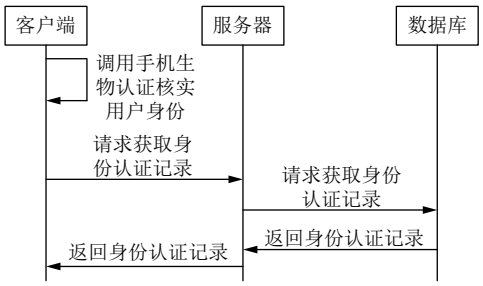

图 8 认证记录模块流程图

注册流程完毕后, 用户可以使用账号登录, 进入系统主页, 进行下一步操作. 系统主页中的“出示身份二维码”和“认证请求处理”两项功能都是对身份信息进行操作, 完成身份的认证和授权.

3 铁旅 ID 系统功能实现

3.1 注册及登录功能实现

用户注册、登录和主页功能界面如图 9 所示, 新用户点击立即注册即可进入注册页面, 铁路旅客可以通过该界面注册自己的铁旅 ID 账号, 用于登录系统. 账号注册完毕后, 用户还需提交自己的身份信息, 如图 10 所示, 通过正则校验和脚本的条件筛查可过滤大部分非法输入, 如果用户名重名、密码复杂度低、两次密码输入不一致、输入格式不匹配等输入错误, 系统界面会显示相应提示. 若服务端验证身份信息真实有效, 在通过生物信息识别后, 系统将身份信息进行摘要哈希处理生成数据摘要并保存在区块链上.

图 9 用户注册登录

3.2 生物信息认证及身份认证功能实现

当用户进行有关身份认证授权的操作时, 系统需先进行生物信息认证, 以确定操作人是身份所有者. 用户进行身份认证授权分两种情况, 主动出示身份二维码和其他 APP 认证请求处理.

在取票与进站等需要出示身份二维码的情景下, 如图 11, 用户点击“出示身份二维码”, 系统会进行生物信息识别, 识别通过后, 系统会显示包含用户名、公钥、时间戳的二维码.

在购票时, 12306 客户端会向铁旅 ID 请求身份认证授权, 此时, 铁旅 ID 会进行认证请求处理, 系统会显示请求时间、请求来源和授权原因, 如图 12, 用户点击“确定授权”, 在生物信息认证成功之后, 授权成功.

3.3 查询认证记录功能实现

身份认证记录查询功能记录了每一次用户身份的授权, 用户点击“认证记录查询”, 系统会先进行生物信息认证, 然后显示身份认证记录, 内容包括认证时间、请求来源和授权原因, 如图 13 所示.

本系统已在 Android、IOS 系统的设备上进行安装调试, 针对铁路旅客购票、取票、进站和检票等场

景, 对系统进行大量性能测试. 测试显示, 在一台八核主频 2.8 GHz 8 GB 的安卓设备上, 通过私钥解密信息的平均时耗为 23 毫秒; 将生成身份二维码的平均时耗为 52 毫秒; 在一台四核 3.3 GHz 8 GB 服务器上, 收到获取链上数据平均时耗为 130 毫秒, 在数据量上升至 20 万条后, 获取链上数据平均时耗为 470 毫秒, 其中测试结果主要受用户移动设备性能、服务器性能和网络延迟影响, 系统功能的可用性、信息验证的有效性、数据交互的正确性、生物认证的准确性都满足业务分析中提到的要求.

图 10 身份信息提交

图 11 身份二维码

4 结论

为了推进铁路旅客身份认证管理由集中式向去中心或多中心化创新发展, 优化铁路旅客身份认证管理的运作流程, 本文面向智能手机用户端, 设计并实现了一套基于区块链应用模式的铁路旅客身份认证管理系统. 第一, 系统把旅客身份信息保存在客户端本地, 信

息摘要封存在链上, 实现了铁路旅客身份信息本地存储、链上校验, 验证时无需出示明文身份信息, 仅需出示存有相关信息的数据摘要、公钥的二维码即可, 校验方通过寻址对比就能验证信息真实性, 有效避免了铁路旅客身份信息泄露问题. 第二, 系统将旅客身份信息数据分布式存储, 采用时间戳技术增强了旅客身份数据的抗篡改性和可追溯性, 利用非对称加密技术在保护旅客隐私、实现实名制的前提下增强了数据的透明性、安全性和鲁棒性, 进行生物信息认证确保了铁路旅客对身份信息的所有权, 部署智能合约提高了铁路旅客身份认证的准确性和智能化水平, 提供 API 实现第三方认证集成调用, 提供 SDK 实现二次扩展集成开发.

本研究的局限表现在没有对生物识别技术进行独立开发, 而是采取调用智能手机用户端自带生物识别接口的方式, 实现生物识别的功能. 下一步的研究可以考虑面向服务端来搭建私有链并对区块数据存储与智能合约的进行深入开发研究.

图 12 认证请求处理

图 13 认证记录查询

参考文献

1 Swan M. Blockchain thinking: The brain as a decentralized autonomous corporation. IEEE Technology and Society Magazine, 2015, 34(4): 41–52. [doi: 10.1109/MTS.2015.2494358]

2 Swan M. Blockchain temporality: Smart contract time specifiability with blocktime. Proceedings of the 10th International Symposium on Rules Technologies. Research, Tools, and Applications. Stony Brook, NY, USA. 2016. 184–196.

3 Fu DQ, Fang LR. Blockchain-based trusted computing in social network. Proceedings of the 2nd IEEE International Conference on Computer and Communications. Chengdu, China. 2016. 19–22.

4 Sullivan C, Burger E. E-residency and blockchain. Computer Law & Security Review, 2017, 33(4): 470–481.

5 Muzammal M, Qu Q, Nasrulin B. Renovating blockchain with distributed databases: An open source system. Future Generation Computer Systems, 2019, 90: 105–117. [doi: 10.1016/j.future.2018.07.042]

6 Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. Proceedings of 2015 IEEE Security and Privacy Workshops. San Jose, CA, USA. 2015. 180–184.

7 Dunphy P, Petitcolas FAP. A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 2018, 16(4): 20–29.

8 Faísca JG, Rogado JQ. Decentralized semantic identity. Proceedings of the 12th International Conference on Semantic Systems. Leipzig, Germany. 2016. 177–180.

9 吕婧淑, 操晓春, 杨培. 基于区块链和人脸识别的双因子身份认证模型. 应用科学学报, 2019, 37(2): 164–178.

10 王成. 基于区块链的保险业务流程优化方法研究. 铁道运输与经济, 2018, 40(10): 61–65.

11 周亮瑾, 王富章. 铁路客运私有链共识机制关键技术研究. 铁道运输与经济, 2018, 40(6): 59–63.

12 陈宇翔, 张兆雷, 卓见, 等. 基于区块链的身份管理研究. 信息技术与网络安全, 2018, 37(7): 22–26.

13 董贵山, 陈宇翔, 张兆雷, 等. 基于区块链的身份管理认证研究. 计算机科学, 2018, 45(11): 52–59. [doi: 10.11896/j.issn.1002-137X.2018.11.006]

14 彭永勇, 张晓韬. 基于区块链应用模式的可信身份认证关键技术研究. 网络安全技术与应用, 2018, (2): 36–37.

15 王成, 史天运. 区块链技术综述及铁路应用展望. 中国铁路, 2017, (9): 91–98. [doi: 10.3969/j.issn.1007-9971.2017.09.017]

16 黄俊飞, 刘杰. 区块链技术研究综述. 北京邮电大学学报, 2018, 41(2): 1–8. [doi: 10.3969/j.issn.1008-7729.2018.02.001]

17 Brito H, Gomes G, Santos e Jorge Bernardino Á. JavaScript in mobile applications: React native vs ionic vs NativeScript vs native development. Proceedings of the 13th Iberian Conference on Information Systems and Technologies. Caceres, Spain. 2018. 1–6.

18 刘红超, 缪燕, 郝悍勇, 等. 基于代理重加密的 PostgreSQL 系统访问控制方法. 计算机工程, 2018, 44(8): 192–198.