

数字人民币硬钱包在轨道交通中应用的安全性研究

朱嘉斌

苏州轨道交通科技创新研究院, 中国·江苏 苏州 215000

摘要: 随着数字人民币试点的持续推进, 其在轨道交通领域的应用不断拓展, 尤其是硬钱包的使用为乘客带来了“无电无网”支付的便利。然而, 安全问题始终是数字人民币广泛应用的核心关注点。本文聚焦数字人民币硬钱包在轨道交通场景中的安全应用, 从硬钱包本身的安全设计、轨道交通票务系统业务流程、系统运行、网络、数据及隐私、审计、异常处理、应急机制等多个维度展开研究分析, 深入剖析数字人民币硬钱包在轨道交通内使用的安全机制, 旨在全面建立针对数字人民币硬钱包的安全保障体系, 为数字人民币在轨道交通领域的安全、高效应用提供理论支撑与实践指导。

关键词: 轨道交通; 数字人民币硬钱包; 安全性

Research on the Security of Digital RMB Hard Wallets Application in Rail Transit

Zhu Jiabin

Suzhou Rail Transit Technology Innovation Research Institute Co., Ltd, China Jiangsu Suzhou 215000

Abstract: With the continuous advancement of the digital RMB pilot program, its application in the rail transit sector has been expanding. Particularly, the adoption of hard wallets has introduced the convenience of "power-free and network-independent" payments for passengers. However, security remains a core concern for the widespread application of digital RMB. This paper focuses on the secure implementation of digital RMB hard wallets in rail transit scenarios, conducting comprehensive research and analysis across multiple dimensions. These include the intrinsic security design of hard wallets, operational processes of rail transit ticketing systems, system operations, network infrastructure, data privacy protection, audit mechanisms, exception handling, and emergency response protocols. Through an in-depth examination of the security mechanisms governing digital RMB hard wallets in rail transit environments, this study aims to establish a holistic security assurance framework. The findings seek to provide both theoretical foundations and practical guidance for ensuring the secure and efficient application of digital RMB in the rail transportation sector.

Keywords: Urban railway transit; Digital RMB hard wallet; Security

0 引言

数字人民币硬钱包(以下简称“硬钱包”)是指基于安全芯片等技术, 能够实现数字人民币相关功能的集成电路(IC)、手机终端、物联网设备等硬件载体, 为用户提供数字人民币相关服务。硬钱包作为数字人民币的一种重要组成部分, 与软钱包一样属于法币。与软钱包相比, 硬钱包具有不依赖手机和网络使用的优势, 支持离网状态下“碰一碰”使用, 操作简单, 对老人和儿童更加友好, 尤其适合在无网无电场景下使用。随着基于 IC 卡、手机 PAY、用户标识模块(SIM)卡等形态的硬件钱包近段时间陆续面向大众进行推广, 硬钱包在轨道交通中应用关乎用户资金安全、隐私保护以及轨道交通系统的稳定运行, 深入研究数字人民币硬钱包在轨道交通内使用的安全机制具有重

要的理论与实践意义。

数字人民币硬钱包在轨道交通中的安全机制设计是一个多维度、多层次的综合性问题, 其核心在于保障支付过程的安全性、隐私保护以及系统的可靠性。本文从硬钱包产品、票务系统运行和支付流程设计等方面详细分析其安全性设计。

目前针对硬钱包在轨道交通应用的研究文献较少。何书亮^[1]研究了在数字经济时代将数字人民币支付手段应用在轨道交通售票检票系统的需求, 并比较了数字人民币软硬钱包在票务系统中的差异及其存在的问题, 最后阐述了数字人民币支付在轨道交通领域所带来的优势, 并对未来发展进行展望。朱嘉斌^[2]总结了数字人民币在轨道交通中的主要支付场景, 以及几种主要的应用方式, 提出了轨道交

通需要研究的系统所实现的主要内容,总结了数字人民币在未来轨道交通中应用的研究方向。许玲等^[3]介绍了宁波地铁应用数字人民币软钱包的主要场景,以及运营的改造实施方案。周世爽等^[4]根据数字人民币软件钱包与硬件钱包的应用规范,分析软件钱包直接支付、免密支付、收银台支付以及硬件钱包价值支付、准账户支付,在城轨交通领域的应用场景、应用方案与应用特点,并结合实际应用经验对各种应用模式进行利弊分析。总结软件钱包与硬件钱包最优应用场景与方案,提出数字人民币应用的系统架构及“数字人民币+公共交通卡”双应用的建议。袁媛等^[5]研究基于超级SIM卡安全芯片能力,存储数字人民币币串实现双离线交易,打造具有运营商特色的硬钱包产品SIMPAY,是SIM卡技术和数字人民币技术的创新融合,为硬钱包技术的实际应用提出了新的思路和解决方案。苗守庭等^[6]阐述了数字人民币运营机制、特性及“铁路客票+业务”的特点,在此基础上研究设计了铁路客票+业务数字人民币独立数字钱包体系、多级数字钱包体系,分析了基于数字人民币智能合约的铁路客票+支付结算业务流程,以及不同资金收付模式下的资金流程,提出了与传统支付方式统一结算的可行性方案,可为未来数字人民币在铁路客票+业务的运用提供参考。黄芸等^[7]对数字人民币在高速公路联网收费领域中落地应用的可行性进行了分析,包括数字人民币在联网收费发行场景应用、在交易场景进行应用。许文达等^[8]开展数字人民币在电网中的应用研究、收支结算、规范管理及实施部署等。朱嘉斌等^[9]深化探讨数字人民币硬钱包在无网无电情况下直接过闸项目的主要研究内容和路径。重点分析研究硬钱包过闸流程、计费机制、收款对账以及与银行平台的连接方式等关键技术,并比较每个关键技术可选方案的优缺点,提出推荐方案。

1 硬钱包在轨道交通中应用安全性研究综述

当前主流的硬钱包从外在形式上分为基于智能卡的卡片式硬钱包、基于运营商数字人民币SIM卡的硬钱包以及基于SE芯片NFC移动设备(手机PAY)的硬钱包3种类型。

研究硬钱包在轨道交通中应用的安全性主要分为数字人民币硬钱包本身的安全性、轨道交通票务系统可靠性设计、票务系统支付流程的安全设计、异常处理与应急机制等方面与内容。

2 数字人民币硬钱包本身的安全性设计

2.1 硬钱包硬件层面安全设计

数字人民币硬钱包通常采用安全芯片作为核心组件,

安全芯片具备强大的加密运算能力,能够对私钥、交易信息等关键数据进行加密存储,结合先进的非对称国密算法,如椭圆曲线加密算法(ECC),在保障安全强度的同时,提高了加密和解密的效率。硬钱包内部集成了多种安全功能模块,包括随机数发生器、加密引擎和安全存储单元。随机数发生器生成高强度的随机数,作为加密密钥的种子,确保每次加密的密钥都是独一无二的,极大地增加了破解难度。安全存储单元采用特殊的物理结构和存储技术,防止数据被非法读取和篡改。

由于SIM卡本身具有加密功能,再加上数字人民币软钱包的关联,使得数字人民币SIM卡硬钱包在使用过程中具有更高的安全性。一旦发生丢失或被盗的情况,用户可以通过远程锁定或删除该钱包来避免损失。此外,数字人民币SIM卡硬钱包还支持匿名支付,用户可以设置匿名支付密码,保护个人隐私。

2.2 软件层面安全设计

硬钱包所采用的操作系统经过专门定制和安全加固。以基于Linux内核定制的操作系统为例,对内核进行了深度裁剪,去除了不必要的功能模块,减少了系统的攻击面。在操作系统层面,采用了严格的访问控制机制,根据用户角色和操作需求,设置了不同的权限级别,只有经过授权的用户才能访问特定的文件、设备和系统功能,有效防止非法用户入侵。同时,对敏感数据进行全生命周期的加密保护,在数据存储阶段,采用磁盘加密技术,将数据以密文形式存储在存储设备中;在数据传输过程中,使用安全的通信协议,如传输层安全性协议TLS(Transport Layer Security)协议,对数据进行加密传输,确保数据的安全性和完整性。

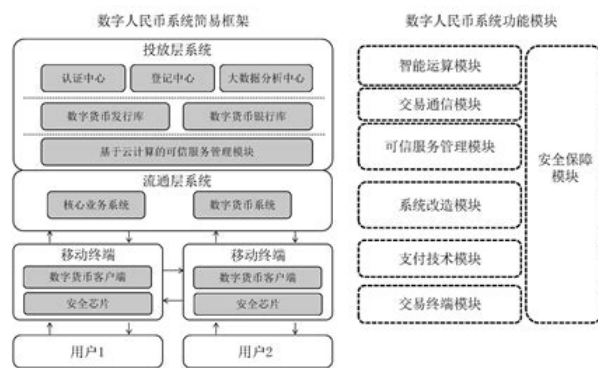


图1 数字人民币系统框架及功能模块

硬钱包中的应用程序在开发过程中遵循严格的安全规范。开发人员采用安全编码技术,避免出现常见的安全漏洞,如缓冲区溢出、SQL注入(欺骗数据库服务器执行非

授权的任意查询)等。在应用程序架构设计上,采用分层架构和模块化设计,将不同功能模块分离,降低模块之间的耦合度,提高系统的安全性和可维护性。例如,将用户界面层、业务逻辑层和数据访问层进行分离,各层之间通过严格定义的接口进行通信。此外,应用程序还采用数字签名技术,开发者使用私钥对代码和数据进行签名,用户在安装和使用应用程序时,通过验证开发者的公钥来确认应用程序的完整性和真实性,防止应用程序被恶意篡改。

3 数字人民币硬钱包在轨道交通中应用的安全性设计

3.1 轨道交通应用硬钱包的业务流程安全性设计

轨道交通应用数字人民币硬钱包的业务流程分为交易开始、交易处理中、交易完成等几个主要环节,安全性设计分别从交易的合法验证、安全评估和风险控制等方面展开。

交易开始时,轨道交通票务系统终端设备与数字人民币硬钱包之间的读写操作严格遵循安全规范,握手交互后,票务系统对该硬钱包进行合法性验证,检查硬钱包账户是否合法、硬钱包是否有违规记录等。轨道交通票务系统对硬钱包设计黑名单规则,对乘车记录可疑或过往乘车未付款的硬钱包设置黑名单或灰名单,禁止乘坐或限制乘坐轨道交通。

在交易处理过程中,实时记录交易状态和相关信息,如交易发起时间、交易流水号等,系统生成包含交易金额、时间、设备标识等信息的交易凭证,并对该凭证进行数字签名。闸机在接收到交易凭证后,对签名进行验证,确认交易的真实性和完整性。为防止离线交易中的重复支付问题,硬钱包和闸机均采用序列号管理机制,每一笔交易都有唯一的序列号,硬钱包在完成一笔交易后,记录该交易的序列号,下次交易时检查序列号是否重复,闸机在接收到交易凭证后,也检查该序列号是否已处理过,若发现重复序列号,则拒绝该交易。

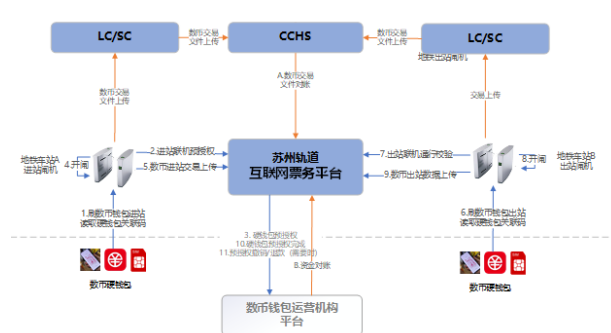


图2 硬钱包过闸业务流程图

交易完成后,对交易结果进行验证和确认,确保交易的准确性和完整性。同时,建立交易异常处理机制,当出现交易失败、交易超时等异常情况时,有相应流程措施能够及时应对,如自动重试交易、向用户发送异常提示信息等,客服系统也设计了软件流程保证交易安全。

3.2 轨道交通应用硬钱包的系统运行安全性设计

数字人民币硬钱包在轨道交通中的应用涉及多类设备,包括闸机、客服设备、车站服务器、线网票务平台等。为确保数字人民币硬钱包应用过程中,轨道交通票务系统的高可用性和高安全性,系统运行采用冗余设计和备份机制,能够实现7×24小时不间断运行。在硬件层面,关键设备如服务器、存储设备等采用云技术、冗余配置等,当某一设备或某单一节点出现故障时,系统不受影响,能继续正常运行。在软件层面,采用集群技术,将票务系统多个服务器组成一个集群,共同承担业务负载,提高系统的处理能力和可靠性。

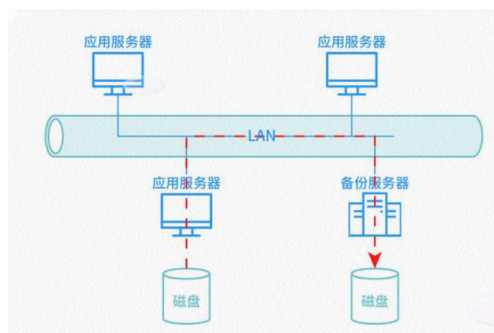


图3 票务系统冗余备份图

3.3 轨道交通应用硬钱包的网络安全性设计

在网络架构方面,轨道交通票务系统采用多层次的网络安全防护体系。包括边界隔离、内部监测和主机审计等措施,以全面防御外部攻击和异常事件。

轨道交通票务系统与银行之间采用专线连接,保证整体数据传输的安全高效。在网络边界部署防火墙设备等,对进出票务系统的网络流量进行严格访问控制。防火墙根据预先设置的安全策略,允许合法网络流量通过,阻止非法网络访问和攻击。例如,只允许来自数字人民币运营机构的特定IP地址段的流量进入票务系统核心交易区域,禁止其他未经授权的外部网络访问。同时,采用入侵检测系统(IDS, Intrusion Detection System)和入侵防御系统(IPS, Intrusion Prevention System)对网络流量进行实时监测和分析。IDS实时监测网络中的异常流量和攻击行为,一旦发现潜在安全威胁,立即发出警报通知系统管理员;IPS则在检测到攻击行为时,主动采取措施进行防御,

如自动阻断攻击源网络连接,防止攻击扩散。

为防止内部网络安全风险,采用虚拟专用网络(VPN, Virtual Private Network)技术,将票务系统内部不同区域网络隔离,限制不同区域之间网络访问。例如,将负责数字人民币硬钱包交易处理的服务器区域与其他业务服务器区域通过VPN隔离,只有经过授权的内部用户才能通过VPN访问特定区域服务器,提高内部网络安全性。

数币硬钱包应用的主机审计包括系统资源监控、硬钱包用户行为审计、硬钱包交易日志管理与智能分析等。

3.4 硬钱包在票务系统中的数据安全性及隐私保护设计

数字人民币硬钱包在轨道交通应用中会产生较多敏感数据,包括用户交易记录、账户信息、设备信息等,都需要进行安全存储、传输。

在处理硬钱包业务过程中,无论是在线交易还是离线交易,票务系统都对硬钱包交易数据的传输进行严格加密和完整性保护。硬钱包交易数据在传输过程中,为了防止敏感信息泄露,交易报文中的金额、交易双方钱包地址、交易时间等敏感信息进行加密处理。可同时采用两套安全的加密算法进行保护并相互认证,一套为高级加密标准AES(Advanced Encryption Standard)+非对称加密算法(RSA2),另一套为信息摘要算法(MD5)。乘客使用数字人民币硬钱包过闸时,硬钱包与闸机间的数据先经过加密处理,以密文形式在网络中传输。为确保交易数据在传输过程中不被篡改,采用数字摘要技术,信息摘要算法(MD5)。发送方在发送交易数据前,使用信息摘要算法(MD5)算法对交易数据进行计算,生成一个固定长度的数字摘要,并将该数字摘要与交易数据一起发送给接收方。接收方在接收到交易数据后,同样使用信息摘要算法对交易数据进行计算,得到一个新的数字摘要,然后将接收到的数字摘要与新计算得到的数字摘要进行比对,如果两者一致,则说明交易数据在传输过程中未被篡改;若不一致,则说明交易数据可能已被篡改,接收方拒绝该交易。

数字人民币硬钱包在轨道交通应用中遵循可控匿名原则,保护用户隐私的同时,满足监管机构对反洗钱、反恐怖融资等合规性要求。在轨道交通场景中,数字人民币硬钱包相关各方遵循数据最小化收集与使用原则,仅收集和使用为实现业务功能所必需的用户数据。轨道交通运营方在用户使用数字人民币硬钱包乘坐地铁时,仅收集与乘车交易相关的数据,如进出站时间、站点信息、支付金额等,不会收集与乘车业务无关的用户个人信息。对于收集到的

数据,也仅用于乘车费用计算、票务统计、运营分析等与轨道交通运营直接相关的业务目的,不会将数据用于其他未经用户授权的商业用途。例如,轨道交通运营方不会将用户乘车数据出售给第三方广告商用于精准营销。此外,各方在数据使用过程中,对涉及用户个人信息的数据进行去标识化处理,通过技术手段将用户个人身份信息与其他数据分离,降低因数据泄露导致用户个人信息暴露的风险。在进行数据分析和挖掘时,使用去标识化后的数据,既能满足业务需求,又能有效保护用户隐私。

3.5 轨道交通关于硬钱包的安全审计、异常处理、应急机制设计

轨道交通票务系统应针对数字人民币硬钱包相关的操作和交易设计全面审计机制。安全审计系统实时记录和收集系统中的各种安全事件,包括交易操作、系统配置变更等。对这些信息进行分析和挖掘,及时发现潜在的安全威胁和异常行为。例如,通过对交易数据的分析,发现某一用户在短时间内进行了大量异常交易,安全审计系统能够及时发出警报,提示系统管理员进一步调查。同时,定期生成安全审计报告,对系统的安全状况进行评估和总结,为系统的安全改进提供依据。

轨道交通票务系统须针对数字人民币硬钱包设计相关异常处理机制。如当系统设备离线后原认证机制无法正常运行,设计票务系统设备的降级模式,只在终端设备做合法性校验,成功后就放行持硬钱包的乘客。后续待网络恢复后,上传相关交易数据信息。其他异常票务场景通过自助终端或半自动售票机设计相应流程处理。异常处理机制确保了乘客在极端情况下仍能顺利完成支付和进出站操作。另外,针对可能出现的安全事件,轨道交通票务系统应设计对应的应急机制。应急机制将根据安全事件的分类、分级标准,设计不同级别安全事件的应急处理流程。当发生安全事件时,系统能够迅速启动应急机制,采取相应的应急措施,如立即停止相关业务操作、隔离受影响的系统模块、进行数据备份和恢复等,以降低安全事件造成的损失和影响。同时,考虑建立与数字人民币运营机构、监管部门等相关方的应急沟通协调机制,及时通报安全事件情况,协同开展应急处置工作。此外,定期对应急响应预案进行演练和评估,不断完善应急预案,提高系统的应急响应能力。

4 结语

数字人民币硬钱包作为一种新兴的支付工具,在轨道交通内的使用为乘客带来了便捷、高效的支付体验,同时

也为轨道交通运营管理带来了新的机遇和挑战。随着技术的不断发展和应用场景的不断拓展,数字人民币硬钱包在轨道交通内使用的安全问题需要持续关注和研究。未来,需要进一步加强技术创新,提高安全防护能力,完善安全管理制度,以应对不断变化的安全挑战,推动数字人民币硬钱包在轨道交通领域的安全、广泛应用,为数字经济的发展提供有力支撑。

参考文献:

- [1] 何书亮. 数字人民币在地铁票务系统中的应用研究[J]. 智能建筑与智慧城市, 2023(03):160-162. HE Shuliang. Application study of digital RMB in subway ticketing system[J]. Intelligent Building & Smart City, 2023(03): 160-162.
- [2] 朱嘉斌. 数字人民币在轨道交通中的应用实践[J]. 智慧轨道交通, 2023, 60(04): 73-76. ZHU Jiabin. Application practice of digital currency electronic payment in rail transit[J], Smart Rail Transit, 2023, 60(04): 73-76.
- [3] 许玲, 曾海军, 汪可可等. 宁波轨道交通数字人民币票务场景应用项目实践[J]. 城市轨道交通, 2023(08): 44-45.
- [4] 周世爽, 梁靖, 王欢等. 数字人民币在城轨交通领域应用模式研究[J]. 都市快轨交通, 2022,35(04): 161-167. ZHOU Shishuang, LIANG Jing, WANG Huan, et al. E-CNY application mode in urban rail transit[J]. Urban Rapid Rail Transit, 2022, 35(04): 161-167.
- [5] 袁媛, 郑建兵, 许军等. 基于超级 SIM 卡的数字人民币硬钱包应用研究[J]. 江苏通信, 2023, 39(05): 61-63. YUAN Yuan, ZHENG Jianbing, XU Jun, et al. Research on the application of digital RMB hard wallet based on super SIM card [J]. Jiangsu Communications, 2023, 39 (05): 61-63.
- [6] 苗守庭, 景晓志, 冉泽宇等. 数字人民币智能合约在铁路客票 + 业务支付结算的应用研究[J/OL]. 铁道运输与经济, 1-9[2024-03-18]. <http://kns.cnki.net/kcms/detail/11.1949.U.20231102.1639.004.html>. MIAO Shouting, JING Xiaozhi, RAN Zeyu, et al. Research on the application of digital RMB smart contract in railway ticket + business payment and settlement [J/OL]. Railway Transportation and Economy. 1-9[2024-03-18]. <http://kns.cnki.net/kcms/detail/11.1949.U.20231102.1639.004.html>.
- [7] 黄芸, 刘旭, 郑婧婧等. 数字人民币在高速公路联网收费中的应用[J]. 中国交通信息化, 2022.06.
- [8] 许文达, 桑文奇, 杨宇等. 数字人民币推广应用的电网模式[J]. 国企管理, 2023,(11): 108-113.
- [9] 朱嘉斌, 付保明, 陆金睿等. 数字人民币硬钱包无网无电直接过闸关键技术研究[J]. 现代城市轨道交通, 2024(05): 138-143.

作者简介: 朱嘉斌 (1983.05-), 男, 江苏省靖江市人, 硕士, 高级工程师, 苏州轨道交通科技创新研究院有限公司资深主管、票务及智慧化应用。