

数字人民币乘车码在城市轨道交通中的应用*

张 森¹ 于 敏² 李守杰³

(1. 广州地铁设计研究院股份有限公司, 510010, 广州; 2. 工业和信息化部电子第五研究所, 511370, 广州;

3. 宁波市城市轨道交通集团有限公司, 315100, 宁波)

摘 要 [目的]随着数字人民币(以下简称“数币”)在我国各行各业全面开花,城市轨道交通数币应用场景也逐步丰富,传统上数币在轨道交通仅作为第三方支付应用,功能与支付宝、微信相似。为进一步扩展应用场景,提出使用数币 APP(应用软件)直接生成数币乘车码,乘客直接使用数币二维码进出车站,使数币出行场景更便捷。[方法]介绍了城市轨道交通应用场景下的数币支付系统整体架构及各模块功能;介绍了数币二维码设计方案,以及关键业务流程。[结果及结论]采用数币软钱包,并基于数币密钥及地铁密钥两个非对称密钥,同时参考交通部二维码编码格式,生成数币二维码。以数币密钥及地铁密钥为安全保障,明确了 APP 请码、闸机验码、支付结算等关键业务流程。

关键词 城市轨道交通; 数字人民币; 二维码

中图分类号 U293.22; TP393.09

DOI:10.16037/j.1007-869x.2024.12.052

Research on the Application of E-CNY Boarding Code in Urban Rail Transit

ZHANG Sen¹, YU Min², LI Shoujie³

(1. Guangzhou Metro Design & Research Institute Co., Ltd., 510010, Guangzhou, China; 2. The 5th Electronics Research Institute of the Ministry of Industry and Information Technology, 511370, Guangzhou, China; 3. Ningbo Rail Transit Group Co., Ltd., 315100, Ningbo, China)

Abstract [Objective] As in China E-CNY (hereinafter referred to as "digital currency") flourishes in all walks of life, the application scenarios of digital currency in urban rail transit are gradually enriched. Traditionally, digital currency is only used as a third-party payment application in rail transit, with functions similar to those of Alipay and WeChat. In order to further expand the application scenarios, it is proposed to use the digital currency APP (application software) to directly generate the digital currency boarding code, so that passengers can directly use the digital currency QR code to enter and exit the stations, making the digital currency travel scenarios more convenient. [Method] The overall architecture and each module

functions of the digital currency payment system in urban rail transit application scenarios are introduced; the digital currency QR code design schemes and key business processes are introduced. [Result & Conclusion] Using digital currency soft wallet, and based on two asymmetric keys, the digital currency key and the subway key, the digital currency QR code is generated with reference to the Ministry of Transport QR code encoding format at the same time. With the digital currency key and the subway key as security guarantees, key business processes such as APP code request, gate code verification, and payment settlement are clarified.

Key words urban rail transit; E-CNY; QR code

随着网络技术和数字经济蓬勃发展,中国数字人民币(以下简称数币)发展迅猛,自 2017 年人民银行开展法定数字货币研发以来,已发布多批次试点城市或区域。截至 2022 年 12 月,数币试点地区共有 17 个省市 26 个试点地区,包括北京、上海、广州、深圳、海南、长沙、西安、青岛、大连、天津、重庆、福州、厦门、浙江省承办亚运会的 6 个城市、南宁、昆明等,数币已经逐步向全国各行各业扩展开来。

根据《中国数字人民币研发进展白皮书》要求,零售支付体系中,数字人民币和指定运营机构的电子账户资金具有通用性,共同构成现金类支付工具。为落实《中国城市轨道交通智慧城市轨道交通发展纲要》,促进数币在城市轨道交通内更广泛的应用,为丰富智慧城市轨道交通多元过闸手段,构建更便捷的智慧乘客服务具有重要的现实意义。

在城市轨道交通领域,北京、深圳、杭州、苏州、广州等多地城市轨道交通已开通支付应用场景^[1],即乘客开通数币免密支付,作为第三方支付关联地铁虚拟票种,其功能定位与支付宝、微信一致^[2]。但数币软钱包二维码直接作为票卡使用,目前国内还处于探讨试点阶段。本文仅对数币乘车码在

* 广东省基础与应用基础研究基金项目(2019B1515120086)

城市轨道交通领域应用进行研究,提出了支持在线、离线应用方式,研究成果供各城市应用参考。

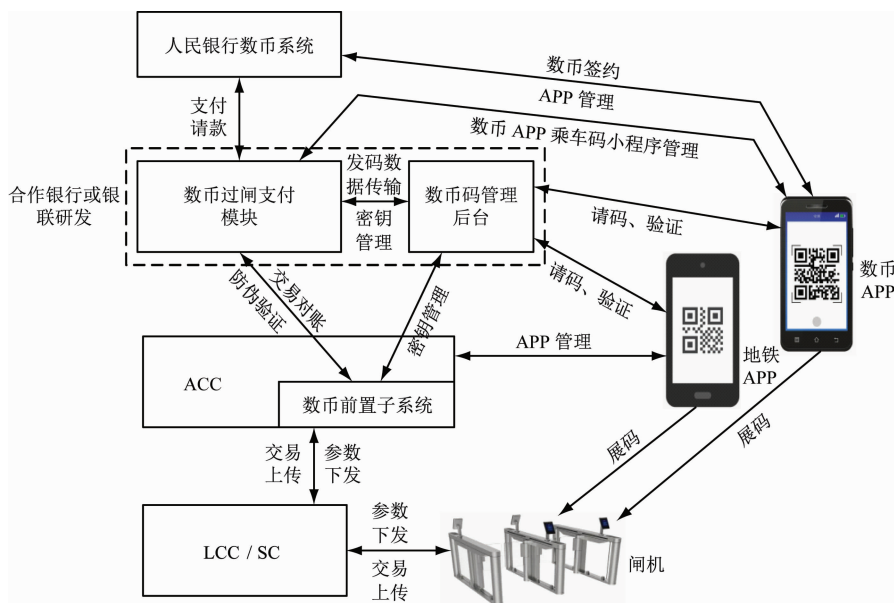
1 城市轨道交通数币乘车码应用架构及各模块功能分析

数币乘车码在城市轨道交通中的应用^[3]涉及

地铁自动售检票系统升级、数币 APP(应用软件)和地铁 APP 的升级,需新建数币过闸支付模块及数币码管理后台,整体架构如图 1。

1.1 数币过闸支付模块

新建数币过闸支付模块完成乘车码支付管理、收入结算、运营监管、数据统计报表以及相应的权



注:ACC 为自动售检票清分中心; SC 为车站计算机; LCC 为线路中央计算机。

图 1 城市轨道交通数币乘车码应用架构图

Fig. 1 Architecture diagram of urban rail transit digital currency boarding code APP

限管理和操作日志管理等功能,以便安全规范地管理乘车码和全方位了解运营的数据。

1) 支付管理:对数币乘车码订单进行支付管理,可以按订单类型、运营商、支付状态进行筛选、检索。

2) 结算管理:对数币乘车码收单账户结算管理,与地铁自动售检票清分中心实现对账、日结等管理功能。

3) 异常坏账处理:对多次请款失败的乘客账单,根据合作协议进行坏账分担,同时为防止风险扩大,将此类乘客账户列入黑名单。

4) 运营监管:对数币乘车码的人群、人次、线路、区域以及使用次数进行实时监测,为运营决策提供数据支撑。

5) 报表统计:实现注册开通、经营财务、坏账欠费、刷码流量、刷码金额等报表统计功能。

数币过闸支付设备可由合作银行进行研发,当有多家合作银行时,建议由银联负责研发。

1.2 数币码管理后台

新建数币码管理后台负责乘车码密钥管理及根据乘车码编制规则生成唯一的数币乘车码并下发。

密钥管理对数币和(地铁)行业两个非对称公私密钥进行管理,包括公私钥对生成、状态查看、安全管理等功能。

数币码管理后台可由合作银行进行研发,当有多家合作银行时,建议由银联负责研发。

1.3 地铁 APP 及数币 APP

研发数币二维码小程序,嵌入数币 APP 或合作银行 APP;地铁 APP 按需使用 SDK(软件开发工具包)嵌入实现申请、获取及显示数币码,此时地铁 APP 会存在数币乘车码和地铁乘车码两个互不关联的二维码票种,各城市可按需使用。

1) 注册开通:按步骤提示乘客实现录入信息注册、绑定数币免密支付、开通乘车码功能。

2) 请码展码:在线向数币码管理后台请码及离

线请码、展示数币乘车码,实现扫码进/出站。

3) 数据存储:将下发的数币码及公钥在本地存储,用于有效期内的离线请码。

4) 信息通知:接收数币过闸支付模块推送的已进站、已出站消息,并展示。

5) 补款通知:对于未支付的异常乘车记录,在乘客下次打开 APP 时实现补款提醒。

1.4 清分中心

ACC^[4]增设数币前置子系统,负责数币交易验证、账单对账、运营监管、日结管理、统计分析等功能。

1) 交易验证:对闸机上传的实时交易进行防重、单边、合法性验证,对结算交易进行 CRC(循环冗余校验)码及 TAC(型号分配)码防欺诈检查、交易配对、计算票价、无效交易可疑账单处理等操作。

2) 账单对账:向数币过闸支付设备进行交易请款及对账。

3) 运营监管:接收上层系统下发的数币参数并下发;对数币乘车码交易进行存储及分析,可按人群、人次、线路、车站、区域进行分析挖掘,为运营决策提供数据支撑。

4) 其他功能:具有数币票款清分、日结管理、报表统计等功能,与 ACC 原功能类似,本文不再赘述。

1.5 LCC 及 SC

LCC 及 SC 负责闸机与上层系统之间的数据上传下达的工作,即增加数币参数下发、数币交易上传等功能。

1.6 闸机升级分析

自动检票机增加验证数币乘车码功能,具体包括乘车码读取、有效性检查、交易数据打包上传、在线接受数币前置子系统开闸指令、离线开闸放行等功能。

其中有效性检查主要包括:安全性检查、验真检查、有效时间检查、状态检查、超时检查、黑名单等。

2 数币二维码设计方案

目前,人民银行尚无全国交通领域的数币乘车码标准,本次研究参照 JT/T 1179—2018《交通一卡通二维码支付技术规范》进行码设计(见表 1)。待人民银行有新标准发布后,可重新设计,原理相似。

3 关键业务流程

3.1 APP 请码

3.1.1 在线请码

数币 APP/地铁 APP 需在线并已签约数币支

表 1 数币二维码格式建议表

Tab. 1 Suggestion table for digital currency QR code format

序号	字段	长度/字节	备注
1	版本号	1	
2	码数据量	2	
3	发码机构公钥	117	数币公钥
4	支付账户号	16	缺省值
5	用户账户号	10	以手机作为唯一标志
6	发码机构代码	4	合作银行代码
7	发码机构平台编码	4	合作银行编码
8	用户账户类型	1	为数币用户定义新类型
9	单次消费金额上限	3	缺省值
10	用户公钥	33	行业(地铁)公钥
11	支付账户系统授权过期时间	4	按需设置
12	二维码有效时长	2	一般为 10~30 s,按需设置
13	发码机构自定义域长度	1	
14	发码机构自定义域	20	按不同的 APP 渠道定义,如数币 APP、地铁 APP 等
15	发码机构私钥的签名	65	
16	二维码生成时间	4	
17	用户私钥的签名	65	

注:不适用于数币的字段使用缺省值填充。

付,APP 请求数币码管理后台获取乘车码字段信息,并缓存本地。

在线请码步骤为:

步骤 1: 乘客打开手机 APP 中数币乘车二维码功能。

步骤 2: APP 自查是否封码,即是否存在未支付账单,若有则提醒乘客在线补款。

步骤 3: APP 打包乘客账户标志(手机号)、时间、位置等数据,向数币码管理后台申请数币密文。

步骤 4: 数币码管理后台将 APP 发送的信息使用数币公钥进行加密,并返回 APP。

步骤 5: APP 打包乘客账户标志、请码渠道、时间、位置、步骤 4 返回的数币密文等数据,向数币码管理后台申请地铁密文。

步骤 6: 数币码管理后台将 APP 发送的信息,附加有效期等,生成二维码字段信息,使用地铁公钥进行加密,并返回 APP。

步骤 7: APP 将二维码字段信息在手机端存

储,生成二维码图片,向乘客展码。

在线清码流程示意图如图 2 所示。

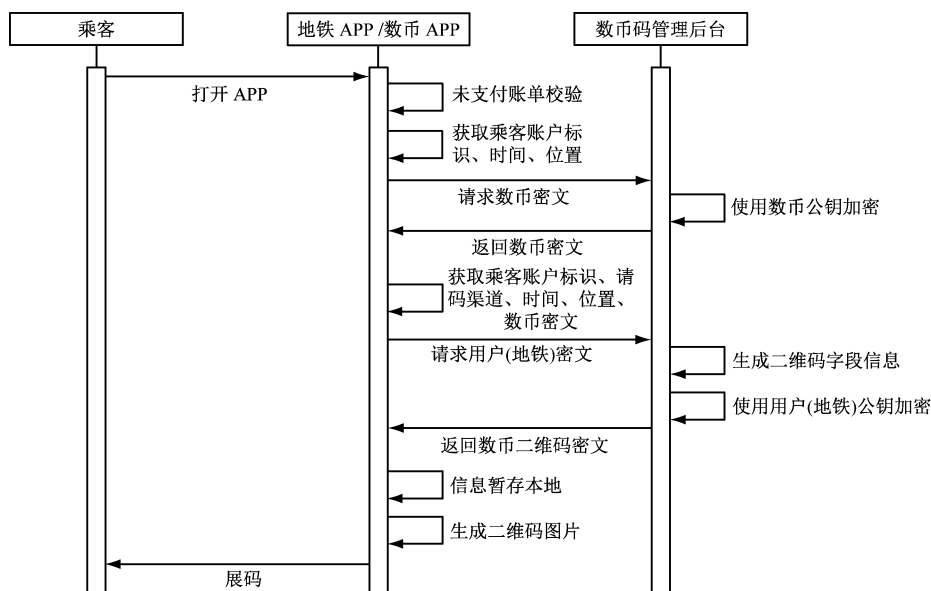


图 2 在线清码流程图

Fig. 2 Online code request flow chart

3.1.2 离线清码

离线清码读取最近一次在线清码时本地缓存的二维码字段信息,按与在线清码一样的规则生成完整乘车码。

APP 离线清码功能存在少量的票务风险,本文设计的离线清码流程,可按需使用。

为降低票务风险,应先设计本地缓存可用次数 N (例如 $N=5$) 及有效期 (例如 $2\sim 3\text{ h}$)。若 APP 在线时,在线清码;若 APP 离线时,当剩余请码次数 $N_s > 0$ 及在有效期内,则使用本地缓存的信息生成完整乘车码,而当 $N_s = 0$ 或超出有效期,则必须恢复在线清码。

离线清码步骤为:

步骤 1: 乘客打开手机 APP 中数币乘车二维码功能。

步骤 2: APP 自查是否封码,即是否存在未支付账单,若有则提醒乘客在线补款。

步骤 3: APP 自查手机是否离线;检查与数币码管理后台网络是否连接良好,若离线或网络不良,则进入离线清码模式。

步骤 4: APP 校验最近一次在线清码缓存的信息是否过期,判断剩余可用次数 N_s 是否有余值,若 $N_s = 0$ 或超出有效期,则必须恢复在线清码。

步骤 5: APP 打包乘客账户标志 (手机号)、时间、位置等数据,使用缓存的数币公钥进行加密。

步骤 6: APP 打包乘客账户标志、请码渠道、时间、位置、步骤 5 的数币密文等数据,生成二维码字段信息,使用缓存的地铁公钥进行加密。

步骤 7: APP 生成二维码图片,向乘客展码。

离线清码流程示意图见图 3 所示。

3.2 闸机验码

乘车码验证由闸机完成,校验通过后开闸放行,校验失败则提示乘客乘车码异常。

闸机验码步骤为:

步骤 1: 乘客打开手机 APP 展示数币二维码至闸机扫码。

步骤 2: 闸机对扫码的结果使用地铁私钥进行解密,解密出乘客账户标志、请码渠道、时间、位置、数币密文。

步骤 3: 闸机根据地铁编码规则对第 2 步解密数据进行数据验真、黑名单检查。若验真失败或在黑名单上,则提示乘客乘车码异常。

步骤 4: 闸机将此次交易数据上传至清分中心数币前置子系统,请求防重、单边、合法性在线验证;若闸机网络中断,则优先放行乘客,待网络恢复后再将数据重新上传。

步骤 5: 数币前置子系统进行防重、单边、合法性在线验证;若验证失败,则提示乘客乘车码异常。

步骤 6: 验证成功,数币前置子系统通知闸机开闸放行。

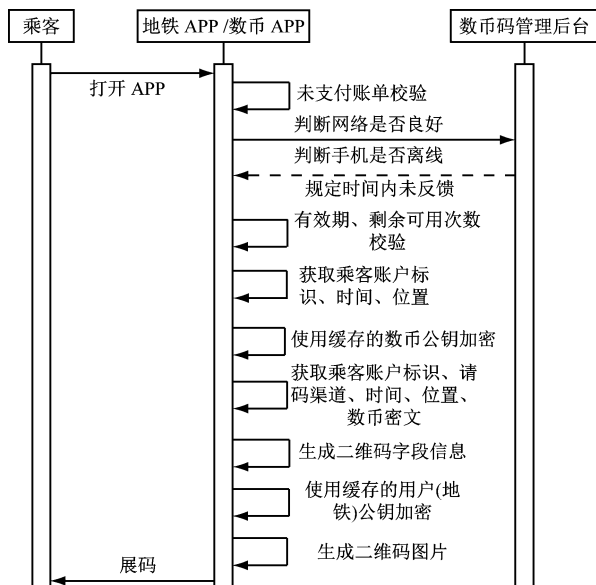


图 3 离线请码流程示意图

Fig. 3 Offline code request flowchart

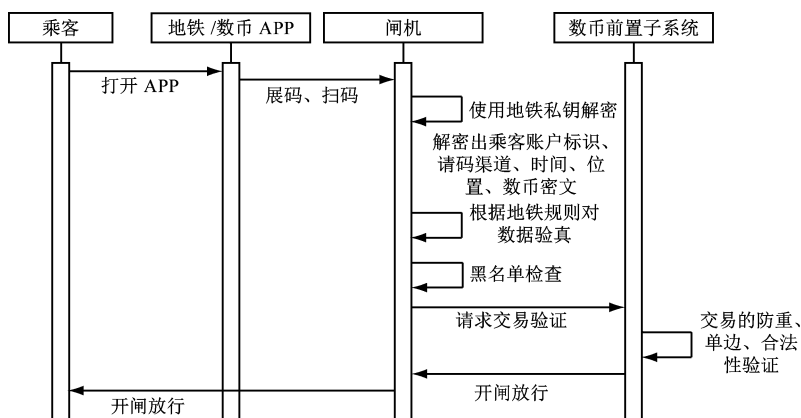


图 4 闸机验码流程示意图

Fig. 4 Gate code verification flowchart

录时,则搜索同样的进站交易记录进行交易匹配,并计算票价,将整个交易订单信息传至数币过闸支付模块请求支付扣款。

步骤 4: 数币过闸支付模块使用数币私钥对数币密文解密,并按数币编码规则进行数据验真;若验真失败则本交易结算异常,列入坏账。

步骤 5: 数币过闸支付模块向人民银行数币系统请求支付扣款。

步骤 6: 人民银行数币系统支付扣款,并反馈;若扣款失败,由数币过闸支付模块对乘客数币二维码进行封码,乘客补款完成后,再行解码。若离线操作多次并长时间不补款的乘客,可列入黑名单并封码,地铁与银行根据协议承担票款损失。

支付结算流程见图 5 所示。

闸机验证码流程示意图见图 4 所示。

3.3 信息通知

乘客扫码进/出站后,数币前置子系统将出行信息推送至数币过闸支付模块,该模块再将出行信息推送至数币 APP/地铁 APP,向乘客展示。

3.4 支付结算

支付结算负责完成交易对账、结算、扣款等工作。

支付结算步骤为:

步骤 1: 闸机将每笔数币交易记录数据,含乘客账户标志、时间、位置、进/出站点、票价及数币密文等,上传至 ACC 数币前置子系统。

步骤 2: 数币前置子系统经 CRC 码及 TAC 码防欺诈检查对上传交易进行合法防伪验证;若验证失败则本次交易异常,列入坏账。

步骤 3: 数币前置子系统每当收到出站交易记

4 结语

数字人民币作为法定货币,具有无限法偿性,势必要在城市轨道交通乘车场景推广使用。本文的研究采用数币软钱包,基于数币密钥及地铁密钥两个非对称密钥,参考交通部二维码编码格式,生成数币二维码。此方法是乘客及城市轨道交通行业最容易接受的应用模式。本文分析了应用于城市轨道交通场景下的数币支付系统整体架构、各模块功能,并详细阐述了 APP 请码、闸机验码验真、支付结算等关键业务流程。

数币乘车码基于法定数字货币而生,其在全国城市轨道交通推广具备天然的优势。扩展的,数币二维码通过行业地铁密钥可以应用于多城市多地

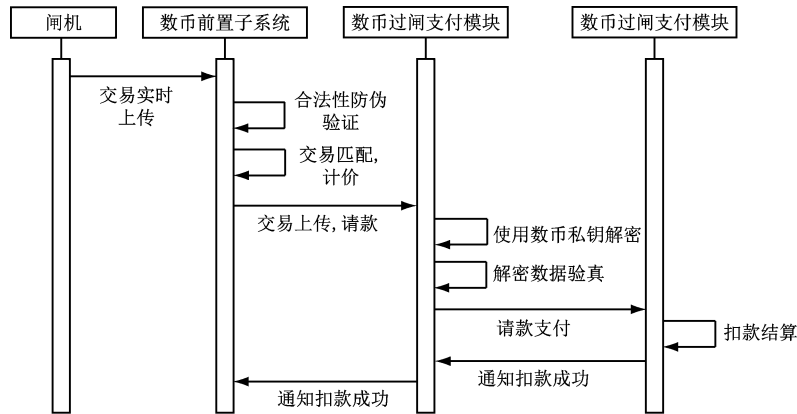


图5 支付结算流程示意图

Fig.5 Payment settlement flowchart

区,实现全国城市轨道交通“一票通”,进一步还可以定义其他行业密钥,如道路公交行业,以实现多行业的“一票通”,使数字货币二维码成为一张全国通的“万能票卡”。

参考文献

- [1] 朱嘉斌. 数字人民币在轨道交通中的应用实践[J]. 智慧城市轨道交通, 2023, 60(4): 73.
ZHU Jiabin. Application practice of digital currency electronic payment in rail transit [J]. Smart Rail Transit, 2023, 60(4): 73.
- [2] 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(4): 161.
ZHOU Shishuang, LIANG Jing, WANG Huan, et al. E-CNY application mode in urban rail transit[J]. Urban Rapid Rail Transit, 2022, 35(4): 161.
- [3] 李承志, 戚广杰, 方文玉. 一种结合数字人民币的城市轨道

交通票务支付系统: 2021110708187 [P]. 2021-12-10.

LI Chengzhi, QI Guangjie, FANG Wenyu. A rail transit ticketing payment system combining digital yuan: 2021110708187 [P]. 2021-12-10.

- [4] 李道全. 城市轨道交通自动售检票系统多元化支付研究与应用[J]. 都市快轨交通, 2019, 32(4): 126.
LI Daoquan. Research and application of diversified payment for automatic fare collection system in urban rail transit[J]. Urban Rapid Rail Transit, 2019, 32(4): 126.

· 收稿日期:2023-08-03 修回日期:2024-01-26 出版日期:2024-12-10
Received:2023-08-03 Revised:2024-01-26 Published:2024-12-10
· 第一作者:张森,正高级工程师,zhagnsen@dsjy.com
通信作者:于敏,高级工程师,yumin@ceprei.com
· ©《城市轨道交通研究》杂志社,开放获取 CC BY-NC-ND 协议
© Urban Mass Transit Magazine Press. This is an open access article under the CC BY-NC-ND license

(上接第 310 页)

- [2] 邓连波, 杨翊, 高勋, 等. 基于票价率偏差最小化的地铁分区票价优化方法[J]. 铁道科学与工程学报, 2017, 14(11): 2473.
DENG Lianbo, YANG Yi, GAO Xun, et al. Metro zonal fare optimization based on the minimum of fare rate deviation[J]. Journal of Railway Science and Engineering, 2017, 14(11): 2473.
- [3] 陈锋锋, 余子威, 杨岸磊. 轨道交通分区计时票制介绍[J]. 交通与运输, 2018, 34(5): 50.
CHEN Fengfeng, YU Ziwei, YANG Anlei. Introduction of time

ticket system in rail transit district[J]. Traffic & Transportation, 2018, 34(5): 50.

· 收稿日期:2023-09-28 修回日期:2024-01-09 出版日期:2024-12-10
Received:2023-09-28 Revised:2024-01-09 Published:2024-12-10
· 通信作者:李晓玉,高级工程师,lxy_90@yeah.net
· ©《城市轨道交通研究》杂志社,开放获取 CC BY-NC-ND 协议
© Urban Mass Transit Magazine Press. This is an open access article under the CC BY-NC-ND license