ICS 35.100.20
CCS R 80

团 体 标 准

T/CI 1152—2025

基于区块链的交通数据流通安全治理规范

Blockchain-based security governance specification for transportation data circulation

2025-08-25 发布 2025-08-25 实施

中国国际科技促进会 发 布

湖北科学技术出版社 出 版

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由南京理工大学提出。

本文件由中国国际科技促进会归口。

本文件起草单位：南京理工大学、郑州大学、内蒙古工业大学、重庆邮电大学、重庆钮维思网络科技有限公司、南昌大学、天津大学、云南民族大学、江苏省智能交通与车联网工程研究中心。

本文件主要起草人：戚湧、付守利、李雷孝、周由胜、杨宜平、余礼苏、许光全、潘文林、郝冠亚、李世雨、卫荣慕、林楠、刘媛妮、刘且根、刘健。

本文件为首次发布。

引　言

随着智能交通的发展，交通数据的安全性和隐私保护问题日益凸显，各级政府都提出加强对数据流通的监管和管理。为提升数据安全性、保障数据完整性、增强数据可追溯性、促进数据高效流通、建立信任机制以及符合政策与法规要求等方面要求，我们提出制定基于区块链的交通数据流通安全治理技术规范。该规范的制定将有助于交通行业更好地遵守相关政策和法规要求，降低法律风险并提升行业形象，为交通数字化的可持续发展提供强有力的支持。

本规范主要针对交通数据流通及安全进行规范和指导，旨在规范相关技术的使用，提高交通数据的使用效率，保障交通数据安全。本规范的使用对于保障交通系统的安全稳定运行、提升交通决策的科学性和准确性、促进交通数据资源的共享与利用、加强交通行业的监管与管理以及提升公众对交通系统的信任度等方面都具有重要意义。

基于区块链的交通数据流通安全治理规范

1 范围

本文件规定了基于区块链的交通数据流通参与方、流通过程及管理、安全治理的总体框架、安全治理的技术要求等。

本文件适用于交通数据管理、数据交互、数据监管等方面。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25058—2019 信息安全技术 网络安全等级保护实施指南

GB/T 25069—2022 信息安全技术 术语

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28452—2012 信息安全技术 应用软件系统通用安全技术要求

GB/T 36343—2018 信息技术 数据交易服务平台 交易数据描述

GB/T 42752—2023 区块链和分布式记账技术 参考架构

3 术语和定义

GB/T 25069—2022、GB/T 36343—2018 界定的以及下列术语和定义适用于本文件。

3.1

数据流通 data flows

桥数据从数据供方（提供方）按照一定的规则，通过特定的渠道或平台，传递给数据需方（需求方）的过程。

3.2

区块链 blockchain

在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

3.3

智能合约 smart contract

存储在分布式账本(3.10)中的计算机程序，是现实世界中合约和规则的算法实现。

注：智能合约的共识执行结果都记录在分布式账本中。

[来源：GB/T 42752—2023，3.13，有修改]

3.4

完整性 integrity

准确和完备的性质。

[来源：GB/T 25069—2022，3.612]

3.5

可用性 availability

数据可被授权实体访问并按需求使用的特性。即数据服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

[来源：GB/T 25069—2022 3.345]

4 缩略语

BT：区块链 blockchain technology

5 交通数据流通

5.1 交通数据流通参与方

5.1.1 数据源提供方

数据提供方应包括如下单位：

a) 政府部门：负责交通运输行业的监管和管理，拥有大量的交通基础设施、运营数据以及监管数据的单位，包含：交通运输部、省交通厅、地方交通运输局；

b) 交通运营企业：公路、铁路、航空、水运等日常运营中产生大量运营数据的运营企业（如高速公路运营公司、客货运平台公司、公交公司、地铁公司、航空公司、铁路公司）；

c) 智能交通系统管理及运营单位：通过智能交通信号控制系统、智能停车系统、车联网系统利用感知设备采集交通数据的单位。

5.1.2 数据处理与分析方

数据处理与分析方主要指提供数据处理、分析、挖掘等技术服务的数据技术服务商（如大数据公司、数据分析公司等）。

5.1.3 数据应用与服务提供方

数据应用与服务提供方包括：

a) 交通规划与设计单位：利用交通数据进行交通规划、设计、优化等工作的单位；
b) 出行服务平台：通过收集和分析用户出行数据，为用户提供更便捷的出行服务的平台；
c) 智慧城市与交通管理部门：通过整合和分析交通数据，提升城市交通管理水平和效率的智慧城市建设部门和交通管理的部门。

5.1.4 数据监管与保障方

数据监管与保障方包括：

a) 数据监管机构：负责数据流通的监管、保障交通数据安全、合规流通和使用的监管机构；
b) 数据安全服务商：为交通数据流通提供安全保护、隐私保护服务的企业。

5.1.5 其他参与方

其他参与方包括：

a) 公众与个体用户：公众和个体用户作为交通数据的最终使用者和服务对象通过出行服务平台、地图导航应用等方式获取和使用交通数据；
b) 行业协会与标准组织：制定交通数据流通相关标准和规范的行业协会和标准组织。

5.2 交通数据流通过程及管理

5.2.1 数据采集

交通数据的采集是数据流通过程的起点，主要通过多种设备和手段获取与交通运输相关的数据。这些数据包括静态数据和动态数据两大类：

a) 静态数据：指较长时间内保持不变的数据（如道路环境、车辆信息等）；
b) 动态数据：指在交通运行中产生的实时数据（如车辆的实时位置、速度、状态等）。这类数据主要通过 GPS 全球定位技术、手机信号、交通摄像头等设备进行实时监测和采集。

5.2.2 数据传输

对交通数据按一定的格式进行规范，以确保不同系统之间的数据能够正确传输和解析。

5.2.3 数据处理

收集到的原始数据须经过预处理、清洗和校准过程，以确保数据的准确性和一致性。处理过程包括：

a) 数据清洗：去除重复、错误或无效的数据；
b) 数据脱敏、脱密：对敏感和加密数据根据数据的特点和具体需求选择恰当的加密算法，如 AES、RSA 等，并确保算法的正确实施和密钥的安全管理。对敏感和加密数据，应用零知识证明技术，保证数据隐私的前提下进行数据的验证和交易；
c) 数据校准：对数据进行修正和调整，以提高数据的准确性；
d) 数据挖掘：对处理后的数据进行深入分析，以揭示交通运行的规律和趋势。

5.2.4 数据储存

经过处理后的交通数据需要按照一定的结构形式进行储存，以便后续的分析和使用。储存方式包括：

a) 结构化数据存储：可通过传统结构化数据库系统存储结构化数据；
b) 非结构化数据存储：可使用非关系型数据库（如：NoSQL）或分布式文件系统存放非结构化数据，也可以通过架构设计和系统集成的方式将分布式文件系统和非关系型数据库结合起来使用，通过在应用层面设计数据访问接口，使得用户可以根据需要选择使用分布式文件系统或非关系型数据库来访问和存储数据。

5.2.5 数据管理

数据管理涉及对交通数据的整体把控和维护，包括：

a） 数据备份和恢复：建立数据的备份和恢复机制，以防止数据丢失或损坏；
b） 数据安全：采取合理的数据脱敏和匿名化技术，确保个人信息不被滥用。加强数据传输和存储的加密措施，以防止数据泄露和篡改；
c） 数据授权与鉴权：针对数据安全需求和合规性要求，建立身份鉴别和数据访问控制机制，降低对数据的未授权访问风险。

5.2.6 数据应用

通过对交通数据进行分析和挖掘，可以应用于以下方面：

a） 交通规划：为交通规划提供依据，优化道路网络布局和交通设施配置；
b） 交通运营：提高交通运行效率，减少拥堵和事故；
c） 交通安全：加强交通安全监管，预防交通事故的发生；
d） 商业化应用：为出行服务平台、停车服务平台、网络货运平台等提供数据支持，推动交通行业的商业化发展。

5.2.7 数据销毁

对于过期的交通数据需要采用安全数据销毁流程进行销毁，具体如下：

a) 根据数据的敏感程度和用途进行分类，明确需要销毁的数据范围和存储位置；
b) 建立数据销毁的审批流程，确保销毁操作符合要求；详细记录销毁操作的时间、内容、责任人等信息；定期对数据销毁流程进行监督和审计，确保操作规范；
c) 使用专业的数据销毁工具，确保数据被彻底删除且无法恢复。

6 交通数据流通安全风险防范

6.1 数据泄露防范

本项要求包括：

a) 符合数据安全管理的目标、原则、责任和流程，为数据安全管理提供制度保障，包括但不限于GB/T 22239—2019、GB/T 25070—2019、GB/T 25058—2019；

b) 建立数据安全管理体系,包括完善的组织结构、规范的管理流程、科学的技术手段以及完善的安全管理制度，确保数据的全生命周期（采集、传输、存储、处理、使用等）都得到有效的管理和控制；
c) 对重要、敏感数据采用国密（SM2 或 SM9 非对称加密算法）进行加密处理，确保数据在传输、存储和处理过程中不被窃取或篡改；
d) 建立健全权限管理制度，确保数据的访问和使用受到严格控制。采取分级管理和分级授权的原则，对数据的权限进行精细化管理；
e) 结合隐私计算技术可以实现数据的所有权、使用权分离，交互双方无须传输原始数据，而是通过隐私计算平台完成数据需求，以输出计算结果的形式完成信息交互；
f) 建立网络安全管理制度，加强网络风险监测和评估，采取有效措施防范网络攻击；
g) 定期对数据的使用情况进行审计和检查，发现异常行为及时处理和纠正，确保数据使用的合法性和规范性。

6.2 数据篡改防范

本项要求包括：

a) 利用区块链技术将数据分散存储在多个节点上，而非传统的中心化服务器。这种分布式存储方式避免了单点故障和数据集中泄露的风险，即使部分节点受到攻击，数据也不会完全丢失或篡改；
b) 区块链上的数据具有不可篡改的特性，可以通过此特性追溯到数据的原始状态和变化过程，有助于在数据发生问题时迅速定位原因并采取措施；
c) 利用区块链智能合约自动执行预设的规则和条件,确保数据的处理过程符合既定的规范和标准，防止人为因素对数据的篡改；
d) 为政府监管机构预留监管接口，以便对区块链上的数据交易和处理过程进行实时监管和审计，确保数据的合法性和规范性。

6.3 数据不一致风险防范

6.3.1 加强数据质量管理

本项要求包括：

a) 制订数据质量标准，明确交通数据的采集、处理、存储、传输等各个环节的数据质量标准，含数据格式、精度、完整性等要求；
b) 在数据流通前，对数据进行清洗和校验，去除重复、错误、无效的数据，确保数据的准确性和一致性；
c) 建立数据溯源机制，记录数据的来源、修改历史等信息，以便在数据不一致时能够快速定位问题源头并进行修复。

6.3.2 采用加密与区块链技术进行防范

本项要求包括：

a) 利用区块链技术确保数据在流通过程中的完整性和可用性,并为数据提供可追溯且防篡改功能；

区块链应用应按照 GB/T 20271—2006 中 6.2.2.3 以及 GB/T 28452—2012 中 6.1.4 的要求；

b) 在数据传输和存储过程中采用加密技术，确保数据的安全性；

c) 通过智能合约自动执行数据流通中的规则和条件，减少人为干预和错误，提高数据流通的效率和准确性。

6.3.3 完善数据流通机制

本项要求包括：

a) 搭建统一的数据共享平台，实现交通数据在不同部门、不同机构之间的共享和交换。平台应具备数据清洗、校验、转换等功能，以确保数据的一致性和可用性；

b) 制订明确的数据流通规则，包括数据的流通范围、使用权限、更新频率等要求。各参与方应遵守规则，确保数据流通的有序进行；

c) 建立数据流通的监管和审计机制，对数据的流通过程进行实时监控和审计。发现数据不一致问题时，及时采取措施进行修复。

6.3.4 建立应急响应机制

本项要求包括：

a) 针对可能发生的数据不一致问题，制订详细的应急预案。预案应包括问题发现、报告、处理、修复等各个环节的流程和措施；

b) 组建专门的应急团队，负责处理数据不一致等突发事件。团队成员应具备丰富的经验和技能，能够迅速响应并有效解决问题。

6.4 完整性和可恢复性

本项要求包括：

a) 对交通数据进行定期备份，确保数据的完整性和可恢复性。应按照 GB/T 20271—2006 中 6.2.2.5 以及 GB/T 28452—2012 中 6.1.6 的要求，对交通数据进行备份；

b) 定期对交通数据进行定期备份，确保数据的完整性和可恢复性。应按照 GB/T 20271—2006 中 6.2.2.5 以及 GB/T 28452—2012 中 6.1.6 的要求，对交通数据进行备份。

7 基于区块链的交通数据流通安全治理框架

7.1 区块链技术在交通数据流通中的应用

本项要求包括：

a) 通过区块链的分布式账本技术，可以确保交通数据的透明性和不可篡改性，从而增强数据的可信度；

b) 通过智能合约自动执行预设的规则和协议，减少人为干预和错误；

c) 利用区块链的去中心化特性，实现数据的分布式存储、验证和传输，防止单点故障，提高系统的鲁棒性和安全性。

7.2 交通数据流通安全治理原则

交通数据流通安全治理应遵循以下原则：

a） 数据隐私保护：确保个人和车辆数据在传输和存储过程中受到保护，防止未经授权的访问；

b） 数据完整性：确保数据在传输和存储过程中不被篡改；

c） 数据可追溯性：通过区块链技术，实现数据流通的全程可追溯，确保数据来源可验证；

d） 系统可靠性：确保系统在高流量和恶意攻击下仍能稳定运行；

e） 合规性：遵守相关法律法规和行业标准，确保数据流通符合要求。

7.3 交通数据流通安全治理架构

7.3.1 基于区块链的交通数据量安全治理架构如图 1 所示：

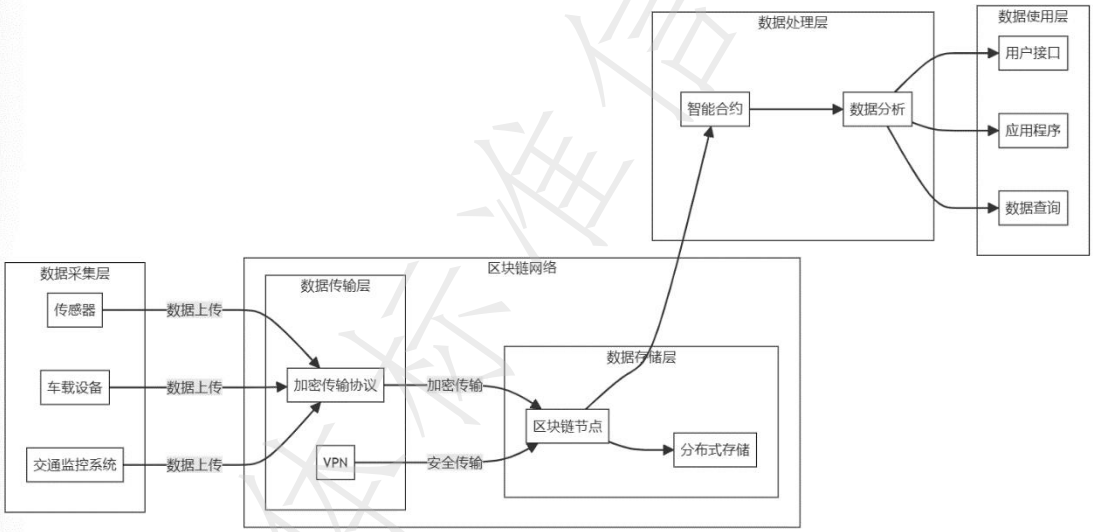

图 1 基于区块链的交通数据量安全治理架构

7.3.2 交通数据流通安全治理架构应包括以下几个关键组件：

a）数据采集层

1）传感器

在道路、路口及固定设施上安装各类传感器，用于实时采集车流量、车速、环境温度等交通相关数据；配置定期校验机制，保证采集数据的准确性。

2）车载设备

利用车辆内置 GPS、OBD 等设备收集行驶轨迹、车辆状态、油耗等数据。实现数据本地缓存和批量上传，确保在网络条件较差时数据不丢失。

3）交通监控系统

部署摄像头、雷达与其他视频监控设备，实时捕捉交通异常、事故及违章行为。对视频以及图像数据进行预处理，转化为结构化信息以便后续分析。

b）区块链网络层

1）数据传输层

利用 TLS/SSL 等加密通信协议确保数据在传输过程中不被窃取或篡改。通过建立 VPN 隧道，为数据传输提供更高的安全保障。

2）数据存储与验证层

使用区块链技术对采集到的数据进行记录，确保数据的防篡改性和全程可追溯性；利用各区块链节点共同维护分布式账本，通过共识机制对数据进行验证；数据在各节点间进行分布式存储备份，防止单点故障及数据丢失风险。

3）智能合约

部署自动化智能合约，实现数据共享权限、访问控制及自动预警机制；预设合约规则，以便在数据传输、存储和后续处理过程中自动执行合规性检查。

c）数据处理层

1）数据分析

基于区块链存储的数据进行深度挖掘、统计分析，生成具有价值的信息和趋势报告；综合大数据分析与人工智能算法，提升对交通拥堵、事故预警及资源调配的响应速度。

2）智能合约驱动数据处理

通过智能合约自动处理数据的验证、共享及审批流程，确保业务逻辑符合预先设置的安全策略；实现多方数据交互时的自动权限控制和数据完整性检查。

d）数据使用层

1）用户接口

提供直观易用的用户界面（支持 Web 端和移动端），便于管理人员及广大用户实时查询和监控交通数据；根据用户角色分配不同的数据访问权限，确保数据仅在授权范围内进行查看与操作；

2）应用程序

开发多种基于交通数据的应用，如导航优化、交通预测、事故预警以及智能调度系统；提供接口与第三方系统对接，实现数据与其他平台的互联互通；

3）数据查询

提供高度安全的数据检索功能，利用区块链的不可篡改特性确保查询结果的真实性与准确性；支持历史数据的追溯与下载，以便进行二次数据处理或跨平台数据共享。

8 交通数据流通安全治理技术要求

8.1 数据采集环节

8.1.1 数据采集安全要求

本项要求包括：

a) 数据加密：确保采集到的数据在传输至区块链网络之前进行加密；

b) 身份认证：对数据采集设备进行身份认证，防止伪造设备上传虚假数据；

c) 数据完整性校验：在数据采集过程中进行完整性校验，确保数据未被篡改。

8.1.2 数据采集技术方案

本项要求包括：

a) 使用加密传感器：采用支持数据加密的传感器和车载设备；
b) 多因素认证：结合硬件和软件多因素认证技术，确保采集设备的合法性；
c) 数据校验算法：使用哈希算法对采集数据进行完整性校验。

8.2 数据传输环节

8.2.1 数据传输安全要求

本项要求包括：

a) 加密传输：使用安全的通信协议（如 TLS/SSL）加密数据传输；
b) 安全通道：建立虚拟专用网络（VPN）或其他安全通道，防止数据在传输过程中被截获；
c) 传输日志记录：对数据传输过程进行日志记录，确保数据传输的可追溯性。

8.2.2 数据传输技术方案

本项要求包括：

a) TLS/SSL 协议：采用 TLS/SSL 等加密协议，确保数据在传输过程中的安全性；
b) VPN 技术：使用 VPN 技术建立安全的数据传输通道；
c) 传输日志系统：建立完善的传输日志系统，记录数据传输的每个环节。

8.3 数据存储环节

8.3.1 数据存储安全要求

本项要求包括：

a) 数据加密存储：所有数据在存储前进行加密处理；
b) 访问控制：严格控制数据访问权限，确保只有授权人员和系统可以访问数据；
c) 数据备份：定期备份数据，防止数据丢失。

8.3.2 数据存储技术方案

本项要求包括：

a) 区块链存储：利用区块链技术存储数据，确保数据的不可篡改性和可追溯性；
b) 加密技术：采用高级加密标准（AES）对数据进行加密存储；
c) 访问控制系统：使用基于角色的访问控制（RBAC）系统，管理数据访问权限。

8.4 数据使用环节

8.4.1 数据使用安全要求

本项要求包括：

a) 数据脱敏：在使用数据时，进行数据脱敏处理，保护个人隐私；

b) 使用审计：对数据使用过程进行审计，记录数据使用情况；
c) 权限管理：严格管理数据使用权限，防止数据被滥用。

8.4.2 数据使用技术方案

本项要求包括：
a) 数据脱敏工具：使用专门的数据脱敏工具，确保数据使用过程中的隐私保护；
b) 审计系统：建立数据使用审计系统，记录和监控数据使用行为；
c) 权限管理系统：使用权限管理系统，管理和分配数据使用权限。

8.5 数据区块链管理环节

8.5.1 区块链技术安全要求

本项要求包括：
a) 共识机制安全性：选择安全且高效的共识机制（如 PoW、PoS）以确保网络的安全性和数据的有效性；
b) 智能合约安全性：对智能合约进行审计，确保其逻辑正确且不易受到攻击；
c) 节点认证：对参与区块链网络的节点进行严格的身份认证，防止恶意节点的加入。

8.5.2 区块链技术方案

本项要求包括：
a）选择合适的区块链平台：根据需求选择合适的区块链平台（如 Ethereum、Hyperledger 等），以支持特定的应用场景；
b）多链架构：考虑采用多链架构以提高数据处理能力和灵活性，确保不同数据源的有效整合；
c）链上数据加密：实施链上数据加密措施，确保存储在区块链上的数据在任何情况下都能保持机密性和完整性。

8.5.3 区块链可追溯性要求

本项要求包括：
a）数据追溯机制：建立完善的数据追溯机制，确保每一笔交易和数据变更都可以被追踪和审计；
b）时间戳功能：利用区块链的时间戳功能记录数据采集、传输、存储和使用的时间，确保数据的时效性和可靠性；
c）透明度要求：确保区块链网络的透明度，允许授权用户随时检查数据的流通和使用情况。通过增加这些区块链技术的具体要求，可以进一步增强交通数据流通的安全治理。

9 交通数据流通安全治理运营管理

9.1 角色与责任划分

本项要求应包括如下人员：

a) 数据管理员：负责数据的采集、存储和管理工作；
b) 安全管理员：负责系统的安全策略制定和实施，确保数据安全；
c) 合规管理员：确保数据流通和使用符合相关法律法规和行业标准。

9.2 安全监控与审计

本项要求包括：

a) 安全监控系统：建立实时安全监控系统，监控数据流通中的安全事件；
b) 定期审计：定期对系统进行安全审计，发现和解决潜在的安全问题；
c) 日志管理：对所有操作和事件进行详细记录，确保系统的可追溯性。

9.3 应急响应与恢复

本项要求包括：

a) 应急预案：制订详细的应急预案，快速响应和处理突发安全事件；
b) 应急演练：定期进行应急演练，确保各部门熟悉应急预案；
c) 数据恢复：建立数据备份和恢复机制，确保在发生数据丢失时能够快速恢复。

10 交通数据流通安全治理测试与评估

10.1 交通数据流通安全治理的测试方法

10.1.1 功能测试

目的：验证系统各个功能模块是否按设计要求正常工作。
方法：编写测试用例，模拟各种正常和异常操作，检查系统的响应和处理情况。
内容：数据采集、传输、存储和使用等各个环节的功能测试。

10.1.2 安全测试

目的：检测系统的安全性，发现潜在的安全漏洞和威胁。
方法：使用渗透测试工具和技术，模拟攻击者的行为，对系统进行全面的安全测试。
内容：身份认证、数据加密、权限管理、日志记录等方面的安全测试。

10.1.3 性能测试

目的：评估系统在高负载情况下的性能表现，确保系统的稳定性和响应速度。
方法：使用性能测试工具，模拟大量数据和并发请求，观察系统的处理能力和响应时间。
内容：数据采集频率、数据传输速度、区块链写入速度、数据查询响应时间等。

10.1.4 兼容性测试

目的：确保系统在不同环境和设备上的兼容性。

方法：在不同操作系统、浏览器和硬件设备上进行测试，检查系统的兼容性和稳定性。

内容：各种操作系统、浏览器版本、移动设备等的兼容性测试。

10.1.5 用户测试

目的：收集用户反馈，改进系统的用户体验和易用性。

方法：邀请实际用户参与测试，记录和分析用户的操作行为和反馈意见。

内容：用户界面、操作流程、功能易用性等方面的测试。

10.2 评估指标

在对交通数据流通安全治理系统进行评估时，需要定义一系列评估指标，以量化系统的安全性和性能表现。这些评估指标包括但不限于：

a) 安全性指标

1) 身份认证成功率：系统正确识别合法用户的比例；
2) 数据加密成功率：数据在传输和存储过程中加密的成功率；
3) 权限管理有效性：权限控制是否能有效防止未经授权的访问；
4) 安全漏洞数量：系统中存在的安全漏洞数量和严重程度；
5) 安全事件响应时间：系统对安全事件的检测和响应时间。

b) 性能指标

1) 数据采集频率：系统能够支持的最大数据采集频率；
2) 数据传输速度：数据从采集点到区块链网络的传输速度；
3) 区块链写入速度：数据写入区块链的速度和延迟；
4) 数据查询响应时间：用户查询数据时系统的响应时间；
5) 系统吞吐量：系统在高负载情况下的处理能力。

c) 可靠性指标

1) 系统可用性：系统在一定时间内无故障运行的时间比例；
2) 故障恢复时间：系统在发生故障后的恢复时间；
3) 数据恢复成功率：系统在故障后数据恢复的成功率。

d) 用户体验指标

1) 用户满意度：用户对系统的整体满意度评分；
2) 操作便捷性：用户完成特定任务所需的操作步骤和时间；
3) 界面友好度：用户对系统界面的美观性和易用性的评价。

团 体 标 准

基于区块链的交通数据流通安全治理规范

T/CI 1152—2025

*

湖北科学技术出版社出版发行

武汉市雄楚大街268号湖北出版文化城B座

13—14座 (430070)

总编室:（027）87679429

湖北新华印务有限公司印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 1.125 字数 9 千字

2025年9月第一版 2025年9月第一次印刷

书号: 155706 · 151 定价：53元

6 977819 691504