ICS°35.080
L77

团　体　标　准

T/JSHLW ###-####

基于区块链的车联网数据应用技术规范

Technical Specification for Data Application of Internet of Vehicles Based on Blockchain

（征求意见稿）

####-##-## 发布　　####-##-## 实施

江苏省互联网协会 发布

目　录

前　　言

本标准依据 GB/T 1.1-2009《标准化工作导则》给出的规则起草。

本标准由江苏省互联网协会提出并归口。

本标准起草单位：南京理工大学，江苏源驰科技有限公司，江苏智城慧宁交通科技有限公司，华设设计集团股份有限公司，连云港杰瑞电子有限公司，斯润天朗（无锡）科技有限公司

本标准主要起草人：戚湧、赵学龙、朱世龙、刁含楼、何流、谢豪、章涛涛、邹奕润、郝冠亚、高宁波、万剑、谢家阳。

1 范围

本标准基于区块链技术架构描述了车联网数据应用技术架构，本标准规定了基于区块链的车联网数据应用技术的术语和定义、系统框架和一般要求等内容。

本标准为实现基于区块链的车联网数据应用平台提供参考。

本标准适用于车联网产业的数据应用开发、运营和使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的应用文件，仅注日期的版本适用于本文件，凡是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。

YD/T 3746-2020 车联网信息服务 用户个人信息保护

GM/T 0111-2021 区块链密码应用技术要求

GB/T 37973-2019 信息安全技术 大数据安全管理指南

T/CESA 6001-2016区块链 参考架构

GM/T 0024-2014 SSL VPN 技术规范

T/CESA 1050-2018 区块链智能合约实施规范

3 术语和定义

下列术语和定义适用本文件。

3.1

区块链 Blockchain

区块链技术是运用块链式数据结构存储数据、运用共识机制更新数据、运用智能合约操作数据的一种分布式系统架构。

3.2

共识机制 Consensus Mechanism

共识机制是区块链系统中为实现不同节点之间建立信任、获取权益采用的数学算法。

3.3

智能合约 Smart Contract

智能合约是一种用计算机语言取代法律语言记录条款的合约。

3.4

数字签名 Digital Signature

数字签名是签名者使用私钥对签名数据的杂凑值做密码运算后的结果，该结果只能用签名者的公钥进行验证，是对信息发送者发送信息真实性、完整性的有效证明。

3.5

车联网 Internet of Vehicles

车联网是指车辆上的车载设备通过无线通信技术，对信息网络平台中的所有车辆动态信息进行有效利用，在车辆运行中提供不同的功能服务。

3.6

数据脱敏 Data Desensitization

数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

3.7

对等网络 Peer to Peer

对等网络，即对等计算机网络，是一种在对等者之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。

3.8

交易 Transaction

交易是指对智能合约的一次调用。

3.9

默克尔树 Merkle Tree

默克尔树（Merkle 树）又叫哈希树，是区块链数据存储运用到的一个重要的技术算法。

3.10

对称加密 Symmetrical Encryption

对称加密是一种密码加密方法，采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密。

3.11

时间戳 Timestamp

时间戳是使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。

3.12

联盟链 Alliance Chain

联盟链，只针对某个特定群体的成员和有限的第三方，其内部指定多个预选节点为记账人，每个块的生成由所有的预选节点共同决定。

3.13

无线电接入技术 Radio Access Technology

无线电接入技术是用于一个基于无线电的通信网络的基础物理连接方法。

3.14

专用短程通信技术 Dedicated Short Range Communications

专用短程通信技术是一种新型的技术，专门用于机动车辆在高速公路等收费点实现不停车自动收费 ETC 技术。

3.15

高级加密标准 Advanced Encryption Standard

高级加密标准是美国联邦政府采用的一种区块加密标准。

3.16

安全套接字层 Secure Socket Layer

安全套接字层是在传输通信协议上实现的一种安全协议，采用公开密钥技术。

3.17

传输层安全 Transport Layer Security

传输层安全其新继任者安全套接层在互联网上提供保密安全信道的加密协议，为诸如网站、电子邮件、网上传真等等数据传输进行保密。

3.18

证书管理机构 Certification Authority

证书管理机构是认证机构的国际通称，它是对数字证书的申请者发放、管理、取消数字证书的机构。证书管理机构的作用是检查证书持有者身份的合法性，并签发证书（用数学方法在证书上签字），以防证书被伪造或篡改。

4 缩略语

下列缩略语适用于本文件：

RAT	无线电接入技术（Radio Access Technology）
DSRC	专用短程通信技术（Dedicated Short Range Communications）
AES	高级加密标准（Advanced Encryption Standard）
SSL	安全套接字层（Secure Socket Layer）
TLS	传输层安全（Transport Layer Security）
CA	证书管理机构（Certification Authority）

5 车联网数据分类类型要求

基于区块链的车联网数据应用技术中，对于采集的数据应进行数据类型分类和数据敏感性等级划分。

5.1 数据类型分类

基于区块链的车联网数据应用技术数据应按照数据主题进行分类，可分为六大类：基础属性类数据、车辆工控类数据、环境感知类数据、车控类数据、用户个人信息和应用服务类数据。

5.1.1 基础属性类数据

基础属性类数据应是车辆基础属性数据，即与车辆的某些特性相关的数据，包括但不限于车牌号、发动机号、车联网移动终端应用软件的开发商等相关数据。

5.1.2 车辆工况类数据

车辆工况数据指与车辆实际运行特征或车辆实际操作系统有关的数据，包括但不限于动力系统、底盘系统、车身系统等相关运行状态、系统工作参数，以及整车控制器等相关的工况数据。

5.1.3 环境感知类数据

环境感知类数据主要是与车辆所处外部环境相关的数据，包括车联网信息服务中与车辆进行通信或交互的外部设备、终端、行人等相关的数据，包括但不局限于车辆位置、车辆速度、红绿灯信息、行人位置、视频图像等相关数据。

5.1.4 车控类数据

车控类数据指车联网信息服务中对车辆操控直接相关的指令数据，包含对车辆的智能控制行为数据、对车辆实施远程操作以及远程诊断等指令数据。

5.1.5 用户个人信息

用户个人信息是用户基本信息和区块链中用于身份识别的数字证书。用户基本信息应遵循 YD/T 3746-2020 的规定。

5.1.6 应用服务类数据

应用服务类数据指除了基础属性类属性、车辆工况类数据、环境感知类数据、车控类数据和用户个人信息之外，还包括与车联网信息服务相关的数据，如交通安全管控数据、涉及车辆服务如车辆维护、金融保险等。

5.2 数据敏感性等级划分

车联网数据应根据车联网数据的安全目标和重要性等对数据进行敏感性分级，应分为一般数据、重要数据和敏感数据。根据敏感性分级提供不同等级的安全保护。

a） 一般数据应为车联网服务中，能公开获取或能在一定范围内公开的数据，此类数据泄露造成的影响范围与程度有限，不会对财产和人身安全构成危害。包括但不限于车辆的车牌号、道路情况等。

b） 重要数据指车联网各节点间进行信息交互时的数据，此类数据能标识到车联网信息服务的主体、对象或其重要特征，此类数据泄露将对一定范围内影响经济效益或造成财产损失，或对人身和财产安全造成较大影响。包括但不限于车辆行驶信息，发

动机号等。

c） 敏感数据指能标识车联网节点的敏感数据，关系用户个人隐私，此类数据泄露将造成严重后果。包括但不限于车辆核心数据、车辆驾驶员身体健康状况、出行路线等。

6 基于区块链的车联网数据应用技术的基本要求

6.1 车联网数据共享能力要求

对于车联网数据共享能力应满足以下要求：

a） 基于区块链的车联网数据应用技术应采用联盟链的形式，对不同敏感性等级的数据进行不同访问权限设置。

b） 对于一般数据，应支持大范围内所有主体进行访问。对于重要数据，应支持基于区块链的车联网数据应用技术范围内合法节点进行访问，且要求访问时需要进行授权和身份验证。对于敏感数据，应根据 YD/T 3746-2020 的相关要求实施安全保护。

6.2 车联网数据应用基本要求

车联网系统架构可分为六个层次，包括应用层、处理层、控制管理层、通信层、预处理层和感知层。车联网系统架构如图 1 所示。

感知层即数据采集层，即通过相关设备如智能设备、路侧基础设施等实体采集信息。

预处理层主要是对感知层收集的数据进行过滤和预处理。

通信层含有 RAT、DSRC 等多种类型的通信技术，数据可以在服务器的控制下进行交换和传输。

控制管理层主要是车联网的网络服务管理者。如交通处理系统，授权/认证系统等。

处理层提供存储及服务、网络即服务等多种服务，负责处理从车辆节点接收的有关交通状况、交通安全等相关的所有数据，对数据进行处理和分析。

应用层主要包含企业与政府机构，如交通管理部门，用于未来基础设施的开发等服务。

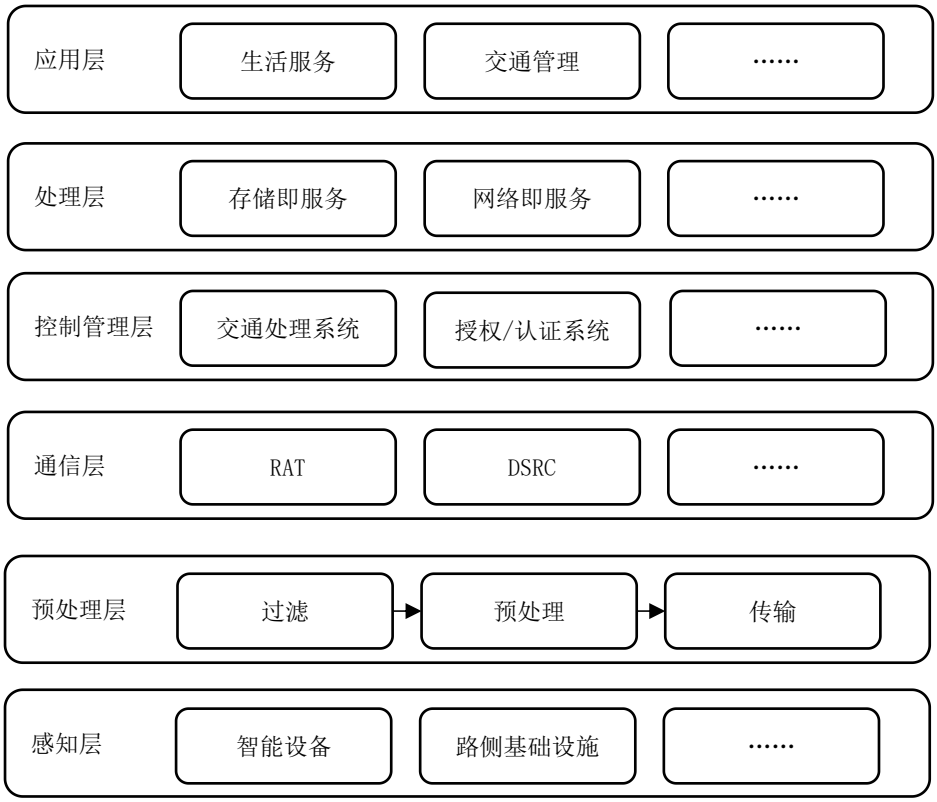

图 1 车联网系统架构

基于区块链的车联网数据应用技术应用架构包括数据采集、数据传输、数据共享和数据传输等子模块。基于区块链的车联网数据应用技术应用架构如图 2 所示。相应的模块应满足相应的要求。

图 2 基于区块链的车联网数据应用技术应用架构

6.2.1 数据采集

基于区块链的车联网数据应用技术中需要利用相关设备采集道路和车辆的相关数据。数据采集过程中应满足以下要求：

a) 采集的数据应根据不同的应用场景符合相应的数据要求。
b) 可采取路况分析、实时仿真、交通量预测等分析技术，对采集的数据进一步提取。
c) 信息上传者将自己的身份信息等提交给认证中心用于产生数字证书。
d) 系统应验证数字证书的有效性，确保信息上传者身份合法，保证信息上传后可溯源。
e) 应对采集的数据进行分类和敏感性分级。
f) 应根据技术成熟度、安全性等要求对数据进行脱敏，实现节点敏感隐私数据的可靠保护。

6.2.2 数据传输

数据传输应满足以下要求：

a） 应能够检测数据在传输过程中的完整性，包括节点身份信息、车辆采集的数据等，并能在数据遭到破坏时采取必要措施恢复或重新获取数据。

b） 应利用共识机制和智能合约，验证信息的有效性和合法性，防止恶意上传无效信息，保证数据质量。

c） 节点在传输数据时应满足数据格式要求、样本质量要求、以及脱敏要求、性能要求。

d） 数据传输时采用符合国家密码标准的 SSL/TLS 协议安全产品，应符合 GM/T 0024-2014 的相关要求，保证数据的保密性。

6.2.3 数据存储

数据形成区块存储到区块链上时，应满足以下存储要求：

a） 每个区块应包含区块头和区块体两部分，区块结构应符合 T/CESA 6001-2016 相关要求。

b） 应采用安全的加密算法加密数据，采用的加密技术应符合 GM/T 0111-2021 的相关要求。

c） 应利用合适的共识机制保证数据的完整性，保障存储的数据不被篡改。

d） 应对存储的数据进行定期备份或提供多副本备份机制。备份数据应与原数据具有相同的访问控制权限和安全存储要求。

e） 数据的管理应符合 GB/T 37973-2019 的相关要求。

6.2.4 数据共享

数据上传后，可供节点和用户访问，在节点或用户访问链上数据时，应满足以下要求：

a） 利用合适的区块链的加密算法、访问控制策略进行访问控制，对不同敏感性等级设置相应的访问权限。

b） 应对访问节点进行身份识别，节点需要获得 CA 颁发的证书，证书经过区块链网络验证后才能进行相关的操作。身份识别和授权应采用 CA 认证中心和数字证书机制。

c） 应采用车联网设备动态准入认证的方式来登记管理设备，应结合区块链的共识机制实现设备上线自动发现，设备入网自动完成认证，设备状态（维修、更换）自动监测等功能。

d） 节点对链上数据的访问操作应做到有记录、可溯源。

e） 数据共享中应做好数据备份和恢复等相关工作。

f） 数据安全共享应依托区块链共识机制开展应用。

6.3 数据脱敏要求

数据上传和传输时，应对数据进行数据脱敏，实现敏感数据保护。数据脱敏满足以下要求：

a） 数据脱敏前后应保持数据特征。

b） 数据格式上，设备应支持原始二进制数据进行脱敏，对于完成脱敏后上传的数据，应支持范围内输入视频和图像格式的解码。

c） 对脱敏后的数据应进行评估，确保经车端数据处理设备脱敏后的数据达到规定标准。

7 基于区块链的车联网数据应用技术相关安全要求

基于区块链的车联网数据应用技术应满足如下要求：

a） 基于区块链的车联网数据应用技术的使用的密码算法和技术应符合 GM/T 0111-2021 的相关要求。

b） 部署智能合约时，应检查用户是否获得相应的权限，并对用户上传的智能合约进行基础安全检测。同时应采用密码技术防止智能合约被篡改。智能合约的实施应遵循 T/CESA 1050-2018 相应的规范要求。

c） 对链上重要数据以及敏感数据进行操作时，应进行审计，并形成审计日记。

d） 对于敏感数据的使用，应支持数据使用过程中的动态脱敏。

e） 对于数据的备份应提供身份认证等安全认证措施，确保仅授权用户知情或控制下才能执行相应数据备份的操作。

f） 数据共享前应进行网络安全能力评估，保证数据共享的安全实施。