ICS°35.080
L77

团　体　标　准

T/JSHLW ###-####

基于区块链的车联网节点信任管理规范

Trust Management Specification for Internet of Vehicles Nodes 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

本标准按照GB/T 1.1-2009《标准化工作导则》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，南京凌岳区块链科技有限公司，江苏智城慧宁交通科技有限公司。

本标准主要起草人:戚湧、赵学龙、陆治国、郝冠亚、徐志荣、高宁波。

区块链的车联网节点信任管理规范

1 范围

本标准基于区块链技术架构以及车联网的特点，描述了一种基于区块链的车联网节点信任管理系统，规定了管理系统中的术语定义、体系框架和一般技术要求。

本标准适用于区块链平台和应用中车联网节点信任管理系统的设计、实现和使用。

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。凡是注日期的引用文件，仅所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。

GB/T 20271-2016　信息安全技术 信息系统安全通用技术要求

T/JSIA 0002—2020　区块链基础技术规范

T/CESA 6002—2017　区块链数据格式规范

T/SIA 007-2018　区块链平台基础技术要求。

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用本文件。

3.1.1

分布式账本 Distributed Ledger

分布式账本是一种在网络成员之间共享、复制和同步的数据库。分布式账本记录网络参与者之间的数据交换信息。

3.1.2

数字签名 Digital Signature

数字签名是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

3.1.3

区块链 Blockchain

区块链是一种对等网络环境下以块链式存储结构实现数据存储、共享、验证、计算等功能的多方共同维护的分布式账本技术。

3.1.4

智能合约 Smart Contract

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。

3.1.5

时间戳 Timestamp

时间戳是用于标识信息时间的字符序列，具备唯一性，时间戳用以记录并表明存在的、完整的、可验证的数据，是每一次信息记录的认证。

3.1.6

共识机制 Consensus Mechanism

共识机制是在一个时间段内对事物的前后顺序达成共识的一种算法。常用的共识算法包括：工作量证明机制、权益证明机制、拜占庭共识算法等。

3.1.7

安全通道 Secure Channel

安全通道是建立在通信端之间的安全通信通道，使用密码算法和安全协议以保证传输数据的机密性和完整性。

3.1.8

同态加密 Homomorphic Encryption

同态加密是一种特殊的加密方法，允许对密文根据特定的代数运算方式进行处理后得到的仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果是一样的。

3.1.9

节点 Node

节点是区块链分布式系统中的网络节点，是通过网络连接的服务器、计算机、电话等，针对不同性质的区块链，成为节点的方式也会有所不同。

3.2 缩略语

以下缩略语适用于本标准：

IoV　车联网（Internet of Vehicles）
RSU　路侧单元（Road Side Unit）
DS　数字签名 （Digital Signature）
POW　工作量证明（Proof of Work）
POS　权益证明算法（Proof of Stake）
BFT　拜占庭容错算法（Byzantine Fault Tolerant）

4 基于区块链的车联网节点信任管理的基本要求

4.1 对节点的安全评估

要求对车辆节点的行为进行连续监控，获得车辆的历史行为和历史信任数据，进行信任评估。该过程使用区块链技术作为信任值的保障，存储数据记录，使用加密技术防止车辆隐私泄漏、保护车辆节点的隐私。

4.2 信任管理架构的设计

信任管理架构应具有收集车辆节点历史行为并进行信任评估的能力。该架构应分为三个

模块：主基站、从基站和车辆节点。

主基站用于维护主区块链区块，应具有以下功能：

A） 存储与计算车辆节点行为的相关数据；

B）使用区块链的共识机制，将车辆节点作为共识节点参与共识和车辆节点信息交互；

C）依据收到的车辆行为信息数据来计算节点信任值，并实时更新。

从基站用于维护从区块链区块，应具有以下功能：

A） 具有较强的传输、计算与存储能力；

B）使用区块链安全通道技术以及智能合约等技术，接收车辆节点传输的信任凭证信息，维护信任凭证信息，并上传收集到的信任凭证信息。

车辆节点负责收集和传输车联网事件，应具有以下功能：

A） 查询节点信任值；

B）收集和传输车联网事件；

C）生成信任凭证信息并上传。

信任管理架构设计如图 1 所示。

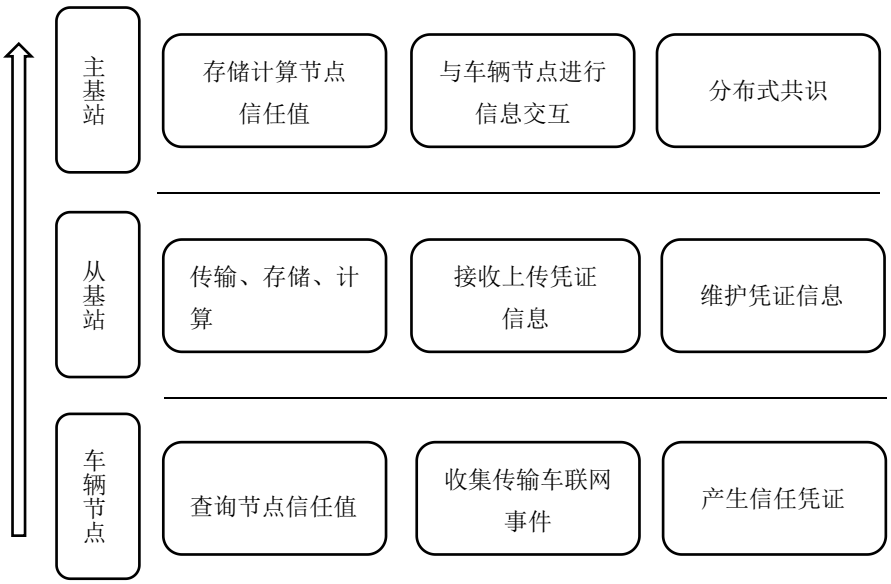

图 1 信任管理架构图

5 信任管理架构的机制要求

基于区块链的车联网节点信任管理架构包含三个机制，消息认证机制、信任评估机制以及信任评估机制，如图 2 所示。

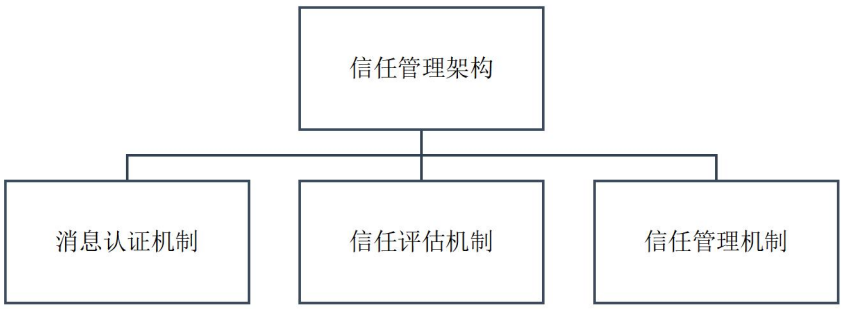

图 2 信任管理架构

5.1 消息认证机制

车辆节点消息认证应包含以下两点：

A） 消息发送方能够按照特定的规则对发送的消息进行变换，消息接收方接收消息后可以根据变换规则并对其进行验证，采用时间戳或数字签名等技术进行实现。

B）该消息认证机制能够验证消息来源的真实性、内容的完整性以及消息的有效性，实现车辆节点之间通信消息的安全性。

5.2 信任评估机制

信任评估机制应包含以下两点：

A） 接收车辆节点发送的消息时，能通过查询节点的信任变化程度来初步判断节点的可靠性和所述事件的真实性。

B） 该机制能综合考虑节点和消息两方面的因素，评估车辆节点的可信程度，计算车辆节点的综合信任值，并由综合信任值决定车辆的可信程度。

5.3 信任管理机制

信任管理机制应包含以下两点：

A） 负责车辆节点信任证书的生成、分发和撤销。

B） 通过该机制得到车辆节点的信任值，生成相应状态的信任证书。

6 信任管理架构相关的技术要求

6.1 信任管理技术要求

使用区块链技术实现对车联网节点的信任评估，维护与管理。要求将车辆节点、RSU 及其服务器构建成一个区块链网络，并将车辆节点的信任值当作车联网中的信息记录，形成新区块，并在该网络中进行传输、存储和维护。

6.2 区块链存储技术要求

使用区块链存储技术，以区块结构存储数据、数据由多方共同维护、并使用密码技术保证传输和访问的安全性。在信任值数据信息的存储过程中，使用加密算法，按照时间顺序将数据记录在区块链系统中，并附带相应的时间戳。数字区块必须通过所有参与节点的一致同意才可以更新，保证数据的安全性。

6.2 信任共识证明技术要求

使用工作量证明算法、权益证明算法、拜占庭共识算法等共识算法，进行分布式共识，将车辆信任值数据变化量最大的节点数据实时上传到分布式账本中，使信任值的更新具有时效性，提高主节点选择的合理性。