面向新能源汽车能源交易系统的PoRT共识机制

张海波[1,2]，李佳琪[1]，刘开健[1]，李方伟[2]
（1. 重庆邮电大学通信与信息工程学院，重庆 400065；2. 公共大数据安全技术重庆市重点实验室，重庆 401420）

摘　要：针对新能源汽车的能源交易系统在交易过程中容易出现隐私泄露等交易安全问题，设计了一种区块链下基于旅行验证的信誉值证明共识机制。首先，可信机构选择RSU作为节点构建区块链网络。然后，车辆采用基于旅行验证的信誉值证明（PoRT），通过位置签名确定、行驶里程验证和信誉值判断与更新3个阶段保证分布式信誉值数据库的迭代更新，进而确保能源交易系统的可持续运行。实验结果表明，与使用其他共识机制的能源交易系统相比，所提机制在面对车联网中常见攻击时具有更高的安全性和更低的交易时延。

关键词：车联网；区块链；能源交易；共识机制
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025016

PoRT consensus mechanism for energy trading system of new energy vehicles

ZHANG Haibo[1,2], LI Jiaqi[1], LIU Kaijian[1], LI Fangwei[2]
1. School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. Chongqing Key Laboratory of Public Big Data Security Technology, Chongqing 401420, China

Abstract: A reputation value proof consensus mechanism based on travel verification under blockchain was designed to address privacy leakage and other transaction security issues that easily occurred in the energy trading system of new energy vehicles during the trading process. Firstly, the RSU was chosen by the trusted authority to serve as nodes for building the blockchain network. Then, the proof of reputation value based on travel verification (PoRT) was used to ensure the iterative update of the distributed reputation value database by the vehicle through three stages, location signature determination, mileage verification, reputation value judgment and update to ensure sustainable operation of the energy trading system. The experimental results show that compared with energy trading system using other consensus mechanisms, the proposed mechanism has higher security and lower transaction latency when facing common attacks in the Internet of vehicles.

Keywords: Internet of vehicles, blockchain, energy trading, consensus mechanism

---

收稿日期：2024–11–07；**修回日期：**2025–01–09
通信作者：刘开健，1795248156@qq.com
基金项目：国家重点研发计划基金资助项目（No.SQ2023YFB250002402）；国家自然科学基金资助项目（No.62371082, No.62271094）；公共大数据安全技术重庆市重点实验室开放基金资助项目（No.CQKL-QJ202300002）；重庆市留创计划创新类基金资助项目（No.cx2020059）
Foundation Items: The National Key Research and Development Program of China (No. SQ2023YFB250002402), The National Natural Science Foundation of China (No. 62371082, No. 62271094), The Foundation of Chongqing Key Laboratory of Public Big Data Security Technology (No. CQKL-QJ202300002), Chongqing Innovation and Entrepreneurship Program for the Returned Overseas Chinese Scholars (No.cx2020059)

0 引言

随着新能源产业和分布式电力系统的发展和进步，新能源汽车作为其主要应用之一，成为车联网领域各大学者的研究热点。但由于充电站分配不均、续航里程难以满足人们需求等问题，新能源汽车目前仍面临诸多瓶颈与挑战[1]。与此同时，汽车到汽车（V2V, vehicle to vehicle）电力传输作为一种新型的充电技术[2]，其便捷、高效的特点使其与新能源汽车高度适配，基于V2V电力传输技术的新能源汽车能源交易系统应运而生[3]。然而，新能源汽车能源交易系统的环境是不可信的，这种点对点信息交互的能源交易模式极易遭受各种网络攻击。

为了确保车主的隐私安全，保证在信息安全的情况下进行能源交易，国内外学者在区块链框架下重新搭建了新能源汽车能源交易系统。区块链技术能够支持车联网进行能源交易的主要原因是其具有去中心化、安全性、透明度、不变性和自动化特性。区块链技术的引入无疑为解决能源交易系统的安全问题提供了一种新的解决方案，最重要的是基于区块链技术的解决方案可以通过建立安全的数据库显著提高车联网应用的安全性[4-8]。传统车联网通过建立集中式数据库对车辆信息进行统一管理[9]，但在车辆数量激增的当下，无论是对服务器算力的高要求，还是对集中式数据库内存的高要求，都使其无法满足日益增长的需求。

文献[10]为了解决联网车辆安全性较低导致的可能威胁用户隐私安全的问题，利用区块链技术的去中心化特性和对数据的篡改保护，提出了一种基于区块链的联网车辆敏感数据隐私保护方案。首先使用去中心化数据库和加密技术生成无限的数据块，并按照时间顺序组织复杂的数据块，然后对区块链的每条信息进行备份，以满足隐私敏感数据的完整性和限制性安全要求。

文献[11]在使用区块链框架的基础上讨论了包括隐私安全、性能和车联网特定优化的共识机制，并特别强调了车联网的不同应用场景以及区块链在车联网应用中存在的关键挑战。同时，文献[10]指出了面向车联网的区块链技术目前仍存在以下问题，即在车联网中使用基于区块链的方法对计算资源和存储资源有巨大的要求，同时区块链难以满足车联网的实时性需求。对于上述问题，优化共识机制是一种可能的解决方案，所以探索更适合车联网的共识机制是未来的主要研究方向之一。

目前已经有大量研究将区块链中的共识机制应用于能源交易平台[12-16]，其中不乏有许多文献使用传统的区块链共识机制，如工作量证明（PoW, proof of work）、权益证明（PoS, proof of stake）、委托权益证明（DPoS, delegated proof of stake）和实用拜占庭容错（PBFT, practical Byzantine fault tolerance）。但近几年的研究表明，在车联网这一特殊环境下直接使用传统的区块链共识机制，其效果并不理想。于是，许多学者陆续提出了面向车联网环境的共识机制。为了解决区块链下的分布式共识问题，文献[12]将雾计算引入共识机制中，该方案通过在DPoS中引入改进的PBFT，缩短了出块周期但降低了系统的容错性。同样，文献[13]提出了区块联盟共识（BAC, block alliance consensus）机制应对去中心化模式下容易受到Sybil攻击的问题，该机制提高了系统的容错性，但是需要解决车辆节点的分片和激励问题。文献[17]利用区块链共享隐私数据，通过改进DPoS共识机制提出了混合拜占庭容错的委托模型证明（DPoM, delegated proof of model）共识机制，在保障数据隐私性和安全性的前提下，提高了共识效率。虽然该轻量化的共识机制改进了拜占庭容错共识算法的不足，减少了系统运行时间，但是仍在动态环境的适用性方面存在不足。

同时，也有不少学者在传统车联网的场景下，通过信任管理机制和建立对应数据库的方式保护车联网信息安全。文献[18]对信任管理机制在车联网中的适配性进行了调研，并在调研基础上基于贝叶斯推理模型验证消息，提出了一种识别和隔离被劫持车辆的信任管理机制。在该机制中，路边单元（RSU, road side unit）负责从车里收集信任数据并维护区块链。文献[19]特别考虑到信任管理机制中的评级问题，并提出了车辆的信誉值是在评级提供商的协议下基于评级所构建的。同时为确保评级在使用过程中不会被任何其他未经授权的实体滥用，使用一个中央服务器来存储和管理所有实体的信誉值数据。该方案可以有效地帮助车辆评估所接收信息的可信度，但是并未考虑车辆自主管理自身信任评级的问题。

进一步地，一些研究开始结合信誉值和共识机制，文献[20]提出了一种委托信誉证明（DPoR, delegated proof of reputation）共识机制，提高了基于区块链的分布式碳排放交易系统的安全性和效率，但是该机制的局限性在于需要提前建立合理的动态信誉评估体系。文献[21]为了满足V2V能源交易对可靠性、吞吐量和扩展性的要求，利用PBFT和信誉证明（PoR, proof of reputation）的优势，提出了一种新的基于实用拜占庭容错的信誉证明（PPoR, PBFT-based PoR）共识机制，但是需要牺牲系统一定的隐私性。文献[22]提出了一种基于许可区块链的能源共享方法，该方法利用微电网的供应状况和信誉值作为区块链准入标准，优化了区块链的共识机制。进一步地，文献[23]设计了一种基于许可区块链的智能交通系统，通过集成PoS和PBFT共识机制提出了一种去中心化的信誉评估机制，提高了系统的共识效率，然而该机制仍然面临安全性不足的问题。

综上所述，现有共识机制难以满足车联网中能源交易系统的安全性要求，故本文提出了一种面向新能源汽车能源交易系统的基于旅行验证的信誉值证明（PoRT, proof of reputation value based on travel verifiation）共识机制，主要工作如下。

1) 构建了一种分布式车联网系统模型，完善能源交易系统中的交易数据传输过程，提出了一种基于旅行验证的信誉值证明共识机制，通过位置签名确定、行驶里程验证和信誉值判断与更新，完成对车辆的认证和区块链的共识。

2) 建立车辆信誉值数据库，在车辆进行能源交易前先对信誉值进行判别，然后在车辆完成能源交易后对信誉值进行相应的更新，确保系统正常运行。

3) 通过仿真实验验证本文机制的合理性和有效性，并分析了本文机制如何应对车联网中的常见攻击。

1　系统模型

1.1　网络模型

如图1所示，为了实现社交车辆的人性化，保障车联网中能源交易的安全性，构建了基于区块链的能源交易系统网络模型。具体而言，整个网络模型分为区块链层、物理层和社交纽带层，包含可信机构（TA, trusted authority）、电动汽车用户（EVU, electric vehicle user）、RSU和区块链四类角色。

1) 可信机构。完全可信的实体，在系统初始化阶段，TA将对电动汽车用户和RSU进行身份注册和密钥管理。初始化后，TA将保持离线状态，避免影响区块链的去中心化特性。当出现恶意行为时（如恶意驱动程序发送伪造数据），TA将会跟踪恶意数据发送者撤销其身份认证。

2) 电动汽车用户。网络中的最小通信实体，其作为能源的供给方或者需求方与其他EVU进行能源交易，并将交易数据发送给RSU。

3) RSU。在路边间隔分布，是组成区块链网络的节点，与EVU进行信息交互，将能源交易数据中的索引信息和车辆的信誉值存储到区块链上，同时将具体的交易数据存储至边缘服务器。

4) 区块链。一个分布式的数据库，可以保障数据的完整性，存储各类实体的身份注册信息、车辆的信誉值和能源交易数据的索引信息，确保数据的真实性、有效性和不可篡改性。

在该网络模型下，利用非线性定价协商算法确保能源交易双方至少能在满足弱帕累托效应的情况下获得最优定价。具体而言，车辆v_i根据车辆v_j所提供的购买价格和数量向v_j提供其所需能源总量，v_i只有在交易无法满足弱帕累托效应时才允许退出此次交易。然后v_i可以选择更换v_j并重复上述过程，同时进行电子货币地址交易。如果v_i在交易中途被强行终止，则v_i的信誉值会被扣除，当其信誉值低于设定阈值时会被剥夺参与能源交易和上传能源交易数据的资格。

1.2　交易数据传输

如图1所示，交易数据传输过程包含实体初始化认证、数据存储和记录共享三步。

1) 实体初始化认证（①）。系统进行初始化，电动汽车用户和RSU向TA申请身份注册成为合法实体，TA完成密钥的分发。

2) 数据存储（②~④）。车辆在能源交易过程中需要向最近的RSU上传交易数据，该行为会自动触发数据存储智能合约（SCDS, smart contract for data storage）。车辆会先将能源交易的原始数据进行匿名和加密处理，然后上传给RSU。这些数据带有车辆的数字签名，对于不同的原始数据，车辆使用不同的假名证书降低其关联度以实现隐私保

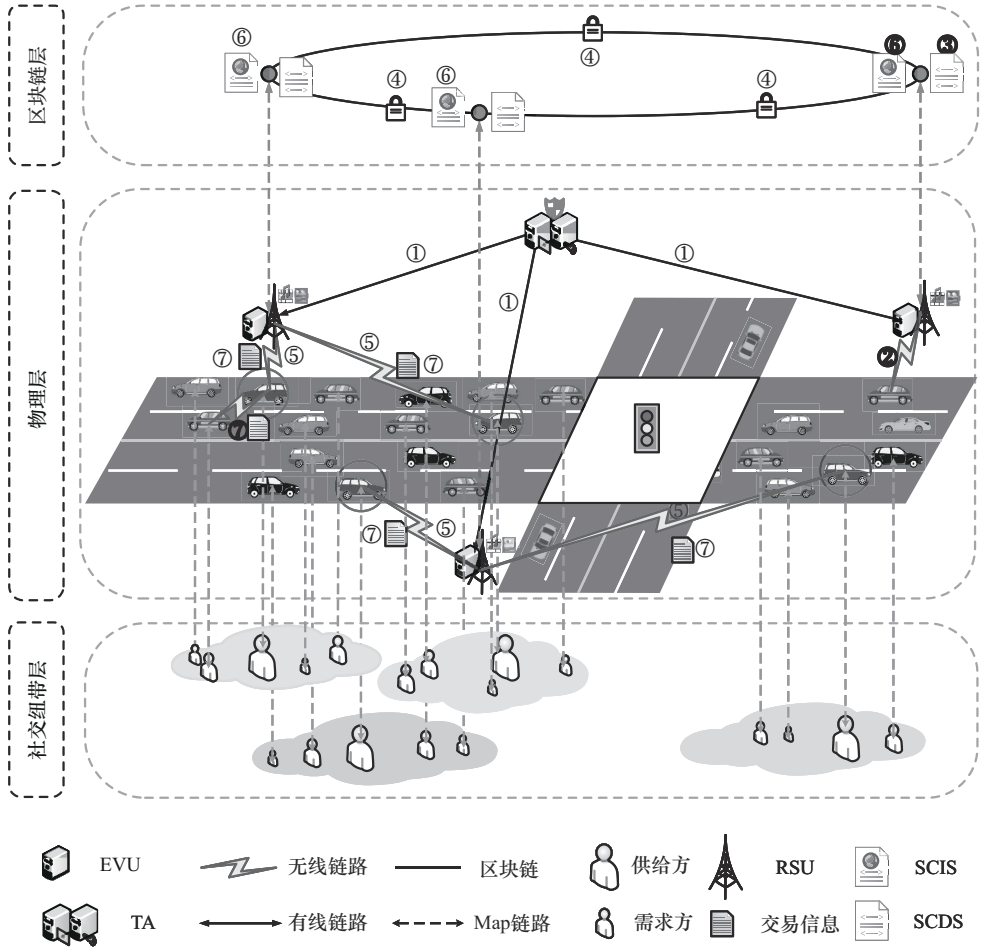

图1　基于区块链的能源交易系统网络模型

护。RSU收到数据后会定期整合打包，经过SCDS存储空间证明的机制达成节点共识。特别地，原始数据块将存储至区块链下的边缘服务器中，同时原始数据的索引信息存储至区块链上。

3) 记录共享（⑤~⑦）。车辆在共享交易数据前，首先会生成原始数据的索引信息，然后上传到RSU，触发信息共享智能合约（SCIS, smart contract for information sharing）并达成共识。具体而言，在上传能源交易数据前，车辆会生成一条原始数据的索引信息，包含时间戳、数据信息描述、数据所有者信息和存储地址。然后，该索引信息会被整合为一个块打包传至RSU处。RSU收到电动汽车用户发送的索引信息块后，先对其进行验证，然后通过PoRT共识机制达成共识。

2　基于旅行验证的信誉值证明共识机制

根据上述基于区块链的能源交易系统网络模型，当网络中的车辆完成能源交易并向RSU上传能源交易数据时，RSU需要处理这些能源交易数据并计算车辆的信誉值。此时，RSU利用PoRT共识机制通过位置签名确定、行驶里程验证和信誉值判断与更新三步完成共识过程，使能源交易数据和车辆信誉值在区块链网络中达成共识。

2.1　位置签名确定

为了便于车辆从其移动路径上的RSU获取位置签名，定义基于旅行验证的信誉值证明共识机制的消息格式和通信过程。TA和RSU利用PoRT共识机制确定车辆的信誉值，并验证车辆发送的车到基础设施（V2I, vehicle to infrastructure）消息中的位置签名，模型如图2所示。

该机制对于正常行驶的车辆没有影响，但能够使试图进行恶意破坏的车辆付出更多的额外资源。如果恶意车辆试图伪造虚假签名以提高自身的信誉值，那么他们将花费更多资源来解析和破译签名。这不仅提高了恶意车辆破坏网络的难度，还增加了它们的资源消耗。

在车辆行驶过程中，车辆所持有的位置签名为

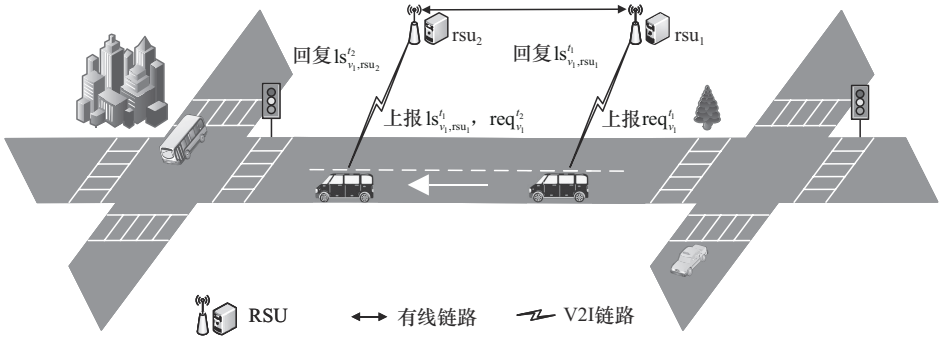

图2　车联网PoRT共识模型

车辆的轨迹提供证明，并用于信誉值的更新。

在 $t = t_k$ 时刻，车辆 v_i 向 rsu_j 发送位置签名，其定义为

$$\begin{aligned}\mathrm{sig} = {} & \mathrm{pk}_{\mathrm{rsu}_j}\|\mathrm{pk}_{v_i}\|t_k\|h_e\|h_{\mathrm{pre}}\|\sigma_{\mathrm{rsu}_j}(\mathrm{pk}_{\mathrm{rsu}_j}\| \\ & \mathrm{pk}_{v_i}\|t_k\|h_e\|h_{\mathrm{pre}})\end{aligned} \tag{1}$$

其中，$\mathrm{pk}_{\mathrm{rsu}_j}$ 为 rsu_j 所持有的公钥，pk_{v_i} 为车辆 v_i 所持有的公私钥对，σ_{rsu_j} 为 rsu_j 的数字签名，h_e 为车辆 v_i 所报告信息的哈希值，h_{pre} 为车辆 v_i 沿其移动路径从前一个RSU处所得到的哈希值，之所以将前一个RSU处所得到的哈希值包含进后一时刻的位置签名中，是为了防止车辆进行轨迹伪造，本文采用SHA-256算法计算哈希值。

为了构造位置签名，rsu_j 基于以上内容生成对应的数字签名 $\mathrm{sig}^{t_k}_{\mathrm{rsu}_j}$，即

$$\begin{aligned}\mathrm{sig}^{t_k}_{\mathrm{rsu}_j} = {} & \mathrm{pk}_{\mathrm{rsu}_j}\|\mathrm{pk}_{v_i}\|t_k\|h_e\|h_{\mathrm{pre}}\| \\ & \sigma_{\mathrm{rsu}_j}(\mathrm{pk}_{\mathrm{rsu}_j}\|\mathrm{pk}_{v_i}\|t_k\|h_e\|h_{\mathrm{pre}})\end{aligned} \tag{2}$$

并将此内容发送给 v_i 和TA，$\mathrm{sig}^{t_k}_{\mathrm{rsu}_j}$ 证明了车辆在给定时间内出现在特定位置上。

2.2　行驶里程验证

为了便于TA和RSU对位置签名进行处理，定义车辆 v_i 的旅行证明签名集为 $\mathrm{ls}^{t_0}_{i,j},\mathrm{ls}^{t_1}_{i,j+1},\cdots,\mathrm{ls}^{t_T}_{i,j+T}$，用于车辆 v_i 在周期 T 内沿其运动轨迹RSU移动的可验证行驶里程的计算。具体而言，车辆的可验证行驶里程主要分为3个阶段。

1) 初始证明生成阶段

从车辆（记作 v_1）加入车联网后遇到的第一个RSU开始（记作 rsu_1），车辆向其发送位置签名请求，记为

$$\mathrm{req}^{t_1}_{v_1} = \mathrm{pk}_{v_1}\|t_1\|e^{t_1}_1\|\mathrm{pos}^{t_1}_1\|\sigma_{v_1}(\mathrm{pk}_{v_1}\|t_1\|e^{t_1}_1\|\mathrm{pos}^{t_1}_1) \tag{3}$$

式(3)包含车辆所经过 rsu_1 的时间、自身身份认证信息、t_1 时刻周边环境流量信息 $e^{t_1}_1$、自身实时位置信息 $\mathrm{pos}^{t_1}_1$ 和公钥 pk_{v_1}，σ_{v_1} 为车辆 v_1 的数字签名。这些信息会经过 rsu_1 进行合理性检测，如果 rsu_1 认为该信息是有效且真实的，那么 rsu_1 会生成位置签名，并将其回复给车辆。

2) 轨迹编码采集阶段

当该车辆继续行驶，在沿途遇到下一个RSU，记作 rsu_2 时，车辆 v_1 将位置签名请求和 rsu_1 所生成的位置签名 $\mathrm{ls}^{t_1}_{v_1,\mathrm{rsu}_1}$ 一同发送给 rsu_2，如图2所示。rsu_2 首先对位置签名 $\mathrm{ls}^{t_1}_{v_1,\mathrm{rsu}_1}$ 进行核查，在核查通过后，生成 $\mathrm{ls}^{t_2}_{v_1,\mathrm{rsu}_2}$ 并将其发送给车辆 v_1。这一过程不断重复，直到车辆收集到足够的位置签名来形成一个证明链，其包含车辆所经过的地理位置信息、时间信息以及沿途RSU所给予的位置签名信息。

3) 可验证行驶里程验证阶段

从 $t = t_k$ 到 $t = t_{k+1}$ 时刻，车辆 v_i 可验证行驶里程定义为

$$\mathrm{vvmt}^{<t_k,t_{k+1}>}_i = d(\mathrm{ls}^{t_k},\mathrm{ls}^{t_{k+1}}) \tag{4}$$

通过轨迹编码采集阶段所生成的证明链，当车辆参与能源交易时，系统通过验证车辆持有的证明链来保证能源交易的合法性。对于首次参与能源交易的车辆，系统会根据位置签名计算该车辆的信誉值，并将此信誉值发送给车辆。

2.3　信誉值判断与更新

假设节点信誉值、节点最大信誉值和全局难度分别记为 R、R_m 和 D，节点受信誉影响后的当前难度为 D_l，信誉值与难度之间的转换因子为 R_c。

如果 $R < R_m$，则该节点的难度为

$$D_l = D + \frac{R_m - R}{R_m}\frac{D}{R_c} \tag{5}$$

如果 $R \geqslant R_m$，则节点的信誉值难度为

$$D_l = D - \frac{R - R_m}{R_m}\frac{D}{R_c} \tag{6}$$

PoRT的奖惩机制包含以下规则。

1) 当一个节点赢得了生成区块的权利，并且成功生成了区块，将区块添加到区块链中，则该节点将获得信誉值奖励。假设奖励周期用C_r表示，竞争周期用C_c表示，B表示一个节点在奖励周期中产生的区块数，而在竞争周期中具有最大信誉值的节点产生的最大区块数为$B_{\max}$。那么对节点良好行为的奖励E_r为

$$E_r = \frac{B}{\frac{C_r}{C_c}\frac{R}{R_m}B_{\max}} \tag{7}$$

如果$E_r \geqslant 1$，那么

$$R = R + \frac{(1 - E_r)(R_m - R)}{D_l} \tag{8}$$

2) 当一个节点赢得了生成区块的权利，但未能在给定时间内生成区块，则会通过式(9)和式(10)降低其信誉值。具有不良行为的节点将在惩罚周期C_p中受到惩罚，在惩罚周期中该节点产生的区块数和信誉值最大节点产生的最小区块数分别用B_p和$B_{\min}$表示。那么对节点的惩罚E_p为

$$E_p = \frac{B_p}{\frac{C_p}{C_c}\frac{R}{R_m}B_{\min}} \tag{9}$$

如果$E_p \geqslant 1$，那么

$$R = R - \frac{(1 - E_p)R}{D_l} \tag{10}$$

3) 如果一个节点当前的信誉值大于或等于R_m，并且该节点在上一个周期中至少产生过一个区块，则在下一个周期中，如果该节点获得了生成区块的权利但第一次没有生成区块，则可以免除一次降低信誉值的惩罚。

2.4 PoRT共识过程

当车辆v_i进行了一次能源交易后，向RSU上传能源交易数据，RSU会设置信誉值阈值$R_{\min}$和可验证行驶里程阈值$\text{vvmt}_{\min}$，只有当$R > R_{\min}$,$\text{vvmt}_i > \text{vvmt}_{\min}$时，RSU才会把本次的能源交易数据打包成块并添加到区块链中，同时广播到整个区块链网络中以达成共识。

3 仿真分析

3.1 安全性分析

本文基于Python3.8和Pycharm软件平台对所提共识机制进行仿真，具体仿真参数设置如表1所示。具体而言，车辆通信条件设置符合国际IEEE 802.11p标准，采用第三代合作伙伴计划（3GPP, 3rd generation partnership project）标准中的信道增益模型。通过模拟交通事件中车辆之间的通信，利用车辆的交互反馈来评估本文机制的性能。

表1 仿真参数

参数	值
MAC协议	IEEE 802.11p
车辆数量/辆	500
稳定通信范围/m	200~500
车辆最大发射功率/dBm	23
RSU最大发射功率/dBm	40
最大车速/(km·h^{-1})	60
道路长度/km	5
车辆长度/m	5
道路范围/km^2	5.4
RSU覆盖范围/m	300~500
信誉值阈值	0.5
消息频率/(次·min^{-1})	10~30

图3为网络拓扑，模拟正常城市环境进行车辆之间的能源交易，设置车辆最大速度为60 km/h，能够参与能源交易的信誉值阈值为0.5。

从表2的区块链仿真结果可以看出，在使用区块链存储相关信息并将其打包成块上传到区块链的过程中，相较于其他信息存储方式，出块时延会有一定的波动。这种波动主要受难度系数的影响，当某个RSU被选为此次共识的负责节点时，它需要在规定时间内完成哈希解密，由于区块链的难度系数不是固定的，因此出块时延会出现波动。

本文将所提共识机制的出块时延可视化，并与传统的PoW[24]和PoS[25]进行了对比，结果如图4所示。可以明显看出，相较于传统的PoW和PoS，本文机制时延波动更稳定，平均时延更低。

为了验证网络在遭受共谋攻击时依然能够正常运行，分别在车联网中存在5%恶意节点、20%恶意节点、35%恶意节点和50%恶意节点的情况下模拟车辆的信息交互，观察信誉值更新情况，仿真结果如图5所示。

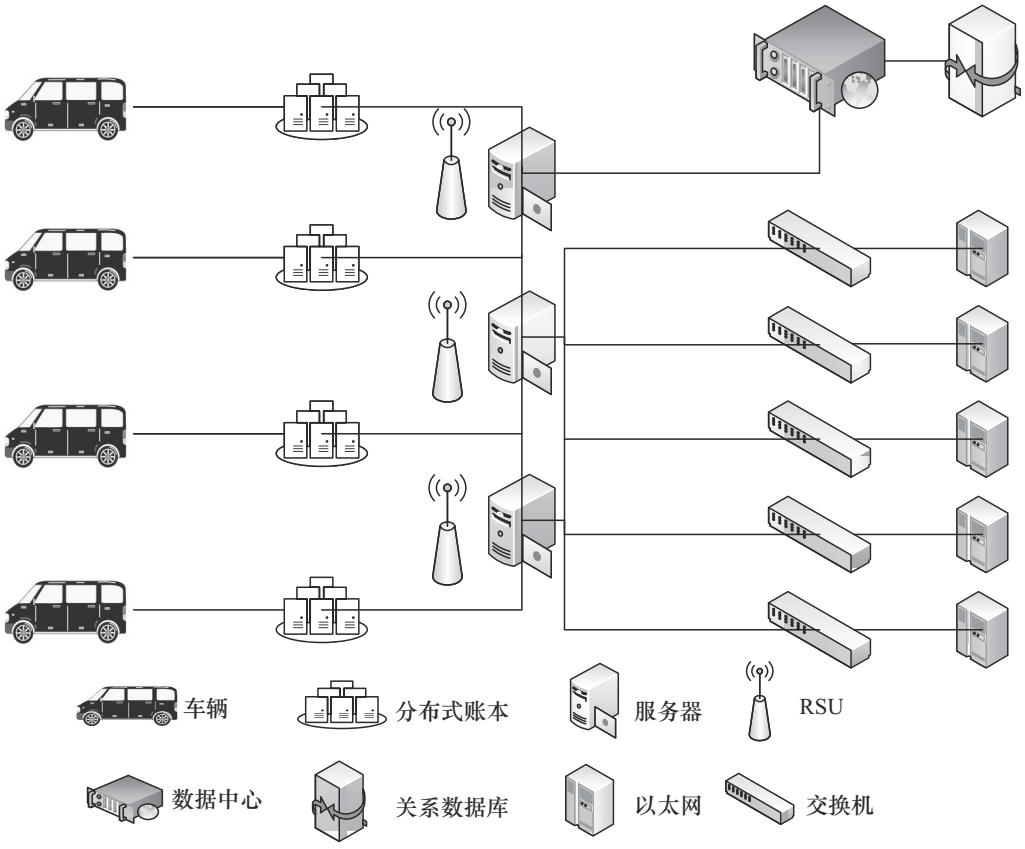

图3　网络拓扑

表 2　　**区块链仿真结果**

存储数据	上次哈希值	本次哈希值	出块时延/ms
KBMOP200	075c27741a3506846368fa6e5b3477f8 5b31ceee71a5716e2f12b40fa21d23aa	000cfbb745e3d504306b8c435b639d1d	0.339 311
BCUSD300	000cfbb745e3d504306b8c435b639d1d	0008fc36bf8a3fac06b898239c5f6ff5	0.084 401
CAHKD400	0008fc36bf8a3fac06b898239c5f6ff5	000d53dca390ad96919423125a898d7b	0.462 242
EIGKD500	000d53dca390ad96919423125a898d7b	00028f1aeae4c259007d4a41eaed19a1	2.174 224
GSQSJGKD600	00028f1aeae4c259007d4a41eaed19a1	000413ca0bed8c018d575de5da26ca18	1.140 511
YTUFHKD700	000413ca0bed8c018d575de5da26ca18	0005644954653353eaa213e294defe04	2.936 089
ASDTEQED800	0005644954653353eaa213e294defe04	00046785d0472821f544efcfa12a8068	2.449 033
OINNHHD900	00046785d0472821f544efcfa12a8068	0009e5e44c5e7ad38a873e76031086a6	1.426 287
YTKJUUY1000	0009e5e44c5e7ad38a873e76031086a6	000a2c11f37abc97ba76e1e7248fa69a	1.193 890
BNLILKD1100	000a2c11f37abc97ba76e1e7248fa69a	00012a74ce6196446435ddf4399d4bc8	0.571 789

从图5中可以看出，本文机制对共谋攻击有较强的抵抗性。在仅有少部分恶意节点时，车联网中正常车辆的信誉值受影响程度较低，而在网络存在50%恶意节点的情况下，随着车辆交互次数的增多，正常车辆的信誉值仍然能够保持稳定上升趋势，从而保证车联网中信息交互的正常进行。

开关攻击需要恶意车辆节点伪装成正常车辆进行正常活动，这使前期恶意车辆处于潜伏期时，网络无法对其进行检测。但当恶意车辆在后期开始进行破坏活动时，在信誉值更新机制的影响下，多次的非正常活动会使其信誉值急剧降低，最终导致其失去参与本网络的资格。这对于虚假信息攻击也一样，当恶意车辆多次发布虚假信息时，信誉值更新机制也会令其信誉值急剧降低，最终无法再参与能源交易。

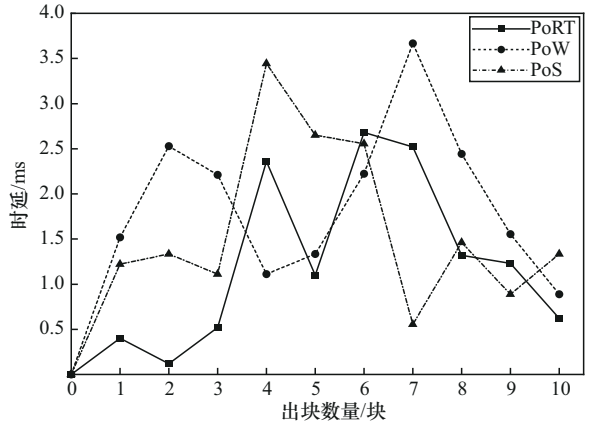

图4　区块链出块时延

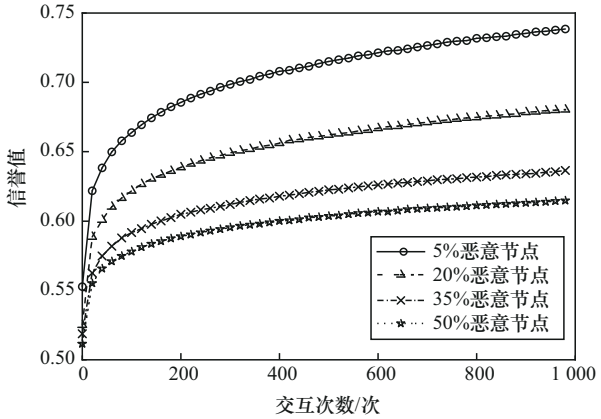

图5　共谋攻击交互次数

由于区块链网络的唯一性和不可逆性，信息重放攻击几乎无法在区块链网络中成功。发布或上传相关信息需要对难度值系数不同的哈希算法进行解密，就算难度系数一定，同一 RSU 都无法满足在相同时间的情况下进行解密，所以自然不存在使用相同 Message ID 或 User ID 进入同一消息队列并对之前信息进行修改的情况。

为了验证本文机制在动态移动情况下的时延变化情况，本文模拟了安全环境下车辆使用 PoRT 共识机制进行信息交互的过程，仿真结果如图 6 所示。

从图 6 可以看出，随着车辆运行速度的加快，车辆参与 PoRT 的时延逐渐增加。随着参与信息交互车辆数量的增加，PoRT 进行共识的时延同样也呈现增加趋势。当车辆速度达到 80 km/h 时，PoRT 时延较大，但在城市环境下，大部分城区路段限速为 60 km/h，所以在设定最大速度为 60 km/h 的限制下，PoRT 在信息交互时延方面有着较好的表现。

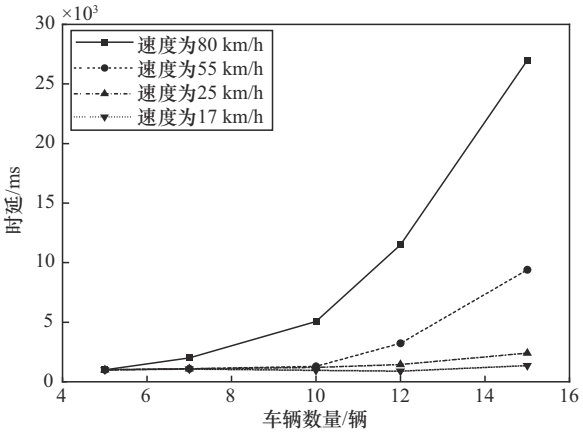

图6　不同车速下 PoRT 时延

本文分别对 $vvmt_{min}=60\%S$、$vvmt_{min}=70\%S$ 和 $vvmt_{min}=80\%S$ 进行了仿真实验，结果如图 7 所示，其中 S 为所有车辆的加权平均可验证行驶里程。从图 7 可以看出，随着恶意车辆比例的增加，能源交易数据共识失败比例也越来越高，符合客观规律，同时，越高的可验证行驶里程阈值能够保障车辆能源交易数据的共识成功率，体现了 PoRT 共识机制的有效性。

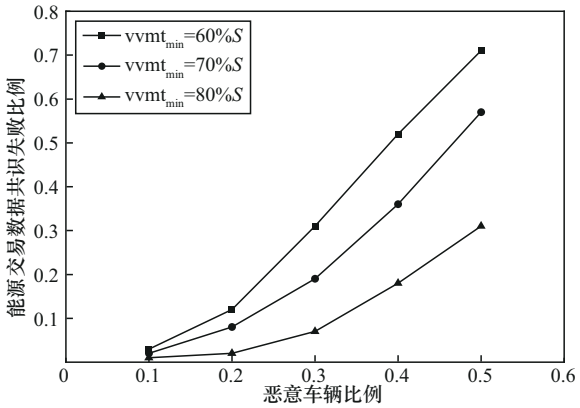

图7　可验证行驶里程阈值对比

3.2　信誉值判断与更新仿真分析

为了验证本文所提信誉值判断与更新方法的有效性，设计如表 3 所示的信誉值仿真参数的仿真实验进行验证分析。从图 8 可以看出，当初始信誉值为 500 时，随着区块数量的增加，节点信誉值呈现阶梯上升的趋势，最后在区块数量为 120 左右时节点信誉值基本稳定。通过分析图 9 可以得出，当初始信誉值为 1 000 时，信誉值先上升后稳定再呈现阶梯上升的趋势。从图 10 可以看出，在初始信誉值为 1 500 的高信誉值基础上，节点信誉值在前几次区块生成后有显著提升，而后保持稳定。

表3　　信誉值仿真参数

参数	值
信誉值上限	2 000
信誉值下限	0
初始信誉值	1 000
信誉值更新周期	12
奖励周期	24
惩罚周期	36
最大区块数量/块	6
最小区块数量/块	2
转化率因子	1

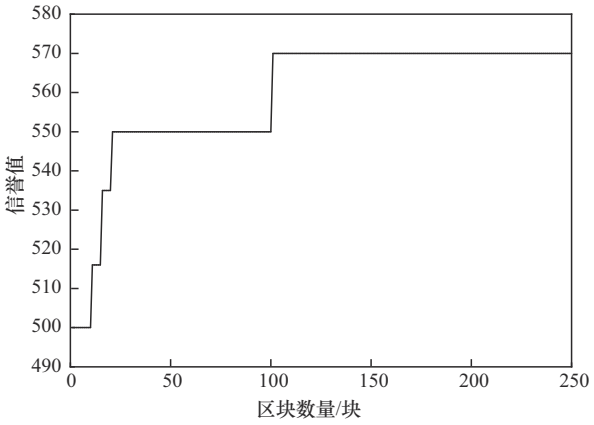

图8　初始信誉值为500时信誉值变化

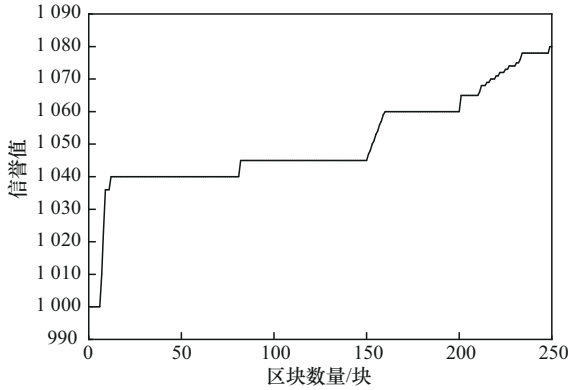

图9　初始信誉值为1 000时信誉值变化

通过分析表4可以得出，在不同初始信誉值的条件下，高信誉值节点成功生成区块的比例远远高于低信誉值节点，这说明通过本文所提信誉值判断与更新方法进行PoRT共识，低信誉值节点能够通过自身良好行为的积累使其信誉值稳步上升，同时，已经获得高信誉值的节点能够在此网络中拥有更多话语权。

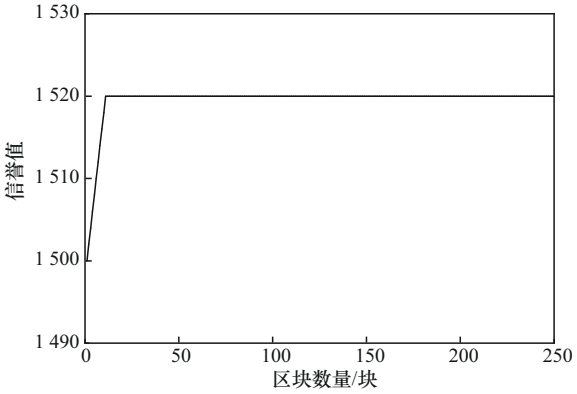

图10　初始信誉值为1 500时信誉值变化

表4　　初始信誉值不同仿真结果

初始信誉值	生成的区块数量/块	生成区块的比例
500	42	14.00%
1 000	68	22.67%
1 500	190	63.33%

4　结束语

本文针对车联网中基于区块链的能源交易系统存在的安全问题，结合可验证行驶里程和位置签名确定提出了PoRT共识机制，在系统中利用区块链技术的特性保证了车辆在不同区域进行能源交易时RSU内信息的安全性、一致性和可追溯性。最后，通过仿真验证本文机制的有效性，以及在面对各类攻击时具备一定的抵抗性。但是不可避免的，本文存在一定的局限性，由于共识机制的多样性使得不同机制下的区块链网络存在较大的时延差异和安全性差异，时延更低的共识机制能够使系统得到更精准的反馈，但如果追求低时延而忽略安全性，则会使此网络极易遭受恶意攻击。所以如何平衡低时延、高吞吐量和安全性是未来研究完善的方向。

参考文献：

[1] YUVARAJ T, DEVABALAJI K R, KUMAR J A, et al. A comprehensive review and analysis of the allocation of electric vehicle charging stations in distribution networks[J]. IEEE Access, 2024, 12: 5404-5461.

[2] YU Y, LI G L, LIU Y, et al. V2V energy trading in residential microgrids considering multiple constraints via Bayesian game[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(6): 5946-5957.

[3] WANG Y S, ZHANG D X, LI Y X, et al. Enhancing power grid resilience with blockchain-enabled vehicle-to-vehicle energy trading in renewable energy integration[J]. IEEE Transactions on Industry Applications, 2024, 60(2): 2037-2052.

[4] ZYSKIND G, NATHAN O, PENTLAND A S. Decentralizing privacy: using blockchain to protect personal data[C]//Proceedings of the 2015 IEEE Security and Privacy Workshops. Piscataway: IEEE Press, 2015: 180-184.
[5] CHANG H G, LIU Y M, SHENG Z G. Blockchain-enabled online traffic congestion duration prediction in cognitive Internet of vehicles[J]. IEEE Internet of Things Journal, 2022, 9(24): 25612-25625.
[6] FERRAG M A, SHU L. The performance evaluation of blockchain-based security and privacy systems for the Internet of things: a tutorial[J]. IEEE Internet of Things Journal, 2021, 8(24): 17236-17260.
[7] SRIVASTAVA V, DEBNATH S K, BERA B, et al. Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for Internet of vehicles environment[J]. IEEE Transactions on Vehicular Technology, 2022, 71(9): 9853-9867.
[8] QI J, LIU Y L, LING Y C, et al. Research on an intelligent computing offloading model for the Internet of vehicles based on blockchain[J]. IEEE Transactions on Network and Service Management, 2022, 19(4): 3908-3918.
[9] SHRESTHA R, BAJRACHARYA R, NAM S Y. Centralized approach for trustworthy message dissemination in VANET[C]//Proceedings of the NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. Piscataway: IEEE Press, 2018: 1-5.
[10] XU C, WU H J, LIU H Z, et al. Blockchain-oriented privacy protection of sensitive data in the Internet of vehicles[J]. IEEE Transactions on Intelligent Vehicles, 2023, 8(2): 1057-1067.
[11] MOLLAH M B, ZHAO J, NIYATO D, et al. Blockchain for the Internet of vehicles towards intelligent transportation systems: a survey[J]. IEEE Internet of Things Journal, 2021, 8(6): 4157-4185.
[12] SUN G, DAI M, ZHANG F, et al. Blockchain-enhanced high-confidence energy sharing in Internet of electric vehicles[J]. IEEE Internet of Things Journal, 2020, 7(9): 7868-7882.
[13] WANG Y S, YUAN L M, JIAO W H, et al. A fast and secured vehicle-to-vehicle energy trading based on blockchain consensus in the Internet of electric vehicles[J]. IEEE Transactions on Vehicular Technology, 2023, 72(6): 7827-7843.
[14] LI M, HU D H, LAL C, et al. Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6564-6574.
[15] AGGARWAL S, KUMAR N, TANWAR S, et al. A survey on energy trading in the smart grid: taxonomy, research challenges and solutions[J]. IEEE Access, 2021, 9: 116231-116253.
[16] BARNAWI A, AGGARWAL S, KUMAR N, et al. Path planning for energy management of smart maritime electric vehicles: a blockchain-based solution[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(2): 2282-2295.
[17] 莫梓嘉, 高志鹏, 杨杨, 等. 面向车联网数据隐私保护的高效分布式模型共享策略[J]. 通信学报, 2022, 43(4): 83-94.
MO Z J, GAO Z P, YANG Y, et al. Efficient distributed model sharing strategy for data privacy protection in Internet of vehicles[J]. Journal on Communications, 2022, 43(4): 83-94.
[18] YUAN M Y, XU Y, ZHANG C, et al. TRUCON: blockchain-based trusted data sharing with congestion control in Internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(3): 3489-3500.
[19] LIU Y, XIONG Z H, HU Q, et al. VRepChain: a decentralized and privacy-preserving reputation system for social Internet of vehicles based on blockchain[J]. IEEE Transactions on Vehicular Technology, 2022, 71(12): 13242-13253.
[20] HU Z, DU Y H, RAO C J, et al. Delegated proof of reputation consensus mechanism for blockchain-enabled distributed carbon emission trading system[J]. IEEE Access, 2020, 8: 214932-214944.
[21] ABISHU H N, SEID A M, YACOB Y H, et al. Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the Internet of electric vehicles[J]. IEEE Transactions on Vehicular Technology, 2022, 71(1): 946-960.
[22] KHALID S, AHMAD I, LEI H S. A consortium blockchain-based approach for energy sharing in distribution systems[J]. IEEE Transactions on Network and Service Management, 2024, doi: 10.1109/TNSM.2024.3501397.
[23] DENG Z H, TANG C M, LI T T, et al. Permissioned blockchain-based trusted and robust consensus optimization orienting intelligent transportation systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, doi: 10.1109/TITS.2024.3496553.
[24] LI W B, CAO M W, WANG Y, et al. Mining pool game model and nash equilibrium analysis for PoW-based blockchain networks[J]. IEEE Access, 2020, 8: 101049-101060.
[25] XU C H, QU Y Y, LUAN T H, et al. A lightweight and attack-proof bi-directional blockchain paradigm for Internet of things[J]. IEEE Internet of Things Journal, 2022, 9(6): 4371-4384.

[作者简介]

张海波（1979– ），男，重庆人，博士，重庆邮电大学副教授、硕士生导师，主要研究方向为车联网、区块链、安全认证等。

李佳琪（2000– ），男，四川内江人，重庆邮电大学硕士生，主要研究方向为车联网、区块链、信任管理。

刘开健（1981– ），女，重庆人，重庆邮电大学高级工程师，主要研究方向为区块链、信任管理等。

李方伟（1960– ），男，重庆人，博士，公共大数据安全技术重庆市重点实验室教授，主要研究方向为下一代无线通信系统的关键技术、移动通信安全、时间反演等。