

# 车载自组织网络中基于区块链的路况预警方案

李春燕<sup>1,2</sup>, 赵佳<sup>1,2</sup>, 刘吉强<sup>1,2</sup>, 张强<sup>3</sup>, 韩磊<sup>4</sup>

- (1. 北京交通大学智能交通数据安全与隐私保护技术北京市重点实验室, 北京 100044;  
2. 北京交通大学计算机与信息技术学院, 北京 100044;  
3. 北京市公安局网络安全保卫总队, 北京 100029;  
4. 信息保障技术重点实验室, 北京 100071)

**摘要:** 路况预警方案是解决车载自组织网络 (VANET, vehicular ad-hoc network) 中车辆拥堵、交通事故问题的有效手段。分析了我国目前的交通状况以及车载自组织网络的发展和应用, 结合区块链技术提出了一种适用于车载自组织网络的基于区块链的路况预警方案。采用 Hyperledger Fabric 联盟链技术平台对该方案进行了仿真实验, 实验结果表明本方案合理、可行。

**关键词:** 车载自组织网络; 区块链; Hyperledger Fabric; 路况预警

**中图分类号:** TP309.2

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2018058

## Blockchain-based traffic condition early-warning scheme for VANET

LI Chunyan<sup>1,2</sup>, ZHAO Jia<sup>1,2</sup>, LIUJiqiang<sup>1,2</sup>, ZHANG Qiang<sup>3</sup>, HAN Lei<sup>4</sup>

1. Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China  
2. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China  
3. Beijing Municipal Public Security Bureau Network Security and Security Corps, Beijing 100029, China  
4. Science and Technology on Information Assurance Laboratory, Beijing 100071, China

**Abstract:** Road conditions early-warning scheme is effective solution to solve vehicle congestion and traffic accidents of VANET. The current traffic conditions in China as well as the development and application of VANET were analyzed. Combined with blockchain technology, a blockchain-based traffic conditions early-warning scheme for VANET was proposed. The Hyperledger Fabric alliance chain technology platform is used to simulate this scheme. The experimental results show that the scheme is reasonable and feasible.

**Key words:** VANET, chainblock, Hyperledger Fabric, road condition alarming

## 1 引言

21 世纪初, 我国国民经济以惊人的速度增

长, 国民生活水平不断提高, 使我国机动车的数量不断增长。数据显示, 从 1995 年到 2014 年期间, 中国机动车的增长率为每年 10%, 达到 1.5 亿辆<sup>[1]</sup>;

收稿日期: 2018-06-10; 修回日期: 2018-06-30

通信作者: 李春燕, 17125202@bjtu.edu.cn

基金项目: 中央高校基本科研业务费基金资助项目 (No.2018JBM016); 国家自然科学基金青年科学基金资助项目 (No.61502030); 信息保障技术重点实验室开放基金资助项目 (No.KJ-17-107)

**Foundation Items:** Fundamental Research Funds for the Central Universities (No.2018JBM016), The National Natural Science Foundation of China (No.61502030), Foundation of Science and Technology on Information Assurance Laboratory (No.KJ-17-107)

截止到 2015 年底,我国机动车数量有 2.79 亿辆,到 2016 年底,我国机动车数量有 2.9 亿辆,到 2017 年底,我国机动车数量持续增长有 3.1 亿辆,图 1 为 2012-2017 年中国机动车保有量柱状图。机动车数量的不断增加导致道路拥堵更加严重,此外,酒后驾车、违反交通规则等行为的增多也增加了道路拥堵的严重性。交通堵塞问题给我国公民的生活带来了严重不便,因此,我国城市的交通堵塞、交通事故等问题亟待解决。

随着 21 世纪互联网行业的发展,智慧城市的建设已是大势所趋,车载自组织网络是智慧城市中极其重要的一部分,未来的智能交通系统将很大程度上依赖于车载自组织网络。有数据显示我国的车辆拥堵、交通事故等交通状况严重困扰着我国公民的生活和出行,同样的交通问题也必将出现在未来智慧城市的车载自组织网络中。

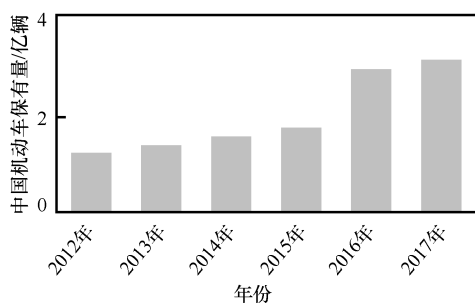


图 1 中国机动车保有量

车载自组织网络是一种具有移动 ad hoc 网络大部分特性的特殊移动自组织网,在车载自组织网络中装配无线通信作用的节点(这些节点大多数情况下由车辆和路边单元构成)有数千个,这些无线节点在车载自组织网络中采用多跳的方式通信。在车载自组织网络中,每一个车辆节点都具有 3 个角色(发送者、接收者和路由器)在车辆网络中收发信息,为人们搭建了便捷舒适的交通路况,这增加了车辆之间沟通方式的积极性,也能准确发现道路状况(车辆拥堵、交通事故等)。在车载自组织网络节点之间采用无线通信方式的包括:车辆节点之间、路边单元 RSU 之间以及车辆节点和路边单元 RSU 之间。车载自组织网络是物联网的一部分,它在实现车辆间无线通信的同时还可以对车载网中的数据进行存储处理,以及

大数据分析,使网络系统得到很大程度的改善、信息服务的质量大幅度地提高,使大数据等行业得到发展的同时,也对国家经济和社会的发展有促进作用。如今,车载自组织网络正在朝着人-车-事物-环境深度融合的方向发展,改善了交通状况,缩短了出行时间,给人们的出行带来了极大的便利。总而言之,车载自组织网络将车辆的功能和设施作为移动信息平台而不是简单的运输实体进行扩展,这大大丰富了车辆系统的功能<sup>[2-7]</sup>。

比特币的公开账本——区块链技术由中本聪在 2009 年首次提出,此后许多其他形式的电子现金也是用类似的结构进行创建,同时区块链技术也广泛应用于物联网等其他领域。区块链的潜在用途超过了比特币,区块链具有以下特性。

- 1) 分散控制:在区块链技术中不需要可信任的第三方制定规则。
- 2) 数据透明性和可审查性:系统中执行的每个事务的完整副本都存储在区块链的每个节点上,且所有节点都是对等公开的。
- 3) 分布式共识:在区块链技术中打破了集中共识的范式,采用所有网络节点共同参与交易的方式。
- 4) 安全性:当区块链被恶意操纵时,所有区块结构都需要改变,这种改变使其他节点知道此节点被别人篡改,能够立即察觉到,此外,区块链还能对交易进行验证。

物联网解决方案基本要素要求具有安全、分布式和自治等特性,区块链技术正是具有这些特性的一门技术。车载自组织网络是物联网的一部分,将区块链技术运用到车载自组织网络中能够很好地解决车载自组织网络中的安全等问题。

根据以上所列出的车载自组织网络中的交通路况问题以及区块链的特性,本文将区块链技术运用到车载自组织网络中,实现车载自组织网络中路况预警,该方案可实现:

- 1) 不需要可信任的第三方处理路况信息,就可辨别出正确路况并将正确的路况广播给其他车辆节点;
- 2) 区块链技术的应用使存储在区块内的正确的路况信息不能被篡改;
- 3) 车辆节点发送的路况信息具有可追溯性,如

果路况信息出现问题,可查找出有问题车辆节点。

因此,在车载自组织网络的路况预警中运用区块链技术保证路况信息具有去中心化、防篡改和可追溯等特性。

## 2 相关工作

从目前的形式来看,区块链技术已被国内外学者广泛应用于各个领域,其中包括物联网领域、云计算领域等。

区块链在物联网领域的应用:文献[8]提出了一种在物联网中基于区块链技术仲裁角色和权限的新的体系结构。文献[9]提出了在物联网中可应用区块链技术解决问题的4个领域:1)供应链管理;2)设备可以销售它们的设备性能;3)在共享经济中,设备可以销售它们的服务;4)设备之间互相通信。此外,文献[9]阐明了区块链能够保证数据的安全性和完整性,将其与分布式注册表技术相结合应用于物联网中会产生巨大的协同效应。文献[10]阐述了物联网中数据交换的需求,但是集中式基础设施无法提供作为数据交换的足够信任的第三方中介,区块链技术能够很好地解决这样的问题,由此,提出了基于区块链的物联网数据可信交换的分散式解决方案。文献[11]针对物联网中的隐私泄露问题,提出了区块链连接网关的方案,该方案中区块链网络自适应地维护物联网设备和用户的隐私,此外,还提出一种基于区块链技术的数字签名机制,来解决隐私纠纷问题。

区块链在云计算领域的应用:文献[12]利用区块链技术提高云取证中所有利益相关者交互记录的可信度。文献[13]针对用户和云服务交互过程中云服务器为了获得奖励而不诚实地删除用户数据问题,提出了一种基于区块链技术诚实地删除数据的方案,该方案不需要可信任的第三方且用户可以对云服务是否已经删除数据进行验证。文献[14]区块链技术的应用使在无信任环境中保管共享医疗数据取得成功。

区块链在其他领域的应用:文献[17]提出一种全新的排放交易计划,此计划中运用了区块链技术。文献[15]提出了一种基于区块链技术的侧管理,用于匹配智能电网层面的能源需求和生

产。文献[16]提出了一种基于区块链技术微电网分散式电力交易模式,使消费者的权益得到保障。

路况预警的发展状况:现有的文献实现路况预警消息的传播,大多采用多播路由协议,难以满足路况预警消息的实时性和可靠性。文献[17]在此基础上提出最优中继算法,中继算法的基本思想是当车辆收到周围邻居广播的告警消息后采用中继算法选出最优中继车辆进一步转发,而本文中提出的路况告警消息是由此路段的车辆节点采用区块链技术对同一条路况告警消息达成共识后,由固定单元在全网进行广播。

自2008年中本聪发表比特币白皮书后,国内外学者开始对区块链技术进行研究,将区块链应用于各个领域。区块链技术的特性(去中心化、防篡改、不可伪造、可追溯)能够很好地解决各个领域中的一些问题。

本文将比特币中传统的区块链结构改造成适用于车载自组织网络的区块链结构,在不需要可信第三方参与的情况下,实现路况预警且保证路况信息在传播过程中的正确性。车载自组织网络中基于区块链技术的路况预警方案的大致思想是:当道路上出现拥堵或交通事故时,该道路上的车辆节点会进行挖矿形成创世区块(即第一个区块),接下来其他车辆节点继续挖矿形成路况信息链,该路况信息链由附近的固定单元进行处理,将路况信息广播给其他固定单元,固定单元再广播给自己区域内的车辆,此外,固定单元还会将提供正确路况信息的车辆节点信息上传给车辆管理中心,车辆管理中心给这些车辆一些奖励。

本文运用区块链技术提出的路况预警方案相对于文献[17]中提出路况预警消息传播方案的优点如下。

1) 从路况消息的产生看,本文路况消息的产生是由多个车辆节点对一条路况消息达成共识,相对文献[17]中路况信息由一个车辆节点产生更加真实可信。且本文运用区块链技术能够有效保证路况告警信息的防篡改性和可追溯性。

2) 文献[17]中对告警消息的传播依然停留在协议层面,协议需要根据车辆接收告警信息功率满足一定的阈值,此方案需要一些算力,而本文

对路况告警信息达成一致后, 直接由路边固定单元进行广播, 节约一定的算力。

3) 本文在路况信息块添加了路况信息块消亡倒计时参数, 有效地保证了车载自组织网络中路况消息的实时性; 区块链技术是一个分布式账本, 保证了路况消息的可靠性。

### 3 车载自组织网络中基于区块链的路况预警方案概述

#### 3.1 车载自组织网络概述

车载自组织网络中大多数情况下包括: 车辆管理中心 (DMV, department of motor vehicle)、固定单元 (RSU, remote subscriber unit) 和车载通信单元 (OBU, on board unit)。每个车辆和固定单元想要加入车载自组织网络都需要到车辆管理中心进行注册 (注册时车辆管理中心将车辆和固定单元的信息以列表的形式存储, 且车辆管理中心给注册的车辆或固定单元发放签名证书和公私钥对), 此外, 在本文中, 车辆管理中心还会对提供路况信息的车辆给以奖励作为鼓励; 车载自组织网络中的每个车辆节点收发信息都是通过装载在车辆节点上的车载通信单元的无线通信; 车载自组织网络中的固定单元与车辆节点的地位相同, 但固定单元在车流量大的路口分布密集, 在车流量小

的地方分布稀疏, 固定单元具有收发信息以及路由的功能。

#### 3.2 区块链技术概述

最初的区块链技术中的区块结构包括区块头和区块体 2 部分, 区块结构如图 2 所示。区块头中包括: 随机数、时间戳、难度系数、前一个区块的 Hash 值 (即上一个区块的 Merkle 树根)、Merkel 树根以及下一个区块的 Hash 值 (即下一个区块的 Merkle 树根)。随机数是节点进行挖矿时, 节点计算出的挖矿结果的解; 时间戳表示区块结构生成的时间, 在区块链结构中, 前一个区块的时间戳会比后一个区块的时间戳小, 能够保证区块链有序地形成, 具有防篡改的作用; 难度系数是节点计算数学难题的难易程度, 可以人为进行调整; Merkle 树根为对每笔交易进行 Hash 运算得到的, 由于每笔交易都不相同, 所以每个区块的 Merkle 树根都不同, Merkle 树根能够实现交易的验证; 通过区块头中存储前一个区块的 Merkle 树根和后一个区块的 Merkle 树根将区块连接成区块链, 把从创世区块开始最长的链式结构称为主链。矿工在挖矿形成区块链的过程中, 会因为网络的延时或其他情况而导致区块链分, 此时会比较从分叉处以后所有区块的难度系数, 把难度系数高 (即工作量大) 的那条支链作为主链,

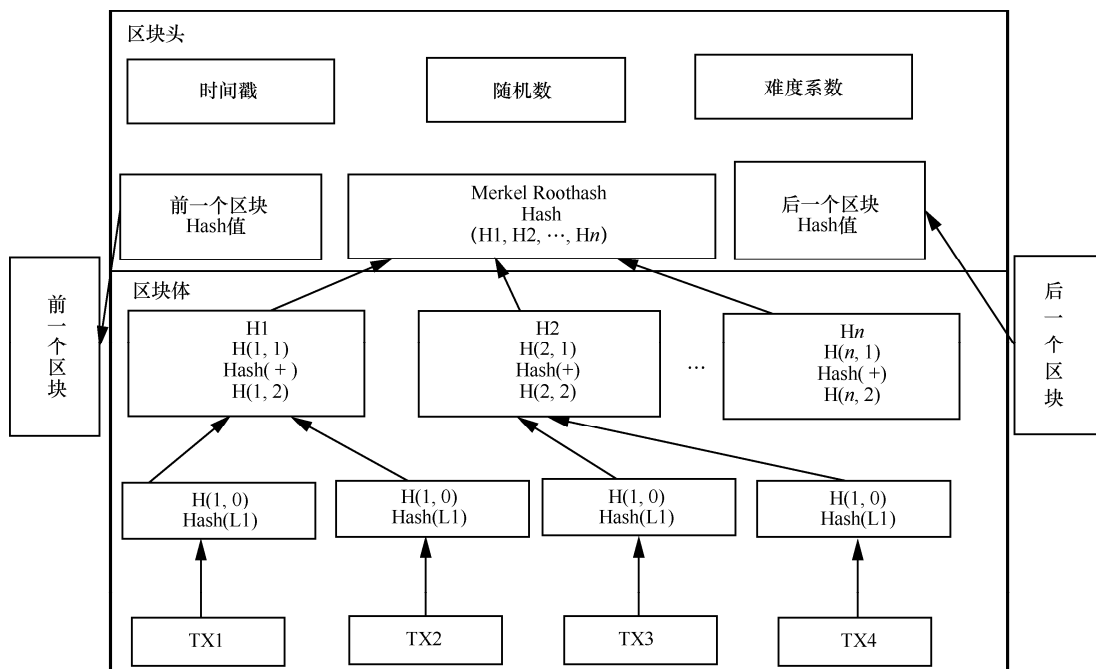


图2 区块结构

把后续形成的区块链添加到这条主链上, 区块链结构如图3所示, 区块链由多个区块组成<sup>[18-20]</sup>。

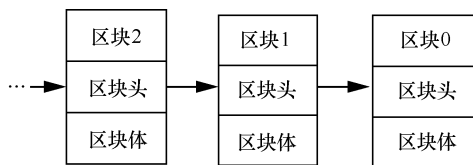


图3 区块链结构

区块链上的点对点网络存在很多簇, 这些簇由节点组成, 簇首节点和簇内节点数目时刻都在发生变化。区块链技术的小世界模型的P2P网络能够保证区块链网络的稳定性, 同时使交易数据具有完整性和一致性。

非对称加密算法用于区块链中交易的数据加密过程和签名过程, 能够保证区块链网络的安全以及用户的隐私保护, 图4为区块链中交易过程。其中, 公私钥的产生利用了密码学中的SHA256散列算法、Base58转换以及secp256k1椭圆曲线乘法签名算法等。区块链中的交易过程如下。假设当前进行的是第2个交易, 用户1为交易的发送者, 用户2为交易的接收者; 数据的加密流程是将交易1和用户2的公钥进行Hash运算获得数据A, 然后用用户1的私钥对数据A签名获得加密后的数据。数据的验证流程为: 采用用户1的公钥对加密后的数据进行解密获得数据B, 将数据A与数据B进行对照, 若数据A和数据B相同, 则证明

用户1与用户2要进行此笔交易, 且发送者是用户1, 接收者是用户2。

Merkel根结构如图3所示的区块体部分, 4个叶子节点需要进行2层Hash算法, 8个叶子节点需要进行3层Hash算法, 16个叶子节点需要进行4层Hash算法, 以此类推, 2048个叶子节点需要进行11层Hash算法, 65535个叶子节点需要进行16层Hash算法, 由上面的数据可以看出, 当叶子节点由4个变为65535个时, 散列算法的层数由1层变为16层, 这为查找某个元素是否存在提供了便利的条件。

共识机制解决了交易在没有完全信任的第三方的情况下, 各个节点如何达成一致意见的问题。目前提出的共识机制有PoW共识机制、PoS共识机制、DPoS共识机制、拜占庭共识机制。

智能合约层包括脚本语言和执行脚本语言的虚拟机, 能够运行图灵完备的脚本语言。智能合约层保证了用户在区块链技术下安全地进行交易, 程序员可在智能合约层编写代码规定交易进行的条件以及结果。

## 4 基于区块链的路况预警方案

### 4.1 车载自组织网络中的区块链

根据车载自组织网络路况报警需求以及比特币中传统的区块链区块结构, 得出适用于车载自组织网络路况报警的区块结构, 车载自组织网络中的区块链称为路况信息链, 车辆节点

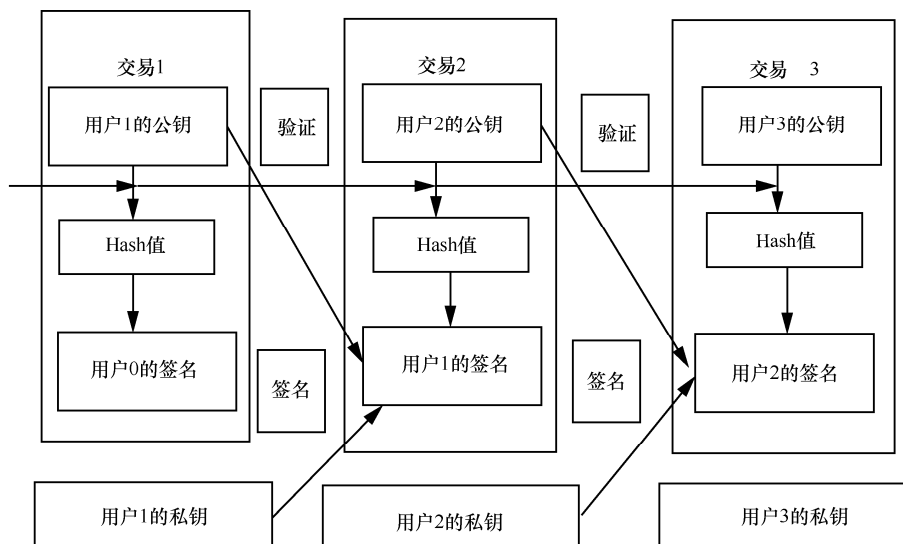


图4 区块链中交易过程



适应车载自组织网络路况信息时刻都在变化的特性。

当路况信息链中全部的路况信息块都失效时，此条路况信息链将不再代表此时此刻此条路段的路况，此条路况信息无效。路况信息块的消亡依靠车载自组织网络中区块结构的路况信息块消亡倒计时，每个路况信息块的消亡倒计时初始值设为 5，每隔 1 min 路况信息块倒计时值减小 1，当倒计时值减小为 0 时，该路况信息块消亡。由于车载自组织网络中车辆和路况变化较快，因此，将路况信息链的消亡时间设为 20（即一条路况信息的有效时间为 20 min，超过 20 min 此条路况信息不再有效）。一条路况信息链的消亡时间用  $TCDead$  表示，这条路况信息链上所有路况信息块的消亡总时间用  $TBDead$  表示， $n$  表示车辆的数量，且  $TBDead=n*$ 倒计时，表 1 为路况信息链的消亡时间和路况信息块的消亡总时间关系。当  $TBDead>TCDead$  时，表明有很多辆车都发送同样的路况，该路况消息是有效的；当  $TBDead\leq TCDead$  时，表明很少的车辆发送同一条路况，该路况消息是无效的。因此，要想保证车辆节点发送的路况信息可信、有效，则应满足  $TCDead=TBDead=n*$ 倒计时，由于倒计时为固定值 5， $TCDead$  最大值为 20，故发送路况信息的车辆节点至少为 4（即至少有 4 辆车发送同一条路况信息，此条路况信息才真实有效）。

表 1 路况信息链的消亡时间和路况信息块的消亡总时间关系

| 路况信息链的消亡时间和路况信息块的消亡总时间关系 | 路况信息有效性 |
|--------------------------|---------|
| $TBDead>TCDead$          | 有效      |
| $TBDead\leq TCDead$      | 无效      |

## 5 仿真实验与分析

Hyperledger Fabric 联盟链具有安全、隐私、可监管等特性，适用于数据只希望在一部分区域内共享的项目开发。车载自组织网络中的路况信息只需要广播给网络内部的车辆节点，从而维护车载自组织网络中的交通，车载自组织网络中的每条路况信息均可看成是一笔交易，因此，本文采用 Hyperledger Fabric 联盟链技术平台对车载自

组织网络中基于区块链技术的路况报警方案进行仿真实验。图 6 为 Fabric 联盟链技术平台架构，Fabric 联盟链技术平台包括：证书服务、客户端、Peer 节点以及共识网络（由许多 orderer 节点组成）。图 7 为 Fabric 联盟链的交易过程。交易过程包括：客户端提案、模拟交易、签名、排序服务、验证交易、将交易写入账本。

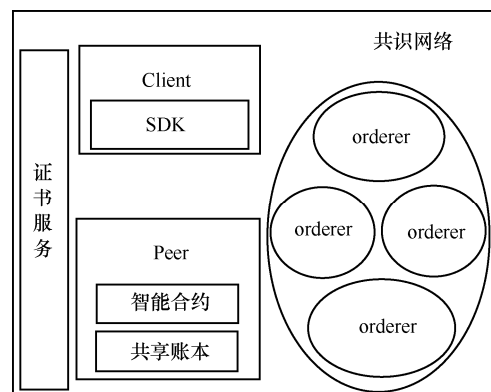


图 6 Fabric 联盟链技术平台架构

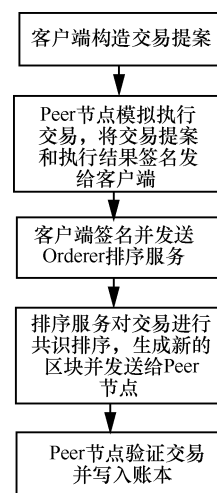


图 7 Fabric 联盟链的交易过程

### 5.1 在 Fabric 联盟链中仿真车载自组织网络中基于区块链技术的路况预警方案

假设存在 FirstRoad、SecondRoad、ThirdRoad、FourthRoad 路段，根据 3.2 节阐述的路况信息有效的条件可知，每条路段若发生拥堵或者交通事故时，此段路上至少有 4 辆车发送相同路况信息，现假设每条路段各有 10 辆车（允许 10 辆车中至多存在 6 辆故障车），此时，FirstRoad 出现拥堵，在 Fabric 联盟链上的仿真步骤如下。

1) 用 Go 语言编写链码 chaincode002.go，链

码中的主要内容如下。

第1步,采用 Import 方法引入依赖包“fmt”“shim”“peer”。

第2步,构建 FirstRoad Congestion 结构体。

第3步,采用 Init 方法进行初始化。

第4步,构建 Invoke 方法实现 FirstRoad Congestion (第一条路拥堵)路况信息。

2) 将链码部署到 Fabric 网络中。打开3个终端,第1个终端用于启动网络,第2个终端用于编译启动链码,第3个终端用于操作链码。

## 5.2 仿真结果与分析

在 Fabric 联盟链上的运行结果如图8所示。实验结果第13行显示 FirstRoad Congestion (第一条路拥堵),与理论结果一致。

上述实验表明,将区块链应用于车载自组织网络中能够对一条真实的路况信息达成共识,即实现车载自组织网络中路况预警。在车载自组织网络中, Fabric 网络中的客户端模拟用户,当用户发现某条路发生拥堵或者交通事故时,及时按动车内的报警按钮; Fabric 网络中的 Peer 节点模拟车辆节点,当某段路附近的车辆节点收到用户发来的路况信息时,此段路区域内的车辆节点开始挖矿并将路况信息打包成区块; Fabric 网络中的证书服务模拟车辆管理中心,车辆想要加入车载自组织网络必须到车辆管理中心进行注册且得到管理中心颁发的签名和公私钥; Fabric 网络中的共识网络模拟固定单元组成的网络,维护路况信息链中区块的有序生成区块链。因此,在 Fabric 联盟链上部署 FirstRoad Congestion 相当于车载自组织网络中车辆节点对于某条路况信息达成共识。

## 6 结束语

综上所述,相对于其他方法的路况报警方案,车载自组织网络中基于区块链技术的路况预警方案的优点如下。

1) 不需要可信任的第三方就可以使车载自组织网络中车辆发送的路况信息达成共识并完成验证。

2) 由于区块链是一个分布式账本,因此,车载自组织网络中每个车辆节点都存有路况信息链这个账本,路况信息具有防篡改和可追溯性。

未来区块链技术在车载自组织网络中的应用,主要包含以下几个方面。

1) 寻找好的激励机制使车辆节点更加积极地发送路况信息。

2) 当车辆节点受到攻击时,如何保证路况信息的正确性。

3) 开发出基于区块链技术的 APP 应用于车载自组织网络。

## 参考文献:

- [1] QI S M. Research on urban road traffic congestion evaluation method and control strategy[D]. Kunming: Kunming University of Science and Technology, 2016.
- [2] SINGH S, NEGI S, VERMA S K. VANET basedp-RSA scheduling algorithm using dynamic cloud storage[J]. Wireless Personal Communications, 2017(6):1-21.
- [3] CIRNE P, ZÚQUETE A, SARGENTO S. TROPHY: trust-worthy VANET routing with group authentication keys[J]. Ad Hoc Networks, 2018, 71:45-67.
- [4] ZHONG H, HUANG B, CUI J, et al. Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks[J]. IEEE Access, 2017(99):1-5.
- [5] WANG L M, LI T, CHEN L. Vehicle network structure and security

```
root@9494a3836ec3:/opt/gopath/src/chaincode# peer chaincode query -n mycc -c
 '{"Args":["get","str"]}' -C myc
2018-05-29 13:13:02.519 UTC [msp] GetLocalMSP -> DEBU 001 Returning existing local MSP
2018-05-29 13:13:02.520 UTC [msp] GetDefaultSigningIdentity -> DEBU 002 Obtaining default signing identity
2018-05-29 13:13:02.520 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 003 Using default escc
2018-05-29 13:13:02.520 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 004 Using default vsc
2018-05-29 13:13:02.521 UTC [msp/identity] Sign -> DEBU 005 Sign: plaintext: 0AA9000A6100031A0C0006C297030510...607963631A0A0A036765740A03737472
Query Result: FirstRoad Congestion
2018-05-29 13:13:02.563 UTC [main] main -> INFO 007 Exiting....
root@9494a3836ec3:/opt/gopath/src/chaincode#
```

图8 实验结果

- based on vehicle identity[J]. Journal of Network and Information Security, 2016, 2(2):41-54.
- [6] ZHANG R F. A survey of research on vehicle self-organizing network communication technology[J]. Journal of Automotive Engineering, 2014, 4(2):79-85.
- [7] ZHANG S. Blockchain technology principles, applications and recommendations[J]. Software, 2016, 37(11):51-54.
- [8] NOVO O. Blockchain meets IoT: an architecture for scalable access management in IoT[J]. IEEE Internet of Things Journal, 2018(3): 1184-1195.
- [9] KUZMIN A. Blockchain-based structures for a secure and operate IoT[C]//IEEE Internet of Things Business Models, Users, and Networks. 2018.
- [10] ZHI Q H, XIONG Y S, YAN X Z, et al. A decentralized solution for IoT data trusted exchange based-on Blockchain[J]. IEEE International Conference on Computer and Communications, 2017(3): 1180-1184.
- [11] CHA S C, CHEN J F, SU C, et al. A Blockchain connected gateway for ble-based devices in the Internet of things[J]. IEEE Access, 2018(99):1-7.
- [12] YONG Z, SONGYANG W, BO J, et al. A Blockchain-based process provenance for cloud forensics[J]. IEEE International Conference on Computer and Communications, 2017(3): 2470-2473.
- [13] YANG C, CHEN X, XIANG Y. Blockchain-based publicly verifiable data deletion scheme for cloud storage[J]. Journal of Network & Computer Applications, 2018, 103-112.
- [14] XIA Q, SIFAH E B, ASAMOAHA K O, et al. MeDShare: trust-less medical data sharing among cloud service providers via Blockchain[J]. IEEE Access, 2017, 5(99):14757-14767.
- [15] KHAQQI K N, SIKORSKI J J, HADINOTO K, et al. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application[J]. Applied Energy, 2017, 209:8-19.
- [16] POP C, CIOARA T, ANTAL M, et al. Blockchain based decentralized management of demand response programs in smart energy grids[J]. Sensors, 2018, 18(1):162-183.
- [17] GUO W J. Research on message transmission problem for security applications in Internet of vehicles[D]. Hefei: University of Science and Technology of China, 2014.
- [18] ZHU Y, GAN G H. Safety research in key technologies of Blockchain[J]. Information Security Research, 2016, 2:1090-1097.
- [19] AN Q W. Research and application of key technology of decentralized transaction based on Blockchain[D]. Shanghai: Donghua University, 2017.
- [20] HUANG X F, XU L, YANG X. A cloud computing electronic forensics model of Blockchain[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(6):1-6.

## [作者简介]



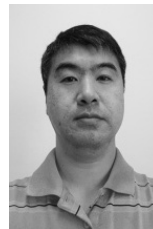
**李春燕**（1995-），女，天津人，北京交通大学硕士生，主要研究方向为车载自组织网络、隐私保护、区块链。



**赵佳**（1980-），女，内蒙古呼和浩特人，博士，北京交通大学副教授，主要研究方向为网络空间安全、可信计算、隐私保护。



**刘吉强**（1973-），男，山东海阳人，博士，北京交通大学教授、博士生导师，主要研究方向为密码学、可信计算、隐私保护技术。



**张强**（1980-），男，河北石家庄人，主要研究方向为网络空间安全、区块链、态势感知。



**韩磊**（1983-），男，内蒙古呼伦贝尔人，博士，信息保障技术重点实验室博士后，主要研究方向为分布式非对称密钥管理、区块链、态势感知。