区块链中非确定性车辆团队移动众包策略的研究与实现

Research and Implementation of Mobile Crowdsourcing Strategy for Non-deterministic Vehicular Team-Cooperation in Blockchain

工程领域：计算机技术
作者姓名：冯欣蕾
指导教师：陈世展　副教授
企业导师：孙提　高级工程师

答辩日期	2020年6月21日		
答辩委员会	姓名	职称	工作单位
主席	喻梅	教授	天津大学智能与计算学部
委员	邵鹏	高级工程师	恩智浦半导体有限公司
	王建荣	副教授	天津大学智能与计算学部

天津大学国际工程师学院
二〇二〇年六月

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作和取得的研究成果，除了文中特别加以标注和致谢之处外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得 **天津大学** 或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

学位论文作者签名：冯欣蕾 签字日期：2020 年 6 月 28 日

学位论文版权使用授权书

本学位论文作者完全了解 **天津大学** 有关保留、使用学位论文的规定。特授权 **天津大学** 可以将学位论文的全部或部分内容编入有关数据库进行检索，并采用影印、缩印或扫描等复制手段保存、汇编以供查阅和借阅。同意学校向国家有关部门或机构送交论文的复印件和磁盘。

(保密的学位论文在解密后适用本授权说明)

学位论文作者签名：冯欣蕾 导师签名：陈世展

签字日期：2020 年 6 月 28 日 签字日期：2020 年 6 月 28 日

摘　要

随着智能城市的发展，车辆互联网（IoV）引起了研究者们的广泛关注。智能车辆可以通过多方合作组建车辆团队，在智慧城市中执行移动众包任务。如何组建车辆团队建立安全的模型以实现最大的社会福利，成为车辆移动众包活动中的巨大挑战。尽管目前的研究已经提出了一些移动众包模型，但是很少有人关注实时车辆团队合作。此外，交通压力带来的拥堵为人们生活带来不便的同时也带来了机遇，闲时团队资源的有效利用成为研究者们一个新兴的研究兴趣点。

针对以上问题，本文提出了第一个以闲时计算车辆团队为最小任务划分单位的移动众包安全模型，称为基于区块链的非确定性团队合作感知（BNTC）模型。实时群智感知任务可以由群智感知平台分配给一个或多个车辆团队，以车辆团队为最小划分。系统通过团队的属性选择合适的团队实现社会福利最大化。本文基于逆向拍卖的 VCG 机制，设计了任务分配算法和奖励定价算法。为了确定任务的分配规则，本文提出了一种基于背包算法的优化逆向拍卖机制，该机制称为 WTS 算法，其中考虑了任务完成率，社会成本和选择的团队数量。对于奖励定价机制，本文考虑信誉因素对关键定价的影响，提出了 CTP 算法，并且提出至关重要团队的概念。这两种算法可以保证模型最大化社会福利。此外，本文还提出了一个基于区块链的通用框架，以解决信任问题和安全挑战。基于理论分析和大量的模拟，实验证明了该模型的性能优于传统算法，并且可以实现最大的社会福利。以太坊的实验表明该模型可以在合理的成本内运行。

关键词： 智慧城市，区块链，移动众包，团队感知

ABSTRACT

With the development of smart cities, the Internet of Vehicles (IoV) has attracted extensive attention from researchers. Intelligent vehicles can form vehicle teams through multi-party cooperation to perform mobile crowdsourcing tasks in smart cities. How to form a vehicle team to establish a safe model to achieve maximum social welfare has become a huge challenge in the mobile crowdsourcing activities of vehicles. Although the current research has proposed some mobile crowdsourcing models, few researchers pay attention to real-time vehicle teamwork. What's more, the congestion caused by traffic pressure brings inconvenience to people's lives and also brings opportunities. The effective use of leisure team resources has become an emerging research interest for researchers.

In response to the above problems, the mobile crowdsourcing security model which uses the leisure computing vehicle team as the minimum task division unit is proposed first. We named the model as the blockchain-based non-deterministic team cooperation perception (BNTC) model. Real-time tasks can be assigned to one or more vehicle teams by the BNTC model. The BNTC model selects the right teamset through the attributes of the team to maximize social welfare. Based on the VCG mechanism of reverse auction, we design a task allocation algorithm and a reward pricing algorithm. In order to determine the task allocation rules, we propose an optimized reverse auction mechanism based on the knapsack algorithm (WTS), which takes into account the task completion rate, social costs and the number of selected teams. For the reward pricing mechanism, we consider the influence of reputation factors on key pricing, named as CTP algorithm. These two algorithms can ensure that the model maximizes social welfare. In addition, we also propose a general framework based on blockchain to solve trust problems and security challenges. Based on theoretical analysis and a lot of simulations, experiments prove that the performance of the model is better than traditional algorithms.We can achieve maximum social welfare. Ethereum's experiments show that the model can be operated at a reasonable cost.

KEY WORDS: Smart City, Blockchain, Mobile Crowdsensing, Team Perception

目 录

第 1 章 绪论

1.1 研究背景及意义

随着创新型智能交通系统的发展，互联网将在智能交通中发挥重要作用。截止 2020 年，全球将有 75% 的汽车可以搭载互联网[1]。车辆拥有更大容量的数据存储单元、无线网络接口、环境传感器设备、更先进的通信模块以及智能化用户接口，可以提高驾驶安全性，便利性和满意度，提供更好的驾驶体验[2]。具有先进设备的车辆和驾驶员形成车辆网络（Internet of Vehicle，IoV）具有强大的信息处理能力。为了有效利用车辆计算资源，国内外科研团队已经提供了一些车辆移动众包研究（Mobile Crowdsensing，MCS），利用车辆的处理能力完成某些任务[3]。车辆众包，作为 MCS 的一种，可以提供比普通众包更经济的众包服务。众包平台根据车辆意愿和投标价格向参与该系统的车辆（工人）发出诸如路况检测，噪声和空气污染检测，广告分发，存储计算等任务[4][5][6][7] 。但是对于大规模计算问题，单辆车辆的处理能力有限，一些计算任务所需的资源需要多辆车辆联合才能满足。然而目前的车辆 MCS 任务的计算聚合是单个车辆计算能力的简单聚合，没有研究显示满足相同局域网中多辆车联合达到的某种计算能力的效果，这使得移动众包的计算任务类型十分有限。因此，如何通过需求自适应方法以规模联合计算能力来适应不断增长的通信和众包任务计算需求仍然是一个悬而未决的问题。

一种解决方案是利用交通系统中尚未充分利用的实时性规模计算能力。据 2018 年的统计，北京等一线城市中，堵车所用时间占通勤时间的一半以上。堵车给车辆司机以及乘客造成很大的困扰，把这种由社会活动现象引起的不便转化为一种优势利用的模式，是一个值得思考的研究方向。堵车，即无计划的车辆聚集行为，形成车辆团队，从硬件角度说，是多个车载计算硬件形成强大的计算资源池。采取合理的激励措施对具有实时性的的车辆计算资源池的利用将成为车辆群智感知模型的重要课题。

为 IoV 建立安全的 MCS 机制，主要面临三个挑战：一是如何为移动众包任务确定合理的工人团队，利用最低的成本提高任务的完成率。二是如何为工人团队确定合理的支付报酬，最大程度地提高定价的合理性和工人的满意度。常用的激励机制有双重拍卖或组合拍卖等。但这些类型的拍卖方法需要多次迭代确认，

多次交互造成延时较长。反向拍卖策略的逻辑关系中主导买家市场，卖家提出竞价报价，比较适合实时车辆群智感知任务的交易。因此，制定有效的车辆群智感知分配定价策略是目前的车联网应用的主要研究方向之一。三是如何建立确保用户隐私和数据完整性的安全系统框架。

区块链作为近几年新兴的技术，可以提供公开透明、安全可信的交易环境。区块链是一种拥有去中心化、保护用户隐私、维护数据安全特性的一种结构性网络。区块链本身的特性可有效避免车联网乃至物联网中存在的数据存储安全威胁，身份泄露等隐患。在车联网众包问题中，利用区块链平台首先可以去中心化，消除平台的权威控制。其次，区块链平台可有效增强公平性，防止第三方作恶。区块链平台可增强对发布任务方和做任务方的约束力，并且保证部分信息公开透明，防止出现做任务方的工作成本与获取的收益不一致的情况。因此，近年来有比较多的研究工作考虑将 MCS 系统与区块链相结合以提高众包系统的安全性。

1.2 国内外研究现状

激励机制用于 MCS 中选择合适的工人并为承担不同任务的工人确定合理的报酬，确保最大限度地提高社会福利[8][9]。一些 MCS 任务需要至少一辆车可以完成。Wang[10]提出了一种基于图的解决方案，将消息传播的最小延迟最大覆盖和最小开销最大覆盖转换为路由搜索问题。并提出了基于贪婪递归优化的方法，以分治模式解决以上问题。基于位置的任务分配需要部署分散的多个检测点。路径覆盖是主要考虑因素。Gao[11] 考虑了不同的车辆轨迹以及行驶路线的不确定性建立 MCS 任务模型，其中每个任务可以由多辆车辆合作完成。Chen[12] 提出了一种车辆追踪系统，多个节点协调通过多角度拍照来共同跟踪正在行驶的车辆，来完成定位速度确定等任务。但是，目前现有的工作无法处理需要在特定时间段快速协调多个工人完成任务。对于实时协作 MCS 的工作，Yin[13] 研究了一种基于时间窗口的方法来管理紧急任务。该方法在发生紧急任务时选择空闲车辆。此外，MCS 任务的高质量驱动[14]也是近年来的一个重要研究方向。文章[14]提出了一种基于质量驱动的拍卖激励机制，但是该模型需要根据提前上传抽象数据参数判断数据质量保证数据的可靠性。以上 MCS 激励机制的团队模型设计中由于任务类型的不同根据不同方法确定候选车辆以形成车辆组，但缺乏对 MCS 的大规模联合计算资源的关注。

为了满足智慧城市中智能设备进行大规模数据收集、运输和处理的需求，IoV 可以用作经济高效的方案之一。在 IoV 系统中，车辆可以成为感测网络内的智能移动节点。Taleb[15] 等人提出了一种适用于长期演进型车辆的调度程序，

该调度程序适用于车载自组织网络（VANET）中的安全应用。Xuet[16] 根据北京市的车辆实验，提出了一种基于车辆自组织网络的时延和覆盖率优化数据收集（LCODC）方案。方案中增加车辆之间的 V2V 传输，提高数据收集效率。基于区块链的 IoV 系统中的安全隐私问题，研究者们已经提出了许多方法来解决当 IoV 与区块链结合时与IoV 相关的安全性和隐私问题[17]。名为 Merkle Patricia Tree （MPT）的一种数据结构用于扩展区块链结构，以允许对 VANET 中的车辆进行私有身份验证[18]。在这种方法中，车辆可以创建多个证书确保有条件的隐私。Lu[19] 使用了两种类型的区块链来隐藏真实身份和公共密钥之间的联系。Ma[20] 提出了一种灵活且可配置的区块链架构。Yao[21]实现了跨数据中心身份验证，并允许用户请求更改其假名以保护个人隐私。以上身份隐私安全方案都是可追溯的，不能有效保证身份的安全性。本文将使用匿名身份证书的方案有效保护用户的身份隐私问题。

综上所述，现有研究缺乏能够利用实时联合计算能力并同时保证安全的 MCS 框架。现有的大多数 MCS 框架都将子任务分配给特定的车辆而不考虑以团队为单位进行划分，这导致执行大型计算任务将产生巨大的时间和资源成本。此外，对规模性计算资源的利用是减少资源浪费的一种有效途径，但关于这方面的研究少之又少。

1.3 主要工作及贡献

为了解决大型计算任务的 MCS 分配与设计，并有效利用实时车辆团队的移动资源，本文设计了一种基于区块链的非确定性车辆团队合作众包模型（Blockchain-based Nondeterministic Teamwork Cooperation，BNTC）。本研究的主要贡献如下:

1）本文设计了一种基于团队协作的非确定性群智感知模型——BNTC。实时群智感知任务可以由群智感知平台分配给一个或多个车辆团队，以车辆团队为最小划分。配备智能设备的车辆组成团队来完成任务。基于团队合作的 MCS 模型可以通过团队的属性选择合适的团队来提高任务的完成率。

2）本文基于逆向拍卖的 VCG 机制，设计了任务分配算法和奖励定价算法。为了确定任务的分配规则，本文提出了一种基于背包算法的优化逆向拍卖机制，该机制称为 WTS （Winning Teams Selected）算法，其中考虑了任务完成率，社会成本和选择的团队数量。对于奖励定价机制，本文考虑信誉因素对关键定价的影响，提出了 CTP （Credit-based Team Payment）算法，并且提出至关重要团队的概念。这两种算法可以保证模型最大化社会福利。

3）本文为非确定性的车辆群智感知模型提出了一个基于区块链的框架。区

块链作为底层系统框架，关键服务由智能合约处理[22]。该框架可以确保用户数据的隐私性和系统的数据完整性。工人可以匿名工作并接收付款，付款的公平性得到保证。

1.4 论文组织结构

本文共有五章内容，每部分如下所示：

第一章为绪论。本章主要指出基于车辆的 MCS 的研究背景以及意义，介绍了目前国内外对于车联网、区块链、群智感知的研究现状。最后对本文的研究主要内容整体简要介绍。

第二章为相关工作概述。主要包括三大部分：首先介绍车联网相关软硬件基础，然后介绍关于群智感知的相关理论，最后介绍区块链的相关技术包括整体框架、智能合约、数字签名等理论。

第三章为系统模型介绍。首先创新性地研究并设计了基于区块链车辆团队的移动众包模型 BNTC，介绍该模型的运行方式，然后提出了获胜团队选择算法（WTS）和基于信用的团队付款算法（CTP），并进行算法的合理性、可行性等分析。最后对该模型进行理论安全性分析。

第四章为实验部分，首先介绍数据集的来源，对获胜团队选择算法（WTS）和基于信用的团队付款算法（CTP）进行对比实验验证和分析，最后对算法在以太坊中的性能进行实验与分析。

第五章为总结与展望。对本文提出的模型以及算法进行总结，并提出了下一步的研究内容。

第 2 章　相关工作概述

对于解决如何有效利用闲时车辆团队的计算能力，合理设计一种基于区块链的移动众包策略是有效的解决方案之一。本章主要介绍移动众包相关概念，激励机制以及车联网区块链的相关背景，为后文的研究与设计提供理论基础。

2.1　车联网 IoV

为了更好地介绍 IOV，首先要介绍 VANET。车辆自组织网络的基本原理是将车辆视为移动节点，该节点与其他车辆连接，创建车辆网络。随着车辆不断进入网络的定义范围之内和之外，车辆分别进行连接和断开连接。车辆通过自组织形式相互连接，这些自组织最终形成了称为“车辆自组织网络”的无线网络，被归为 MANET 的子组（移动自组织网络）。

VANET[23]包含两个大致方向[24]：V2R 通信（也称为车辆到路边通信）和 V2V（车辆到车辆）通信，它被认为是互联网传输系统的重要组成部分。VANET 中的每辆车都将变成一个移动节点，从而创建一个广泛的网络，最终车辆之间会相互连接。该网络本质上是动态的，在这种情况下，由于车辆的运动而导致的车辆不在网络范围之内并断开连接，从而使其他车辆可以连接以创建移动互联网。IoV 是车辆与车辆（V2V）通信的扩展。相互连接的车辆进行远程信息处理和移动互联网传输，构成车辆网络。智能车辆，可以定义为通过整合车辆和驾驶员来创建的一个单元，通过利用诸如群计算、认知计算、深度学习、人工智能等重要技术实现单元智能化。因此，IoV 的重点是智能地整合车辆、事物、人和环境，并创建一个可以为特定提供服务的网络，这些服务可以进一步扩展到一个城市乃至整个国家。IoV 可以用作经济高效的替代方案，以满足智慧城市环境中智能对象进行大规模数据收集、运输和处理所需的需求。与传统的无线传感器网络（WSN）相比，IoV 内的车辆节点不受电池电量和信息处理限制的资源约束[25]。在 IoV 内，车辆充当感测网络内的移动智能节点或对象。智慧城市环境中的每个车辆对象可以扮演四种角色:（1）车辆对象充当节点和对等点，在 IoV 自身内部建立并维护网络连接；（2）车辆对象充当客户端，消费来自 IoV 和 Internet 的服务；（3）车辆对象充当数据收集器或“数据产生源”，将数据从其他智能对象收集并传输到智慧城市内的数据中心；（4）车辆对象充当分布式计算资源，以

补充（较小）智能对象内受约束的信息处理资源。

2.2 移动众包理论基础

智能手机、智能电器、智能汽车等的智能化便携设备的发展，在一定程度上促进移动众包应用程序的迅猛发展。移动众包（MCS），可为人们解决不同类型或规模的问题。移动众包的相关理论研究和发展，可为移动众包应用程序的使用提供技术理论支持。

2.2.1 众包的概念

“众包”（Crowdsensing），又称群智感知，最早由 JeffHowe 在 2006 年美国的《连线》杂志上提出。众包本意指在企业工业中的任务分配定价方式。众包这一理念的产生，对生产模式产生了颠覆性的影响。很快，这种工业生产里创新理念被科研人员引用到互联网平台中。在互联网众包平台中，一些任务在互联网众包平台上以某种价格外包给一个或者多个任务承担者解决。一个众包行为的发生，需要众包平台、任务发布者、任务承担者（Worker）至少三个角色组成[26]。基本角色如图 2-1 所示，目前，国内外已发布的正在运行众包平台网站包括亚马逊的 Mechanical Turk（AMT）等。众包平台可以为任务发布者和任务承担者提供交易场所，通过某种竞价定价机制，切实保证双方的利益，并且平台从交易中获取一定的处理费用作为对平台的报酬。此外，任务承担者往往具有完成任务的能力，在激励机制的合理刺激下，愿意花费时间和资源参与任务中来，为了获取小额费用或者为了累积经验未来获得报酬。

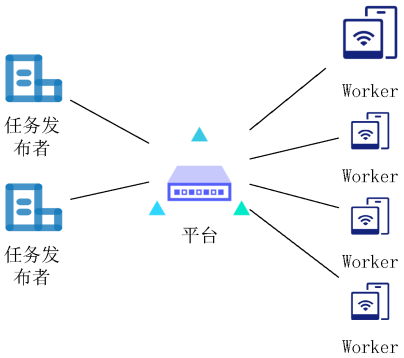

图 2-1　　众包基本角色

2.2.2 IoV中的移动众包

目前，通过向随机人群开放征集任务服务，被称为众包。那么，改变普通众包的工人主体，将拥有先进智能传感器的可移动设备作为任务承担者进行数据采集收集或者认知计算，被称为移动众包。目前已有的移动众包平台包括闲猫平台、微差事等。电子传感器设备，无线网络以及微型计算机的计算能力的迅速发展，使得移动众包工作者可以是从起初的智能手机到现在的智能汽车等拥有一定计算能力和存储能力的设备。平台或信息发布者通过从不同位置的移传感器节点收集、汇聚和分析信息，完成移动众包任务。常见的任务有空气、交通检测型任务，广告传输型任务、采集型任务或者计算型任务。

2.2.3 移动众包中的激励机制

移动众包的本质是，通过互联网平台，集合请求贡献计算力且有能力的参与者来完成某件任务。参与者的规模以及能力可对数据的质量直接造成影响。对于任务承担者而言，参与贡献计算能力的同时会伴随着一些问题使得拥有可完成任务的节点不积极参与到任务中来。因此，总结出节点不积极参与任务的条件如下文所示：

1)客观条件：车辆虽有参与任务的计算能力，但资源处于被占用中，资源空闲时间不足，无法在限定的时间内提供服务。

2)主观条件1：由于车辆性能、网络环境等因素，使得车辆承担任务时损耗电量、内存等成本消耗较高，造成节点本身不具备较强的竞争力。同时，操作者也会损失一定的时间等精力。人力成本和设备成本综合较高，使得具有理性的工作者无意愿或意愿较小的参与到任务中。因此，为了提高节点的参与度，设置合理的激励机制是必要的。

3)主观条件2：任务承担者需要考虑到，如果自己参与到任务中，是否能保证车辆数据安全，即，隐私的保护问题。当任务承担者参与执行任务时，贡献的数据或计算能力可能与位置、时间、用户信息等有关。因此，用户隐私的安全级别可影响用户的参与度。

激励机制的制定应该充分考虑到任务承担者的条件，消除或弥补任务承担者的担忧，提高用户的参与度和诚实度。如果大多用户提交虚假数据，虚假报价，这将影响众包事务的质量，产生较大的负面影响。因此，合理的激励机制的研究是模型具有合理性、可行性的前提。

2.2.4 移动众包中的激励模型

在移动众包问题中，激励模型的选择决定移动众包的合理性[27]。目前激励模型的奖励方式主要有：娱乐奖励、信誉值奖励、报酬奖励等。其中，报酬奖励又分为基于平台的奖励以及基于用户的奖励。激励模型主要分为两种方案：博弈论方案和激励机制方案。博弈论的方案主要有非合作博弈、相互议价的博弈和基于斯坦克尔伯格（Stackelberg）模型[28]。博弈论方案的目标是，通过任务发布方和任务承担方的博弈，达到纳什均衡，从而确定最大收益的分配方案。以拍卖机制为主的激励机制包括：双向拍卖[29]、反向拍卖[30]、VCG 拍卖（Vickrey-Clarke-Groves）等拍卖方式。双向拍卖是买家卖家双向主导，多轮商讨得到最终结果，多用于多方一对一协调模式，即多个买家多个卖家，最终找到达到社会福利最优或者极优的一对一匹配模式，如图 2-2 所示。反向拍卖是买家处于主导地位，属于买方市场。买家从众多的卖家中挑选一家或者多家作为接收任务胜利者，达到社会福利最优状态，如图 2-3 所示。

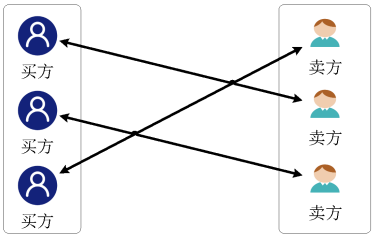

图 2-2　双向拍卖

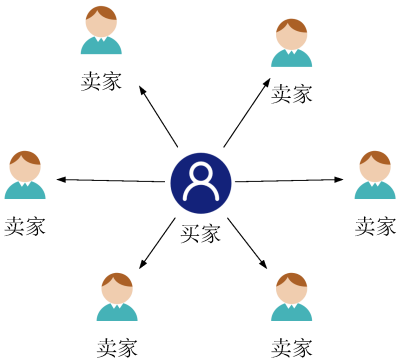

图 2-3　反向拍卖

2.2.5 VCG 机制

维克瑞拍卖机制（第二价格密封拍卖）最早出现在维克瑞（Vickrey）发表的《反投机、拍卖与竞争性密封》一文中，这篇论文在 1961 年发表[31]，被称为有效激励机制的创世之作。基础理念为：暗拍中，出价最高者获胜，用第二高出价支付获胜者奖励。由于报酬获得与自身无关，这种方案更容易获取真实价格。这种方式作为 VCG 拍卖机制的基本理念，将拍卖问题定义为两个部分：分配方案和支付方案。分配方案中，假设所有参与竞价者都是诚实可信的。分配方案可以有多种，根据系统的设计与需求决定分配方案，使社会福利最大化。支付方案的设计，要起到对激励参与者的诚实性与投标的真实性的约束作用，在分配方案中的假设成立。因此采用借助任务承担者的外部性确定价格支付方案，即，在任务承担者 i 为获胜者之一，在不选择 i 的情况下，重新选择获胜的任务承担者，根据新选择的任务承担者的社会福利确定对 i 的支付方案。到 1971 年，克拉克[32] 在公共物品的有效供给问题中使用了维克瑞拍卖机制，并根据公共物品提出了在占优战略中如何实施有效配置的机制。两年后，格罗夫[33] 将该机制从特殊问题转为一般化解决方案。三人在如何有效分配问题中贡献突出，由此以三人按年份顺序命名——Vickrey-Clarke-Groves 机制，简称 VCG 机制。

报酬奖励是移动众包问题常用的激励机制奖励模式，信誉奖励在移动众包问题中可以促进节点的趋优性，鼓励节点做出真实的行为。此外，反向拍卖模型更能提高移动众包问题的解决效率。因此，本文的激励机制设计主要基于 VCG 机制，以拍卖的方式进行。

2.3 区块链基础技术

上一节提到，任务承担者是否有意愿参加到任务中，要考虑安全隐私的问题。因此，安全隐私的有效保护是移动众包任务需要解决的难题。区块链的产生与发展，对解决移动众包中的安全隐私有极大的帮助。本节主要介绍区块链的相关理论知识。

2.3.1 区块链基本结构

最早，中本聪（Satoshi Nakamoto）提出了区块链这一概念，在相互不可信的前提下，提出了一种去中心化、相互信任的分布式数据记录，这一应用首先在比特币（Bitcoin）中实现[34]。目前，区块链的体系架构仍在随着研究的发展而变化，基础分层自底向上可以分为四层：存储层、网络层、扩展层和应用层[35]。

整个架构如图 2-4 所示：

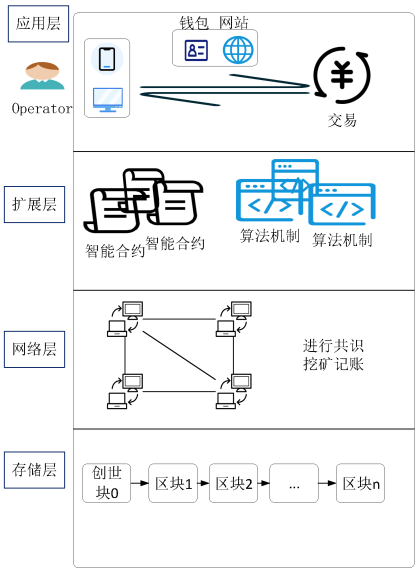

图 2-4　　区块链基本框架[35]

(1) 存储层主要涉及数据的存储，主流的两种存储方式是比特币的默克尔树（Merkle Tree）[36]和以太坊中的帕特里夏树（Merkle Patricia Tree，MPT 树）[37]。

默克尔树（又叫哈希树），可以对大规模数据的树形结构数据进行快速检测。默克尔树以二叉树为主，叶子是数据块的哈希值，非叶子节点是左右孩子节点内容的哈希。因此，叶子节点的变化会使其所有的父节点的哈希值改变，最终导致成根节点哈希值的变化。

MPT 树在默克尔树的基础上，融合了 Tire 树的特点（Tire 树，前缀键相同表示树根到对应值的路径相同），在以太坊中用于存储和管理用户的交易、状态等数据的加密信息。由于以太坊的状态树需要经常查询，因此，与不便于查询的默克尔树相比，MPT 树的有点如下：

- MPT 树可在增删改节点后，较快计算出树的根值。
- MPT 树深度相对较小，查询和更新比较方便。
- MPT 树的根值只与数据有关，与节点的更新时间无关。

(2) 网络层包括系统的组网方式、消息传播、数据验证、共识等。网络层的组网方式主要采用对等式网络（Peer-to-Peer，P2P）[38]，网络中每个节点都是平等的，每个节点都会参与路由、验证区块、等功能。区块链中的节点可分为全节点和轻节点。全节点保存完整的区块链数据，独立进行数据校验、更新、查询等，不依赖其他节点。区块链中的消息传播的基本方式是广播，但不同的区块链会根据自身的特点设计特定的消息传播协议。以太坊中，使用“Gossip”协议相

互通信，“Gossip” 协议的容错性好、扩展性强，一致性收敛降低了因确认速度快导致区块失效率比较高的风险。区块链中的节点收到通过 P2P 网络传播的交易，进行验证，去除无效数据，转发验证通过的数据。此时，矿工收集并验证网络中尚未确认的数据，将有效数据存到区块中。当某一矿工完成共识条件（即挖到矿），广播，所有矿工将该区块链接到主区块链上。记账共识算法[39]主要工作量证明（POW）、权益证明（POS），委托权益证明（DPOS）等十几种共识方案。不同的共识方案对于记账的奖励激励分配方式也不相同。合理的记账奖励分配可以提高区块链的可靠性和安全性[40]。

(3) 扩展层主要设计执行智能合约，用以满足区块链不同的需求[41]。智能合约是区块链上可自动执行的一段代码合约，是区块链去中心化的核心。智能合约在写定的程序下，执行可追溯、不可逆的安全交易，达到条件自动触发。任何节点的宕机不会影响智能合约的运行。以太坊中智能合约账户任何人无法篡改。智能合约通过 P2P 网络分布式扩散在全网各个节点，存储在区块链上。智能合约的运行经过链上所有节点验证，合约可以调用合约，外部账户也可以调用合约。

(4) 应用层目前最火的应用就是区块链钱包和一些小游戏，应用层主要是通过网站、手机移动端、PC 端开发的应用软件。区块链的底层的构建相对比较完整，但是底层支持的真正的应用还比较少，亟待开发中。

2.3.2 数字签名

数字签名是区块链系统对发布的数据进行签名，一般包括签名方案和验证方案。签名方案保证消息是由数据签名者发出的。验证方案验证数据没有被篡改过，保证数据的可靠性。可靠的数字签名方式也可以提高系统的匿名性，保证用户的隐私和安全。常见的加密算法主要分为两类：对称加密、非对称加密。数字签名通常采用非对称加密的形式，即加密解密秘钥互不相同。常见的签名方式主要有：RSA 算法、DSA （Digital Signature Algorithm）算法和椭圆曲线算法（ECDSA）[42]。比特币和以太坊都采用了椭圆曲线算法。其中，不同之处在于，比特币使用 SHA2-256 的哈希算法，以太坊使用的是 SHA3-256 哈希算法。目前比较也有一些新的数字签名方案，大多从椭圆曲线算法演化而来，例如 Schnorr Signatures[43] 签名算法、Pointcheval Sanders（PS）[44]签名算法等。前者比后者签名速度快，后者比前签名长度短更安全，PS签名验证方式中也使用了 schnorr 签名算法，因此，这里详细介绍 Schnorr Signatures 签名算法。

德国数学家、密码学家 Claus Schnorr 于 1990 年提出 Schnorr 签名算法。该方案基于 ECDSA 创建，但在性能方面优于现有的椭圆曲线算法。首先本文对一些变量进行定义如下：

(1) 变量定义：

椭圆曲线 G，me 表示需要签名的数据，这里数据的表现形式通常为一个32字节的哈希值。P 代表公钥，x 代表私钥，这里有 $P = xG$。H 为哈希函数。

(2) 生成签名：

生成签名者已知：椭圆曲线 G，需要签名的数据 me；哈希函数 H 是 SHA2-256 的哈希算法；私钥 x。

1.选择一个随机数 k，计算 $R = kG$。

2.计算 $s = k + H(me||R||P) * x$，其中，$me||R||P$ 表示三个字段拼接后的结果。因此，公钥 P 对数据 me 的签名为 (R, s)，即 Schnorr 签名。

(3) 验证签名：

验证签名者已知：椭圆曲线 G，需要签名的数据 me；哈希函数 H 是 SHA2-256 的哈希算法；公钥 P；已有的签名：(R, s)。

验证签名者验证等式：$sG = R + H(me||R||P)P$，若验证等式两边相等，等式成立，表示该条数据合法，反之，不合法。

算法引入随机数k的必要性：

若不引入 k，

$s = H(me||R||P) * x$，

$sG = H(me||R||P) * xG = H(me||R||P)P$。

此时，任何人都可以获得私钥，$x = s/H$很容易得到。引入 k 后，$x = (s - k)/H$，由于 k 是随机的，因此，计算出 x 不是一件容易的事。

2.4 本章小结

本章首先介绍了移动众包问题的主要概念和核心技术，包括移动众包的激励机制等。然后介绍了区块链核心技术框架，包括存储、扩展、安全隐私等技术。最后介绍了车辆网络的基础知识。为下文研究基于区块链的车辆网络移动众包模型提供理论依据。

第 3 章　非确定性车辆团队合作众包模型

为了有效利用交通拥堵等形成的聚集型实时车辆网络，并提高车辆移动众包的安全性，本章将对基于区块链的非确定性车辆团队合作众包模型（BNTC）进行描述与设计，用以太坊作为基础区块链系统平台。本章中，首先定义了出现在该系统中的实体。说明了整个 BNTC 模型运行流程以及性能分析。然后提出 BNTC 模型中的分配算法和定价算法，最后对系统进行安全性分析。

3.1　BNTC 模型中的角色

首先，本节对 BNTC 模型中出现的实体进行定义。系统中主要定义的实体有：任务发布者节点（T）、RSU 节点（RSU）、车辆节点（y）、私有注册机构（Private Certificate Authority，PCA）。本节主要介绍几种实体。

3.1.1　实体定义

任务发布者节点（T）：大型公司的设备具有大规模计算能力，具有承担记账的能力，可以保存全部的数据信息，保证数据的完整性，因此，任务发布者节点通常是具有一定规模数据需求的组织或公司，在区块链中注册为全节点，担任存储任务的相关内容和付款信息的角色。这些节点还可以通过记账获得报酬。发布任务节点有自己的钱包，为了确保任务执行的安全，任务发布节点需要提前进行资产抵押，在钱包中冻结一部分资金作为验证具有可支付发布任务费用的能力。最后，任务发布者通过区块链系统向工人付款。

RSU节点（RSU）：RSU 传感器设备主要安装在交通信号灯等路边设施上,并与边缘服务器链接，具有网络接口和其他硬件设施，使得其具有用于计算和存储服务的能力。RSU 节点聚合区域内拥有参与众包任务意愿的车辆节点的信息，每个 RSU 节点的边缘服务器维护一个实时列表，用于存储与 RSU 传感器连接的车辆在当前时间段内的团队信息当有任务发布时，智能合约会收集所有符合条件的 RSU 节点的实时团队信息，以确定具有完成任务能力的候选团队。当一个 RSU 上传的车辆团队被任务选择算法选中后，RSU 节点将接收任务信息并将其分发给团队中的车辆，以及收集和上传车辆提交的任务结果。RSU 节点也是区块链系统中的全节点，它们维护区块链，参与共识。

车辆节点（y）：车辆节点是具有车辆计算机、智能传感器和网络接口的车辆，可以收集来车辆内的传感器获取的数据。并且，车辆可以与人进行交互，生成交互数据。车辆节点可以与 RSU 节点通过无线模式通信层交互传输，即 V2I。车辆节点可以向 RSU 提交其状态，完成任务的意愿以及投标信息。他们可以从 RSU 接收任务信息，并将结果提交给RSU。车辆节点的性能限制车辆在区块链系统中注册为轻型节点。

PCA：PCA 是一个管理机构，进入 BNTC 模型中节点到在 PCA 注册。所有节点都必须向 PCA 注册才能添加到区块链中。车辆节点是 BNTC 系统中工人节点，直接参与为别人提供服务的节点，隐私安全是影响其提供服务的一个考虑因素。因此，BNTC 系统需要提供一种很好的方式避免车辆隐私泄露。其中，匿名参与众包工作是一种有效保护车辆节点隐私的一种方式。它功能是给每个节点一个身份，以在区块链系统中用作标识，以保留所有节点的匿名性。

3.1.2 车辆团队性能

(1) 车辆团队具有一定的实时性。随着车辆进出，团队的规模和成员资格总是在变化。但是，团队足够稳定，可以在相对稳定的情况下完成任务，例如交通信号灯或交通堵塞。

(2) 一个车辆团队承担一个子任务或者整个任务，任务的分配数量根据任务分配方案结果而定。车辆团队将收到的任务继续划分，分配给团队内车辆。不同车辆的任务完成率不同，任务完成率相对较低的车辆无法单独承担子任务，不同车辆可联合执行。同理，任务完成率较低的团队也可联合承担子任务，以达到较高的任务完成率。

(3) 车辆团队成员分为两类：正式节点和非正式节点。由于车辆传感器故障或网络通信延迟等问题，某些车辆无法完成任务，导致这些车辆的信誉值降低。因此，BNTC 模型将信誉值高的节点的类型定义为团队中的正式节点，将信誉值低的节点类型定义为非正式节点。正式节点直接影响任务的完成率。此外，正式节点将获得付款和信用奖励，而非正式节点将仅通过在完成任务后增加其信誉值来付款。车辆节点分为正式节点和非正式节点，以提高预测任务的完成率时的准确性，还使性能较低的车辆参与其中，可提高完成率。

3.2 任务类型描述

BNTC 模型中的任务类型比以往的任务类型要广泛，系统将不同任务类型制定不同的任务完成方案。移动众包中的任务分为及时型任务和操作型任务。

及时型任务包括：收集道路信息、交通信息、噪声污染检测、空气质量检测以及车辆本身产生的一些数据信息。及时型任务无需进行人为操作，车辆一旦选择接收该任务，车辆就将自己的信息上传到与已经建立通信关系的 RSU 节点处。但是这样的信息传播可能会有网络不稳定或者传感器故障等造成的任务传输延时、失败或者数据不完整。因此，及时型任务可分发给小规模的车辆团体，保证数据的准确性，提高数据的可靠性和安全性。

操作型任务包括：投票、民意调查、图像语音数据收集等。操作型任务需要人为辅助操作。因交通堵塞形成的车辆团体中，团体中车辆的随机性比较强，那对于收集类信息可以得到相对具有普遍性的结果。例如，可以将一个问卷任务分配给一个适合规模的车辆团队或多个团队，一辆车只回答一道题。多份相同的调查问卷同时交给多个适合规模的车辆团队，当任务节点查看现有的网络规模后，根据自己需要发布工作内容需求，选择合适的车辆团队完成任务，以达到社会效益最大。

此外，前面章节提出一些研究表明计算型任务也可利用移动众包完成，如联合学习、模型训练等。计算型任务大多关注车辆聚集的实时效用，与车辆位置关系无关，多辆车聚集联合，共同完成计算任务。任务的分配与工人的可靠性和竞价价格相关。拥有联合计算能力的车辆团队可以代替本地服务器完成计算任务。

广播的任务中，包括任务的需求，如时间需求，时间间隔为 $[t_0, t_1]$。例如，一个任务要测试下午 5 点至 7 点的某范围内的噪声指数。所以任务的完成时间要在 5 – 7 点之间。超过时间记为任务未完成。另外，由于车辆网络的不稳定性，任务有最晚上传时间 t_{end}，最晚上传时间一般晚于任务要求完成的最晚时间，即 $t_1 \leq t_{end}$。在最晚上传时间之后再提交的数据，同样记为任务未完成。

3.3 车辆团体的形成条件

BNTC 模型认为，当一个 RSU 扫描到车辆节点的数量多于一个固定的值（D）时，该 RSU 附近形成了一个可用于参与计算承担任务的车辆计算团队。此时，RSU 计算该计算团队的车辆数量，统计整个计算团队的计算能力、完成任务率等信息。完成任务准确率是根据历史信息记录获取的，车辆传感器故障、网络通信延时等，可能造成车辆承担任务后，无法按时上传结果。因此，在一个计算团队中，不是所有节点的完成度都很高。对于一个计算团队中计算能力的统计，首先要选取完成概率高于某一个值的节点才能参与到计算能力认定的团队，成为团队中的正式节点。团队中剩余的完成概率不高但又想参与到计算任务中来的节点，本文认为这样的节点也可以进行无奖励参与，但是可以通过做这样的任务获得信誉值奖励，提高节点本身完成任务的概率，进而提升节点在一个团队

中作为主要车辆任务节点的概率。

3.4 BNTC 系统模型

3.4.1 初始化系统

不同角色的节点需要获得进入 BNTC 系统的资格或证明，才能进入该系统。PCA 为中央权威机构（例如，政府的交通管理部门）的一个分布式身份管理系统[45]。节点要通过 PCA 的验证才可以进入 BNTC 系统。经过 PCA 的身份验证后，每辆车都是合法车辆，每个发布任务节点和 RSU 节点都是合法节点。对于任务发布节点和 RSU 节点，PCA 为其生成公私钥对。车辆是区块链中的任务承担者，即共享自己的数据，需要更严格地保护车辆的隐私，因此，这里使用 Pointcheval 和 Sanders （PS-Signatures）设计的 PS-签名对车辆生成匿名身份证书[46]。PS-签名是基于零知识证明和 schnorr 的一种双线性加密模式，达到匿名效果的同时，实现了生成短签名，签名的长度是 32bit。PCA 为车辆颁发进入到 BNTC 系统的唯一的匿名身份证书，并为用户生成的公钥私钥。为保证注册用户的安全，系统对私钥进行销毁，并且，注册用户账户名以及隐私信息之间的关系映射存储在权威机构的数据库中。BNTC 系统中节点的类型不同，并且区块链平台通过发布不同类型的证书来指示 BNTC 中节点的角色，初始化系统中车辆节点注册生成匿名证书的过程如图 3-1 所示，步骤描述如下：

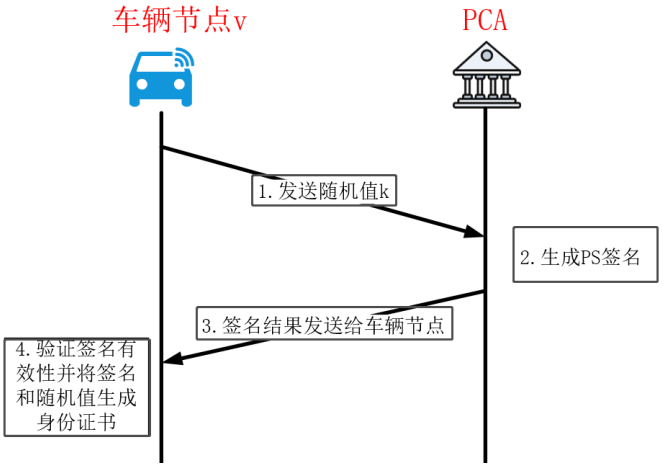

图 3-1　　车辆节点进入区块链的注册过程

首先，PCA 为车辆节点和任务节点生成公开参数。令$(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T)$为三个一阶 p 循环群，其中，p 是$\lambda$ 字节。此外，$g_1, g_2 \epsilon \mathbb{G}_1$，$\tilde{g} \epsilon \mathbb{G}_2$。线性对为 e：$\mathbb{G}_1 X \mathbb{G}_2 \rightarrow \mathbb{G}_T$。哈希函数使用 SHA2-256 的哈希算法 H。PCA 为注册节点生成一个密钥

$SKEY = (a,b)\epsilon_R Z_p^2$。计算 $\tilde{X} = \tilde{g}^a, \tilde{Y} = \tilde{g}^b$。因此，可以得到系公共的参数如下所示：

$$\mathfrak{R} = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, g_1, g_2, \tilde{g}, \tilde{X}, \tilde{Y}, H, e\} \tag{3-1}$$

(1) 车辆节点 y_i 生成一个随机数 $k_i \epsilon_R Z_p$，需要对该随机数加密，即计算 $(T_{i,1}, T_{i,2}) = (g^k, \tilde{X}^{k_i})$，$y_i$ 生成一个证明 π_{k_i}，如 3-2 所示。然后，车辆节点 y_i 发送加密后的 $(T_{i,1}, T_{i,2}, \pi_{k_i})$ 到 PCA 注册机构。

$$PK = \{(k_i) : T_{i,1} = g_1^{\cdot k_i} \Lambda T_{i,2} = \tilde{X}^{\cdot k_i}\} \tag{3-2}$$

(2) PCA 注册机构首先验证 π_{k_i} 的有效性和 $e(T_{i,1}, \tilde{X}) = e(g_1, T_{i,2})$ 是否相等。若验证成功，PCA 生成一个随机数 $u\epsilon_R Z_p$，对车辆节点 y_i 提交的 $T_{i,1}$ 进行 PS-Signatures 签名，如下所示：

$$\begin{aligned} \vartheta_i &= SigCom(T_{i,1}, \mathfrak{R}, SKEY, u) \\ &= (\vartheta_{i,1}, \vartheta_{i,2}) \\ &= (g_1^u, (g_1^a \cdot T_{i,1}^b)^u). \end{aligned} \tag{3-3}$$

PCA 注册机构将处理车辆 y 注册的结果 $(R_i, T_{I,1}, T_{i,2}, \vartheta_i)$ 存储的该机构内，将签名认证结果 ϑ_i 发送给 y_i。

(3) 节点 y_i 接收到 ϑ_i 后，利用零知识证明验证签名结果是不是对本车辆发送消息的生成结果，验证通过后，车辆节点 y_i 存储 (k_i, ϑ_i) 为本车辆进入到 BNTC 系统的身份证明。

$$e(\vartheta_{i,1}, \tilde{X} \cdot k_i) = e(\vartheta_{i,2}, \tilde{g}). \tag{3-4}$$

RSU 节点和任务发布节点在 PCA 中进行注册，PCA 为其生成公钥私钥对 $(S_j, \mathbb{P}_j)$。为了进一步提高系统的安全性，PCA 在将公私钥生成后发送给节点，系统中只保存公钥 $(ID, \mathbb{P}_j)$，私钥销毁。交易中仅存储用户的帐户名，而不是诸如牌照号码或电话号码之类的对隐私敏感的信息。账户名和隐私敏感信息之间的映射关系存储在受信任机构的数据库中。

3.4.2 系统过程

BNTC 系统运行过程如图 3-2 所示。

步骤1.（获取团体列表）：BNTC 系统中，RSU 传感器安装在信号灯上，每个传感器可以扫描车辆迎面来方向的道路区域。区域宽度为与同方向道路数目有关，区域长度设定为 L。车辆团体建立过程如图 3-3 所示。位于交通信号灯处的 RSU 节点与进入其扫描路段的车辆建立连接。以图中 RSU 节点 A 为例，节点 A

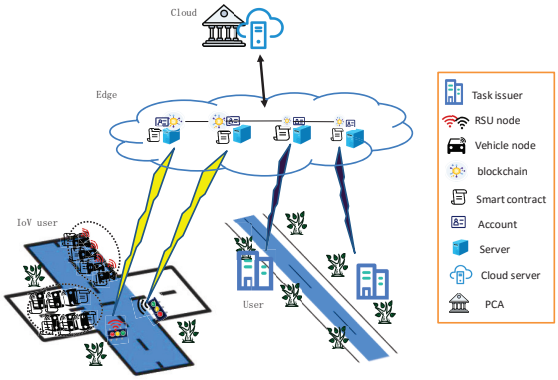

图 3-2　　BNTC 系统基本框架

可扫描的区域为对面路段长 L 宽 M 的区域范围，可以收集到六辆车信息。收集到的车辆信息存储在 RSU 节点的边缘服务器内。实际上，没有任何车辆愿意参加没有报酬的能源消耗工作，因此文中认为，每一辆车报告的是自己可以接受的最低价格。为了提高竞争优势，这里系统认为每一辆车报告的自己做任务的真实成本。后面小结会详细解释该问题。每个 RSU 节点的边缘服务器维护一个实时车辆信息表，包括车辆（ID），车辆与节点 A 建立连接的时刻（t_{in}），离开该扫描区域的时刻（t_{out}），车量完成能力（$scale_i$）车辆任务完成率（q_i），车辆信誉值（r_i），车辆对不同类型任务的竞价报价（bid_i）等信息，如表 3-1 所示。每个车辆都是区块链中的轻节点，车辆任务完成率和车辆信誉值存储在区块链中。RSU 在获得车辆预备接受任务的准备信号连接时，请求区块链，获取车辆的任务完成率和信誉值。

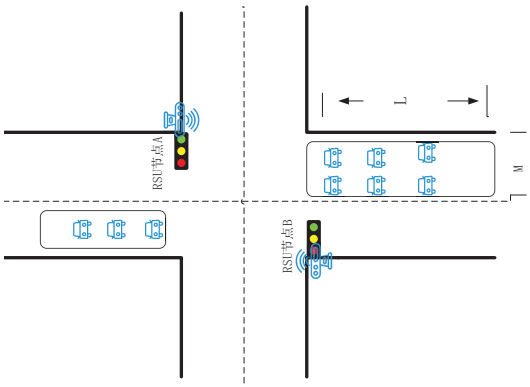

图 3-3　　十字路口车辆识别

说明：

(1) 每一个 RSU 节点收集辐射区域内处于空闲车辆的报告，前提是这些车辆

处于空闲并愿意在该时刻接受自己报告的任务类型。发布任务和分配任务以及传递信息都有网络时延。进一步可以认为，若空闲车辆在尚未改变自己发送给 RSU 节点修改车辆信息前收到一个任务，该车辆接受任务并可以直接执行任务。这一点在实时性车辆网络中十分关键。若在分配好之后无条件不接受任务，对于车辆网络的任务分发机制损失很大，极端情况下会造成大量任务难以完成，进而导致系统的好感度降低。

(2) 每一个 RSU 节点的边缘服务器维护的实时车辆信息表中，如 3-1 所示，边缘服务器对收集到的信息进行统计与计算。首先要获取所有的车辆账户 ID，公私钥对以及身份证书。然后，统计对于不同类型任务，现有的处于空闲并且愿意接受任务的车辆的信息。具体信息内容将在下一章进行详细说明。通过聚合现有车辆的信息，判断是否可以形成车辆团队，若不堵车或车辆聚集规模较小，是无法形成车辆团队的。这样的车辆聚集不满足团队条件，因此不会出现在智能合约收集的实时车辆团队结果中。

表 3-1 RSU 节点维护的实施车辆信息表

ID	t_{in}	t_{out}	q_i	r_i	$scale_i$	bid_i
000001	20200305.10:00:00	20200305.10:10:00	80%	0.8	10	15

这里，车辆上传的信息为匿名信息 $si_{i,j}$，表示车辆 i 对任务 j 这一类任务的竞价信息或者任务数据。并且标有位置信息，即在由同一RSU 边缘服务器统计的车辆才可以形成一个计算团队。以一个 RSU 节点收集与车辆内车辆综合竞价信息为例，详细过程如下：

(1) 车辆 i 可以连接的 RSU 的公钥：pk_C。车辆 i 随机选择 $r\epsilon_R\mathbb{Z}_p$，对 $si_{i,j}$ 加密，如公式（3-5）所示。

$$r_{i,j} = (r_{i,j,1}, r_{i,j,2}) = (pk_C^r g_2^{si_{i,j}}, g_2^r) \tag{3-5}$$

车辆 i 构建生成一个证明 $\pi_{i,j}$，以此证明 $r_{i,j}$ 确实是车辆 i 对秘密 $si_{i,j}$ 的加密。证明如下公式（3-6）所示。

$$PK = \left\{ \begin{matrix} (s_{i,j}, r) : r_{i,j,1} = pk_C^r g_2^{s_{i,j}} \wedge \\ r_{i,j,2} = g_2^r \wedge si_{i,j} \end{matrix} \right\} \tag{3-6}$$

(2) 车辆 i 计算 $d = g_1^{H(T_j)k_i}$，并且选择一个随机数 $k\epsilon\mathbb{Z}_p$，计算出值，如公式（3-7）所示。

$$\begin{cases} a = g_1^{H(T_j)k} \\ ch = H(d, a, T_j, r_{i,j}, \pi_{i,j}) \\ s = k + ch \cdot k_i \end{cases} \tag{3-7}$$

车辆 i 设置 $\sigma = (d, ch, s)$，发送对 $si_{i,j}$ 加密后的信息 $(\sigma, r_{i,j}, \pi_{i,j}, T_j)$ 给 RSU 节点。

(3) RSU 节点接收到车辆 i 发送的加密信息后对其进行验证。首先，RSU 节点用 T_j 的公钥 $\mathbb{P}$ 计算,如公式（3-8）所示。

$$a' = d^{-ch} \cdot g_1^{H(T_j s)} \tag{3-8}$$

用公式 3-8 计算 ch 与 $H(d, a', T_j, r_{i,j}, \pi_{i,j})$ 是否相等。若相等，RSU 节点接收该匿名车辆的报告。

(4) RSU 节点收到所有竞价信息后，将对所有信息进行汇总，RSU 节点 C_n 计算 $s_j = (s_{j,1}, s_{j,2}) = (\prod r_{i,j,1}, \prod r_{i,j,2})$ 使用秘钥 $S_{j,n}$ 进行部分解密，即计算 $p_{j,n} = s_{j,2}^{S_n}$。RSU 节点构建解密证明 $\pi_{j,n}$，如公式（3-9）所示。

$$PK = \{(S_n) : p_{j,n} = s_{j,2}^{S_n} \wedge \mathbb{P}_j = g_2^{S_n}\} \tag{3-9}$$

以上证明通过后，一个 RSU 节点形成的车辆团队对任务的竞价信息如公式（3-10）所示。

$$TR_j = \frac{s_{j,1}}{\prod_{C_n \epsilon \tau_c} p_{j,n}} = g_2^{\sum si_{i,j}} \tag{3-10}$$

RSU 节点获取了在该处形成的车辆团队信息 TR_j。

步骤2（团队信息上传和验证）：当任务发布者 T_j 上传任务进行众包任务时，在区块链账户中存放一笔押金，这笔押金将冻结在区块链中，无法提取直至任务结束。账户中的押金要确保对自己发布的任务有能力结算付款。以防出现任务完成，收到了任务的方案后，但是该账户没有资金和能力进行付款。上传完任务需求后，区块链智能合约将收集目前所在区域的车辆网络中所有 RSU 收集到的车辆团队情况信息。车辆团队信息的上传要求当任务发布立刻做出反应，实时性强。因此这里使用基于 schnorr 的群签名[47]进行签名验证，用非对称加密的方式对数据进行加密。schnorr 签名基于比特币现有的签名算法 ECDSA 进行改进，拥有安全性证明[48] 而 ECDSA 没有。schnorr 签名是线性的，签名可以聚合，可以使得一笔多个签名的交易仅需要一次验证，进而提升验证速度。参与签名的委员会成员为预先选择好的一批高信誉度的 RSU 节点或者任务发布节点（n 个委员会成员），高信誉度的 RSU 节点和任务发布节点是参与任务的次数较多且成功次数较多，这里认为这些节点都是可信的。下面简述基于 schnorr 的群签名签名验证过程[49]：

(1) 变量定义：椭圆曲线 G，m 表示需要签名的数据，这里数据的表现形式通常为一个 32 字节的哈希值，是团队信息加密后的结果。P 代表公钥，x 代表私钥。H 为哈希函数。

(2) 生成签名：n 个委员会成员分别对消息 m 进行签名，签名者已知：椭圆曲线 G，需要签名的数据 m；哈希函数 H 是 SHA2-256 的哈希算法；私钥 x。

委员会成员生成的公私钥对为：私钥 x_1，公钥 $P_1 = x_1 G$。生成随机数为：

k_1，并计算 $R_1 = k_1 G$。

因此生成的聚合公钥为：$P = P_1 + P_2 + ... + P_n$。并计算聚合随机数为：$R = R_1 + R_2 + ... + R_n$。

2.计算 $s_1 = k_1 + H(m||R||P) * x_1$，其中，$m||R||P$ 表示三个字段拼接后的结果。因此，n 签名者的群签名为公式3-11 因此，公钥P对数据m的签名为(R, s),生成的签名为Schnorr签名。

$$\begin{aligned} s &= s_1 + s_2 + ... + s_N \\ &= k_1 + H(m||R||P) * x_1 + k_2 + H(m||R||P) * x_2 + ... + k_n + H(m||R||P) * x_n \\ &= (k_1 + k_2 + ... + k_n) + H(m||R||P)(x_1 + x_2 + ... + x_n) \end{aligned} \tag{3-11}$$

(3) 验证签名：验证签名者已知：椭圆曲线 G，需要签名的数据 m；哈希函数 H 是 SHA2-256 的哈希算法；公钥 P；已有的签名：(R, s)。

根据性质，对公式3-11左右两边同时乘以 G，可以得到公式（3-12）。

$$\begin{aligned} sG &= (k_1 G + k_2 G + ... + k_n G) + H(m||R||P)(x_1 + x_2 + ... + x_n)G \\ &= (R_1 + R_2 + ... + R_n) + +H(m||R||P)(P_1 + P_2 + ... + P_n) \\ &= R + H(m||R||P)(x_1 + x_2 + ... + x_n) * P \end{aligned} \tag{3-12}$$

步骤3（计算分配和定价）：RSU 节点将收集到的车辆账户信息上传到区块链中，通过调用智能合约，传递算法所需的参数，并使用 BNTC 的 WTS 算法根据获胜团队的能力和出价信息来计算最适合该任务的团队。选择出可以胜任任务的团队后，再基于 BNTC 的 CTP 算法，根据车辆团体的信誉值和竞标价格计算出每个已经被选择的车辆团体相应的付款。分配与定价算法在下一章节具体介绍。

步骤4（分发任务结果）：系统将候选团队及其付款信息加密后返回给任务发布者。如果任务发布者同意结果，则对结果进行签名并将付款提交给系统，否则结果将被删除。任务发布者签署结果后，区块链系统会记录团队，车辆，RSU，任务，任务分配，任务发布者和付款的信息。

步骤5（任务执行和收集）：任务被发送到 RSU，并分配给所选团队中的车辆。被选中的车辆将完成的任务数据传输到 RSU 传感器，并通过边缘服务器发送到区块链平台。RSU 节点相当于数据的聚合器。车辆首先向链接的 RSU 发送请求，并发送数字签名和身份证书，确保任务数据的真实可靠性。RSU 节点对数据进行验证，并返回验证通过的标识，这时车辆用任务发布节点的公钥加密任务数据，并发送到 RSU 节点。对于任务的付款交易中，每笔交易包含两个主要组成部分：交易信息和数字签名。交易信息包括付款记录、费用记录和记录交易发生的时间戳。由于 IoV 的存储和计算能力有限，因此将整个检测报告存储在

交易数据中是不明智的。相反，交易数据包含一个索引，指示由付款人和收款人加密的传感数据的特定位置。出于可追溯的原因，交易数据不仅包括前一个区块的哈希值，而且还包括细节感应数据的哈希值。数字签名由付款人和收款人的私钥签名。RSU 节点和任务发布节点具有记账功能收集到一定数量的交易后，会生成一个区块并开始共识过程。

说明：

1.每一个任务发布者申请查看实时车辆团体信息，只能查看到目前处于正在空闲时刻的车辆团队，不统计处于工作中的车辆团队。车辆完成任务后，结果由 RSU 收集。RSU 将结果记录在区块链中，并同时将其发送给任务发布者。精明的合同可确保工人得到正确的报酬。

2.当分配的车辆团体已经接受任务并处于工作中时，若继续有任务发布者发布任务，这些处于工作中的车辆团体将不被统计在现有的实时车辆团体信息统计中。

3.5 BNTC 模型中的任务分配算法和奖励支付算法

模型中设计的符号定义如 3-2 所示：

表 3-2 BNTC 系统中的符号定义

符号	定义
V	现存的车辆团队
V_{-v}	除了团队 v 以外的现存车辆团队
S	任务规模
N	车辆团队总数量
v_k	第 k 个车辆团队
y_k^i	第 k 个车辆团队中车辆i
tc_k	车辆团队 v_k 可完成的任务数量
q_k^i	车辆 y_k^i 的任务完成率
p_k	车辆团队 v_k 的任务完成率
r_k^i	车辆 y_k^i 的信誉值
R_k	车辆团队 v_k 的信誉值
B_k	车辆团队 v_k 的平均竞价
χ	获胜车辆团队
$Cost_\chi$	获胜车辆团队的成本
$Payment_\chi$	获胜车辆团队的报酬
χ_{-v}	除了车辆团队 v 以外的获胜团队
A	获胜车辆团队的数量

3.5.1 问题定义

本小节对算法中用到的表示进行定义。在整个车辆网络中，当任务发布者请求发布任务时，所有 RSU 边缘服务器提交的车辆团队的数量一共有 N 个。所有

车辆团队可以表示为 $V = \{v_1, v_2, ..., v_N\}$。当 RSU 接收车辆链接请求时，RSU 统计收集车辆的请求信息，包括车辆的 id 和车辆的竞价 b。RSU 节点在接受了车辆请求后，传送给链接的边缘服务器，边缘服务器会向区块链请求对应车辆的信誉值 r 和任务完成率 q，这里认为，当一个车辆的任务完成率低于一个值（例如：这个值是 0.5），系统认为这样的节点承担任务不完成的风险很大。所以，按照系统设定的完成率阈值设定，将与请求完成任务的车辆划分为两种节点，高于这一阈值的为正是节点，低于这一阈值的为非正式节点。正式节点是被统计在车辆团队任务完成中的，这样的节点若参与并完成了任务，会获得一定的资金报酬和完成率信誉值的提升。然而，非正式节点在所在团队被选为做任务团队后，也可以参与完成任务，但不是单独承担一个子任务，是作为提高某子任务的完成率参加的。非正式节点参与并完成了任务只可获取任务完成率和信誉值上的提升，但并不能获得金钱上的奖励。若非正式节点没有完成任务，不但不会获得奖励，起信誉值和任务完成率会变得更低。每隔单位时间（例如：每个边缘服务器每隔 10s 统计一次）再根据现有的所有车辆信息，可以形成车辆团队 v_k 包含 m_k 个车辆节点$\{y_k^1, y_k^2, ..., y_k^{m_k}\}$。该团队的整体任务完成能力定义为如公式（3-13）所示。

$$tc_k = \sum_{i=0}^{m_k} c_i \tag{3-13}$$

其中，c_i 表示一辆车在单位时间内完成任务的数量。任务发布节点发布一个任务，最终根据车辆团队的信息被分成 A 个子任务，即，$S = \{s_1, s_2, ..., s_A\}$，选择一个或者多个车辆团队联合完成一个任务。

非正式节点的意义归纳如下：

1. 在车辆众包或者普通众包中，即使是任务完成率高达 100% 的车辆，也只是根据历史值确定的，历史可以预测本次，但本次参与任务也会有完不成任务的可能性。因此，非正式节点辅助完成任务会在一定程度上提高任务的完成率，对系统完成任务本身，不仅没有损失，更是进一步提升了可靠性。

2.非正式节点本身参与任务具有一定的合理性。之前一些关于信誉值问题判断节点是否能参加众包的研究，对于作恶节点的基于作恶时间段监控，从当前开始向前的检测作恶时间段内若无作恶行为，就认为该节点是正常节点。节点的信誉值并不是通过主动分配任务来提升。然而本文模型中，车辆信誉值的提升是通过车辆本身做任务弥补而来的。即使已经通过做任务获得利润，但是可以通过做任务改变车辆的信誉属性，从恶意节点向正常节点转变。单纯的通过历史时间判断恶意选取，不足以确定节点的性质。这种通过做任务弥补信誉值损失的方法的成本耗费比较大，由此更能约束节点的行为，提高作恶的成本，进一步提高节点分配任务的安全性。

对于一个团队 k 中一个车辆 y_k^i 的信誉值为 r_k^i。信誉值与参加任务的次数和

参加任务中失败的次数相关。“n” 表示车辆 y_k^i 参与任务的总次数。“m” 表示车辆 y_k^i 参与任务中失败的次数。“ω” 是公式中调整参数，确保当一个车辆上一次做任务失败对信誉值的损失，这一次任务成功，但是成功一次不足以弥补一次失败对信誉值造成的损失。$flag$ 表示一辆车对一个子任务的完成状态，当 $flag$ 为 0 表示车辆 y_k^i 本次执行任务失败，$flag$ 为 1 表示本次执行成功。因此，信誉值r_k^i可描述为如公式（3-14）所示。

$$r_k^i = \begin{cases} 1 - 0.1m & n \le 5, flag = 0 \\ max(r_k^i * (1 - \frac{n-m}{n} * \omega), 0) & n > 5, flag = 0 \\ min(r_k^i * (1 + \frac{n-m}{n} * \omega), 1) & n > 5, flag = 1 \end{cases} \tag{3-14}$$

模型中，车辆初始信誉值为 1，默认初次参与任务的车辆都是值得信任的节点。在执行任务 5 次之内，如果没有完成任务，按照 5 次之内的少量惩罚策略降低信誉值；如果执行任务超过五次，按照大于五次的方式降低信誉值，这样做保证任何时刻对未完成任务都有惩罚。公式中，以 5 次为阈值区分初始和稳定，初始阶段，车辆进入系统参加众包操作不熟练，任务失败率相对较高，因此轻度惩罚，采用 5 次之内的惩罚方式。随着参与任务的次数的增多，参与环境逐渐稳定，再发生任务失败，则是由作恶造成的可能性较大，因此惩罚程度升高。稳定后的高惩罚率对车辆起到约束的作用，有利于促进节点保持任务成功的状态。信誉值变化中，一次完成任务的奖励不能完全弥补失败带来的损失，由此可见任务失败产生的后续代价很高。根据每一辆车的信誉值，一个车辆团队 v_k 的信誉值可以表示为如公式（3-15）所示。

$$R_k = (\sum_{y_k^i \epsilon v_k} r_k^i)/m_k \tag{3-15}$$

车辆 y_k^i 的完成率与车辆本身的性质有关，车辆本身的硬件设施、网络带宽都会对车辆完成任务的造成影响。因此，系统中设置任务完成率的初始值为每一辆车本身的完成率，即 q_k^i。此外，从公式（3-14 ）中也可以看出，车辆信誉值是根据车辆历史任务完成情况分析得来的。由此，得到车辆任务完成率与信誉值的变化有关，信誉值升高，车辆完成率升高；反之，下降。得出车辆 y_k^i 完成率的计算公式为如公式（3-16）所示。

$$q_k^i = min((1 + \Delta r_k^i) * q_k^i, 1) \tag{3-16}$$

根据车辆的任务完成率，计算一个车辆团队 v_k 的任务完成率为如公式（3-17）所示。

$$P_k = 1 - \prod_{y_k^i \epsilon v_k} (1 - q_k^i) \tag{3-17}$$

模型中设定 η 为车辆团队任务完成率的阈值，当一个车辆团队的完成率低于 η

时，该团队不能单独承担子任务。相同的子任务可以分发给不同的团队，因此，如果两个或多个车辆团队联合承担一个子任务的任务完成率大于阈值,那么这些车辆团体可以联合承担子任务，但任务完成的成本是两个团队成本之和。这里，联合任务的完成率表示为如公式（3-18）所示。

$$\tilde{P}_n = 1 - \prod(1 - P_i) \tag{3-18}$$

每一辆车可以对自己根据自己选择的不同类型的任务进行报价，因此，一个车辆团队的总任务报价为团体中有效车辆节点任务报价之和，即车辆团队 v_k 的竞价报价为如公式（3-19）所示。

$$B_k = \sum_{i=1}^{m_k} b_i \tag{3-19}$$

3.5.2 问题模型

上一节对车辆网络模型中的参数进行了定义，本节对移动车辆网络众包的激励机制进行定义。首先，当有任务发布节点请求发布任务时，智能合约收集到 N 个任务完成率达到 η 的车辆团队信息为如公式（3-20）所示。

$$PV = \{p_1, p_2, ..., p_N\} \tag{3-20}$$

收集到的 N 个车辆团队可以完成的任务规模表示为如公式（3-21）所示。

$$TC = \{tc_1, tc_2, ..., tc_N\} \tag{3-21}$$

$$s.t.tc_i \geqslant \theta \tag{3-22}$$

RSU 节点收到的车辆节点数量多于设置的阈值 θ，可以形成车辆团体。在移动车辆众包问题中，模型中认为，一个车辆的竞价报价与车辆本身的成本相等。因此，后文统一使用竞价 B 来表示，同一时刻 N 个车辆团体对某一任务的竞价报价表示为如公式（3-23）所示。

$$BV = \{B_1, B_2, ..., B_N\} \tag{3-23}$$

任务发布者为了得到任务的结果支付的奖励表示为:

$$Payment_{issuer} = \sum_{\chi} payment_i \tag{3-24}$$

车辆团队参与任务竞价提交真实成本，任务发布者提供恰当的奖励给予车辆团队。超付率[11]是奖励的衡量标准，也是社会福利的指标之一，一个任务的超付

率表示为如公式（3-25）所示。

$$OverPaymentRatio = (Payment - Cost)/Cost \tag{3-25}$$

整个系统的社会福利表示为如公式（3-26）所示。

$$W_{Social} = \frac{S}{\alpha_1 * Cost + \alpha_2 * (Payment - Cost) + \alpha_3 * A} \tag{3-26}$$

S 表示任务发布者发布的整个任务的规模。$Cost$ 表示所有车辆团队为完成任务总的成本。$Payment$ 表示任务发布者发布的整个任务支付的整体费用。$\alpha_1, \alpha_2, \alpha_3$ 是调整参数，用于保证社会福利的大小首先取决于总成本，其次取决于支付与成本的差额，最后取决于获胜团队的数量。获胜的团队组表示为如公式（3-27）所示。

$$\chi = \{x_1, x_2..., x_A\} \tag{3-27}$$

其中，获胜团队的数量为 A 个。获胜团队的数量是根据实时的候选车辆团队的规模报价等信息而定。因此，获胜团队的社会福利表示为如公式（3-28）所示。

$$W_{Social} = \frac{S}{\alpha_1 * Cost_\chi + \alpha_2 * (Payment_\chi - Cost_\chi) + \alpha_3 * A} \tag{3-28}$$

在模型中，需要通过适当的方式计算出当满足任务目标的最大化的社会福利。下面是对问题的一些假设：

假设1：本文认为，现存在的车辆网络必须任务发布者发布任务的需求，如公式（3-29）所示。

$$\sum_{i=0}^{N} tc_i \geqslant S \tag{3-29}$$

假设 2：RSU 上传车辆团队信息到区块链后，车辆团队在任务完成前保持原有的稳定状态。即，当任务发布者收集实时网络信息到通过算法计算任务分配任务，到最后完成任务，车辆网络是要保证可以完成分配的子任务的。因此，模型中一个子任务的完成情况仅仅依赖于车辆团队的任务完成率。

假设 3：车辆的竞价报价与车辆做任务的真实报价一致。

假设 1 和假设 2 在实践中可以满足，假设 3 在进行任务分配算法是默认是假设条件，在任务定价算法后，通过文章[11] 可以证明假设是真实有效的。

3.5.3 获胜团队选择算法（WTS）

任务节点发布任务前获取候选团队，任务完成率高的团队被选择为候选团队，以此提高任务完成率。从候选团队中，选择适当的团队组成获胜团队集合，从而达到满足条件的社会福利最大值。因此，首先，需要从上传的车辆团队信息中筛选出符合任务完成率规定的候选团队。选择适当的团队时，算法中考虑的

因素有：车辆团队的竞价报价以及获胜团队的数量，即多目标满足社会福利最大化。但是，两个目标并不是并列考虑的，本文将设计算法，算法首先考虑成本最小化，成本越小，任务发布方的满意度越高，事实证明，任务发布者往往倾向于在任务质量相同的情况下达到支付的付款越小。在满足成本最小化的前提下，考虑团队数量最小化。团队划分越少，系统分发的压力越小，成本越小。定义 WTS 算法中的满意度公式为如公式（3-30）所示。

$$\begin{aligned} SAT &= -((a_{min} - a_{max} - 1) * \sum_{\chi} B_i - A) \\ &= (1 + a_{max} - a_{min}) * \sum_{\chi} B_i + A \end{aligned} \tag{3-30}$$

$$s.t. \begin{cases} 1 \le a_{min} \le A \le a_{max} \le \frac{N}{2} \end{cases} \tag{3-31}$$

a_{min} 和 a_{max} 是获胜团队数量的边界值。首先，由于候选团队的总任务完成规模可以满足任务发布者发布的任务，一定可以选出获胜团队，由此得出 $a_{min} \geqslant 1$。发布的任务是由团队完成，因此，选出的团队的个数不能大于 N，这是团队的最大承受度决定的，也可以进行调节。下面进行对满意度公式的证明，证明满意度公式的合理性。

证明：首先，完成任务的要求是满足以下三个条件：条件 1. 达到团队成本最小，条件 2. 满足 task issuer 花费最少，条件 3. 选择的团队数量最少。三个条件的关系存在主从关系，在条件1的基础上满足条件 2，在条件 2 的基础上再满足条件 3。对于选择算法来说，没有涉及定价的条件，因此只考虑条件 1 和条件 3。即在条件 1 的基础上满足条件 3。对于满意度公式的定义的证明，要从后向前确定公式合理性，首先假设任务完成的成本相同，在这个前提下，要求，数量越少，满意度越大。因此，第一步，假设：

$$f(A) = k_1 A$$

$$s.t. \begin{cases} A_1 > A_2 \\ f_1 < f_2 \end{cases} \tag{3-32}$$

其中，A 是任务数量，k_1 是常数，f 是数量关系函数，由此得出，

$$k_1 A_1 < k_1 A_2$$

$$k_1 (A_1 - A_2) < 0$$

$$k_1 < 0$$

由上式推到可知，k_1 只要是负数，即可满足条件。为了方便计算和理解，公式中取 $k_1 = -1$，因此得到如公式（3-33）所示。

$$f(A) = -A. \tag{3-33}$$

满足保持控制变量情况下，胜利团队数量越少，满意度越大的条件。

第二步，同理，对于竞价报价 B，按照上面公式的设计原则设计为：

$$g(B,A) = k_2 B - A$$

这里认为，成本越小（即 B 越小），满意度越高。因此，公式 3-33 满足：

$$s.t.\begin{cases} B_1 > B_2 \\ \forall A_1, A_2 \epsilon [a_{min}, a_{max}] \\ g_1 < g_2 \end{cases} \tag{3-34}$$

计算展开$g_1 < g_2$，可以得到：

$$k_2 B_1 - A_1 < k_2 B_2 - A_2$$

$$k_2 < \frac{A_1 - A_2}{B_1 - B_2}$$

首先通过不等式放缩的方式，得到：

$$k_2 < min(\frac{A_1 - A_2}{B_1 - B_2})$$

再次使用不等式放缩，得到：

$$k_2 < a_{min} - a_{max}$$

简单的，可以取：

$$k_2 = a_{min} - a_{max} - 1$$

因此，最终得到公式（3-35）：

$$\begin{aligned} g(B,A) &= k_2 B - A \\ &= (a_{min} - a_{max} - 1) * B - A \end{aligned} \tag{3-35}$$

通过简单的计算，可以将公式（3-35）转化为满意度公式 $S\tilde{A}T$（3-36）.

$$S\tilde{A}T = (a_{min} - a_{max} - 1) * \sum_{\chi} B_i - A \tag{3-36}$$

通过上式可以发现，计算的满意度都是负值，小于 0，因此，为了便于计算，将负数的公式转化为正数。公式将采取取反的方式改变公式符号，即得到公式（3-30）。可以得到正数值越大，满意度越小。因此，为了解决为任务选择获胜团队 χ 这一问题，本文提出使用背包算法(Knapsack-based Algorithm) 选择获胜团队。算法中，使用数组 SA 表示 SAT 的动态转移方程的状态，动态转移方程为如公式（3-37）所示。

$$SA[j] = min(SAT(SA[j - TC[i]], TC[i]), SA[j]) \tag{3-37}$$

公式 3-37 中，j 表示任务规模，当目前可完成的任务规模是 $j - TC[i]$ 时，加入团队 i，可完成的任务规模为 $j = (j - TC[i]) + TC[i]$，对于任务规模 j 的满意度

函数为 $SAT(SA[j-TC[i]],TC[i])$。此时，用 $SAT(SA[j-TC[i]],TC[i])$ 和 $SA[j]$ 中较小的一个值更新 $SA[j]$ 。

算法 WTS 的执行过程如算法 1 所示。其中，任务规模 S，竞价报价组 $BV[N]$ 和团队完成能力 $TC[N]$ 作为算法的输入，算法 WTS 输出获胜团队组 χ。算法中一共需要两层循环，第一层循环从 $0-N$ ，表示增加团队 i 对任务完成的满意度的改变。第二层循环表示任务规模的变化。计算不同任务规模的最小值 SA，表示满意度的最大值。

算法 1 Winning-Bid Selection Algorithm

输入： S,N, $BV[N]$, $TC[N]$
输出： $value$, $nums$, χ

$WinTeamSet \leftarrow []$
$nums \leftarrow 0$
for $i = 0$ to N **do**
    for $j = S$ to $TC[i]$ **do**
        $bs \leftarrow SAT(SA[j-TC[i]],TC[i])$
        if $SA[j] > bs$ **then**
            $SA[j] \leftarrow bs$
            $WinTeamSet[j] \leftarrow WinTeamSet[j-TC[i]] \cup i$
        end if
    end for
    $i \leftarrow i+1$
end for
for i in $WinTeamSet[S]$ **do**
    $value \leftarrow value + B[i]$
    $nums \leftarrow nums + 1$
    $maxCapbility \leftarrow$ ϒΓ′fl:z<i
end for
$\chi \leftarrow WinTeamSet[S]$
return $value$ and $nums$ and χ

算法1中，用到两次循环，时间复杂度为 $O(SN)$。在本文的问题中，是要找到，在至少达到这一容量的标准下，即达不到是不符合要求的，且不能超出很多，是要找到满足容量的最小值。而背包算法的一般问题描述如下：以容量为例，在不超过某个设定容量的前提下，计算出可以使价值最大的选择物品方式。因此，直接通过背包算法不一定可以计算出恰好满足目标任务规模的团队，即 $WinTeamSet[S]$ 可能是个空值，只有恰好满足任务规模之和为 S 的的情况才会直接计算出。为此，本文通过以下方式解决：

从 $WinTeamSet[S]$ 开始逐渐减小，直到找到可以选出候选团队的任务规模的第一个任务规模为止，即 $WinTeamSet[S-k]$。由于背包算法中，状态转移方程按照任务规模来递归的。可以认为，找到的 $S-k$ 为小于 S 的最优获胜团体。并且，如果再加入任何一个备选团队，一定超过目标任务规模。如果加入一个备选团队等于目标任务规模，那么 $WinTeamSet[S]$ 一定不为空。如果加入一个备选团队还不满足目标任务规模，那么寻找到的 $S-k$ 一定不是小于 S 的第一组有结果的任务规模。由于备选团体的任务规模一定可以满足目标任务规模，再候

选节点中，选择一个竞价报价最小的一个团队即可。算法 1 中，用 *maxCapbility* 标记了这个最大不为空的任务规模 $S-k$，因此，可以直接在后续计算中适用。算法如 2 所示： 算法 中，算法的时间复杂度为 $O(1)$，因此，整个胜利者团体选

算法 2 Winning-Bid Selection Algorithm Addition

输入： S,$WinTeamSet$,N，$BV[N]$, $TC[N]$，$maxCapbility$
输出： $WinTeamSet[S]$
1: $x \leftarrow WinTeamSet[maxCapbility]$
2: $newTeam \leftarrow$ 在除了 x 中获胜团队组外，选择一个 $min(BV[i])$ 的团队
3: $WinTeamSet[S] \leftarrow$ x $\cup$ newTeam

择的算法的整体时间复杂度为 $O(SN)$。可以直接计算出目标任务规模的最佳选择的获胜团体，保证在满足成本最小的前提下，团体数量最少。

3.5.4 基于信誉的团队付款算法（CTP）

上一节讨论了如何选出最佳的获胜团体。本节要在选出最佳团体的基础上，根据基于信誉的团队付款算法（Credit-based Team Payment algotirhm for BNTC，CTP）给每个获胜团队定价。

首先，本文定义每个团队x为完成可完成的子任务的效益 $Utilv$ 为如公式（3-38）所示。

$$Utilv = TC_x / B_x \tag{3-38}$$

定义候选团队对任务 S 竞标的获胜团队集合的平均效益 $eUtilv$ 为如公式（3-39）所示。

$$eUtilv = S / \sum_{x \epsilon \chi} B_x \tag{3-39}$$

那么，对于不包含团队 c 的候选团队对任务 S 竞标的获胜团队的平均效益为如公式（3-40）所示。

$$eUtilv = S / \sum_{x \epsilon \chi_{-c}} B_x \tag{3-40}$$

VCG模式的分配定价模型中，工人的定价不是由该工人自己决定的，而是根据外部定价模式中，由假设在该工人不参与竞标的情况下，在新的候选人中选择获胜者，根据重新选择出的获胜者的效益给该工人定价。因此，本文定义对获胜团队x的定价为Pay_x，如公式（3-41）所示。

$$Pay_x = tc_x * ((1/eUtilv + 1/Utilv_{min})/2) + (R_0 - R) * \varphi \tag{3-41}$$

其中，R_0 是奖励分配的基准值，φ 是奖励分配的调整参数。算法中设定基准信誉值 R_0，如果当前信誉值低于基础信誉值，分配的奖励相应减少；反之，分

配的奖励会多。奖励值根据设定的基础信誉值的变化而变化。对于基于信用的团队付款算法描述如算法 3 所示。

算法 3 Rewards Payment Algorithm

输入： $S, N, BV[N], TC[N], \chi$
输出： Reward $Payment_{\chi}$
1: **for** all $x \epsilon \chi$ **do**
2: $TC \leftarrow TC_{-x}$
3: $BV \leftarrow BV_{-x}$
4: 在不包含 x 的候选团队中根据算法 1 和 2 重新计算出满足目标规模任务的结果 χ_{-x}
5: 从 χ_{-x} 选取 $Utilv_{min} = minimum(Utilv)$
6: $payment_x \leftarrow Pay_x$
7: **end for**

算法 3 中，需要依次对获胜组中的每个获胜团队进行竞价，表明定价算法的流程中，每一个工人的定价都要执行一次分配算法。因此，算法的时间复杂度是分配任务算法的时间复杂度的n 倍。即，$O(A * S^{'}(N-1)^2) = O(ASN)$。上文中提到，该算法中为获胜团队定价的策略为，在不选择该团队的选择其他团队完成这个任务的情况下，用新的获胜团体定价。因此，能成功获取新的获胜团队集合的前提条件为，除了该获胜团体外，剩下的候选团体有能力完成任务。因此，满足公式（3-42）：

$$\sum_{i \epsilon N_{-x}} tc_i \geqslant S \tag{3-42}$$

由于网络状态是实时的，每个车辆团队的规模最小的下限为之前设定的值 θ，上限为扫描区域可容纳车辆的最大值，任务发布者发布的任务规模不超过网络容量的最大值，可以是在网络容量控制范围内的任意规模，根据任务发布者的需求决定。但是也有如下情况：给一个获胜团队定价时，该团体规模比较大，在候选团队中不考虑这个团队时，剩下的候选团队的总规模无法满足目标规模的任务，如公式（3-43）所示。

$$\sum_{i \epsilon N_{-x}} tc_i < S \tag{3-43}$$

例如，任务规模 S=100，所有候选团队的总规模为 120，获胜团队之一为 30，由此可知，如果不考虑该团队，所有团队总规模为 90 （小于100），不满足算法运行条件。因此，缺少该团队就无法完成目标规模任务的团队，称为··至关重要团队”（“*CriticalTeam*”），该团队的定价无需根据重新选择出的获胜团队定价。其他获胜团队称为“普通团队”（“*OrdinaryTeam*”）。对于“至关重要”的团队的定价，用所有团队中付款额度最高的团队的定价付款，表示付款值为最多的，即付款为公式（3-44），对于“普通团队”，按照公式（3-41）进行付款。

$$CriticalPay_x = tc_x * (1/Utilv_{min} + (R_0 - R)^2) * \varphi \tag{3-44}$$

因此，付款定价的算法中，对于每一个团队，首先要判断是否是至“关重要团队”，如果是“普通团队”，按照公式（3-41）定价，如果是“至关重要”团队，按照公式（3-44）定价。完整的付款定价算法如算法4所示：

算法 4 Rewards Payment Algorithm

输入： $S, N, BV[N], TC[N], \chi$
输出： Reward $Payment_{\chi}$

for all $x \epsilon \chi$ **do**
  $TC \leftarrow TC_{-x}$
  $BV \leftarrow BV_{-x}$
  if x 是一个“$CriticalTeam$” **then**
    $payment_x \leftarrow CriticalPay_x$
  else
    在不包含x的候选团队中根据算法1和2 重新计算出满足目标规模任务的结果 χ_{-x}
    从 χ_{-x} 选取 $Utilv_{min} = minimum(Utilv)$
    $payment_x \leftarrow pay_x$
  end if
end for

3.5.5 算法性能分析

前面对分配算法和支付算法做了定义，本节分析并证明系统的合理性和社会福利最大值。

理论1： BNTC 系统具有个人合理性。

证明： 以背包算法为核心的任务分配算法中，全局最优解不是局部最优解。如果团队 i 是获胜团队之一，团队 i 如果完成分配的任务，可以通过做任务获得的报酬为： $u_i = pay_i - cost_i$。通常，只要该团队的效用大于 $(1/eUtilv + 1/Utilv_{min})/2$，并且信誉值大于$R_0$，那么报酬 u_i 是一个大于0 的数，表示做任务总会获得报酬。当信誉值低或者效用值低，这个时候可能u_i 是负数。在获胜团队中，可能只有一小部分团队会这样，或者没有团队的效用是负数，是否出现这种情况依靠实时的车辆团队的不同报价和信誉值。

理论2： BNTC 系统可以达到社会福利最大值。

证明： 社会福利考虑任务发布者、工人和系统三个因素。从任务发布者角度来说，社会福利最大意味着完成一件任务过程中，任务发布者需要指出的花费最小。从工人角度来说，通过算法选中的所有车辆团队完成任务需要花费的总成本最低，并且每个工人得到合理的报酬支付。从系统角度来说，系统希望选取的团队数最少，越少的团队数，任务分块越完整，算法存在的意义越大。根据理论1 可知，成本越小，任务发布者的总付款才能越小。因此，社会福利主要取决于成本、支付和成本的差值、获胜团队的数量。规模和车辆团队数量，每50时间片段，获取一次实时车辆团队。为了真实的评估算法的时间结果，本实验中主要评估的系统参数如下：车辆团队做任务的成本，任务发布者支付的奖励花费、

社会福利、超付率和获胜团队数量。

3.6 安全性分析

本节将对基于区块链的实时车辆众包系统 BNTC 进行安全性分析。区块链安全性被正式定义为持久性和活跃性。持久性可以保持公共分类帐的稳定性。活跃度意味着一定时间后，有效交易将被保证包含在区块链中。系统中首选从发布任务节点和 RSU 节点这些具有记账能力的节点中选取一部分值得信任的成员作为委员会成员对信息进行环签名验证提交。环签名的委员会成员根据信誉值和任务成功率进行选定。委员会成员验证一笔交易会获取相应的费用，该阶段的安全性取决于委员会成员的可信度。对于历史信誉值、历史车辆完成率以及任务分配结果是公开的。如果节点作恶，可以直接提出投诉。由于竞标信息的匿名性，发布任务节点无法获知竞标信息的来源。因此对于众多竞标信息，可靠公平地选取最终的竞标获胜者。此外，对于团队的竞标信息时经过整合后参加竞标的。因此，发布任务节点无法直接获取单个车辆的竞标信息。这样的设计进一步保证了系统的匿名性。

3.6.1 身份证书不可伪造性

PCA 部门使用 PS 签名在提交的消息 $g_1^{cs_i}$ 签名，为每一位车辆节点注册者生成匿名身份证书，身份证书的不可伪造性可以归结为 PS 签名的不可伪造性。只有授信机构的数据库才保存账户名和用户的信息之前的关系，并且，众包任务数据仅仅绑定了身份证书，不是私人信息，因此，可以有效帮助用户保护隐私。此外，由于身份证书的不可伪造性和无法链接性，恶意用户无法获取钱包用户的身份证书和私钥，没有恶意用户可以检查其他用户的钱包或窃取硬币，因此保护每个用户的钱包非常有用。

3.6.2 消息签名验证的不可伪造性

区块链中消息的签名与验证过程使用 schnorr 签名验证方式，使用非对称加密对消息进行加密。schnorr 签名验证速度比较快并且步骤比较简单。这种签名验证方式比较适用于区块链中消息实时性比较强的项目，因此在本文设计的实时性车辆系统中使用了这种消息签名方式。schnorr 签名已经具有安全性证明[48]。相反，关于 ECDSA 可证明的安全性的最著名的结果依赖于更强的假设。因此，schnorr 签名可以保证签名的可靠性，真实地证明消息确实由交易发出者发出。环签名也是一种安全的签名策略，委员会的成员不能伪造签名者的签名。环签名

的另外一个优势是无条件匿名性。签名者使用委员会中的成员的公钥生成签名，攻击者无法获知参与生成环的成员。

3.7 本章小结

本章主要详细描述 BNTC 模型运行流程，并针对 BNTC 模型提出获胜团队选择算法（WTS）和奖励定价算法（CTP），并对两个算法进行设计与分析。最后对 BNTC 模型的合理性与安全性进行分析。

第 4 章　BNTC模型实验设计与分析

上一章节介绍了实时车辆网络团体模型运行过程以及获胜团队选择算法和预计信用的团队付款算法的设计。本章节主要进行对上一节设计的算法进行实验

4.1　算法实验结果

本节中，首先介绍实验环境和所需的数据集，然后用实验验证 WTS 算法和 CTP 算法的效果，对上一节的算法设计进行实验结果分析。

4.1.1　数据集描述以及实验设计

本小节主要介绍仿真数据集。本实验用 Python 语言进行模拟不同用户的投标状态。实验中选用的数据集为意大利的 Bologna 城市中采集的数据集[50]，共有 20000 辆车的状态。此数据集收集了一天中，早上 8 点到 9 点一个小时中所有路径的车辆运行状况。此数据集的路径地图如图 4-1 所示。 当多辆车聚集在十

图 4-1　　Bologna 区域地图

字路口的同一条路时（实验中设定的阈值为 10 辆车），这中情况被认为形成了一个车辆团队。实验中，任务发布者根据本身的需求和实时网络中车辆团队可承受的最大能力，在不超过最大能力的前提下，根据自身需求设定任务类型和规模。RSU 传感器安装在交通信号灯上，并且，上一章中提到，每个传感器仅检测车辆迎面来的道路上的车辆，这里包括路上所有的车道的车辆。当路口发生车

辆聚集情况，处于空闲且有意愿做任务的车辆与 RSU 连接，RSU 收集到的信息形成车辆网络。在实验中，认为每一辆车都处于空闲状态且与 RSU 连接，道路上所有车辆都可以接收任务。不同车辆对相同的任务竞价报价是在合理范围内随机产生的。 实验进行前，首先处理数据集。通过用 sumo 运行数据信息发现，

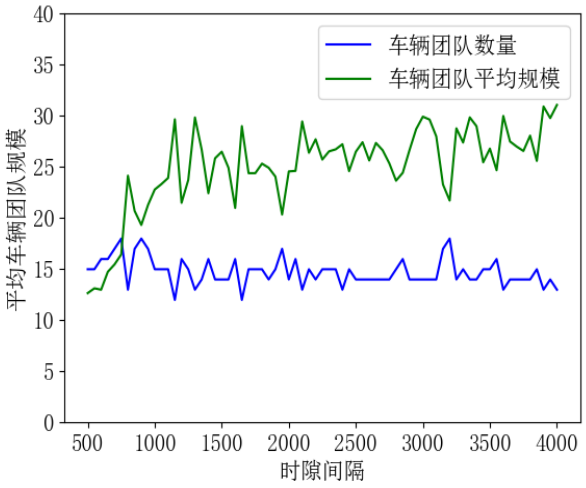

图 4-2　　数据集中的路上车辆平均规模

sumo 运行时间片段 1000-4000（1时间片段为1/7秒）内车辆较为密集，因此，实验中选取该时间段进行数据提取。图4-2 展示了 1000-4000 检测时间内的路面上车辆团队的平均数量和车辆团队平均规模。

4.1.2　实验结果

首先，对实验中用到的参数进行初始化，如表 4-1 所示。 其中，α_1，α_2 和

表 4-1　　主要参数的初始化

参数	初始值
车辆信誉值r	1.0
车辆完成率q	0.8
调整参数δ	0.5
成本竞价报价变化范围	[1,1.5]
ω	0.5
$\alpha_1, \alpha_2, \alpha_3$	0.7,0.2,0.1
R_0,φ	0.5,10

α_3 分别表示在系统中用到的公式（3-26）中的成本、超付和获胜团队数量的调整参数。使得最大福利在模拟数据集中处于100 左右的数值大小。R_0 和 φ 是支付奖励的调整参数，根据经验值被初始化。

本实验的对比实验为 MCBS 算法[11]和 DQDA 算法[14]。MCBS 算法中，主要使用贪心的原则进行选取获胜团队，使覆盖集合最大，定价算法中使用外部定价中的最高付款策略进行效益评估定价。DQDA 算法是基于数据质量的评估算法进行的，需要先对数据集进行 EM 算法评估运算。对比实验中假设数据都是可信的，进行 EM 运算的矩阵中，每个元素都是 1。本文中使用的都是真实数据集的测试数据，车辆是数据集中真实存在的。每辆车的完成情况根据车辆设置的概率随机生成，每辆车的竞价报价根据初始参数表中的竞价报价范围规定下随机生成。由于交通网络的实时变化，不同时刻，团队的组成不相同，团队报价不一定相同，车辆网络中的团队规模和信誉值等都不同。因此，即使目标任务规模相同，不同时刻的中标结果的社会成本、社会支付、社会福利也不一定相同。下面分别对不同任务规模下的社会成本、社会福利、社会支付、超付率和获胜团队这些指标对算法进行性能测试实验。对团队信誉值对超付率的影响和车辆信誉值的变化进行实验展示。

社会成本（Social Cost）：基于不同的目标规模任务负载，同一时刻不同车辆团队竞价，最终被算法选择的优胜团队的总成本显示在图 4-3 中。实验结果表明，随着任务规模增大，车辆团队需要付出的成本逐渐增加。在相同条件下，BNTC 的算法计算得出的成本在三种算法中是最低的，BNTC 算法可以获得最优解。BNTC 中，WTS 算法计算得出选出的优胜团队和社会成本。WTS 算法的基本思路是将多变量的多重背包算法通过满意度公式变成普通背包算法。

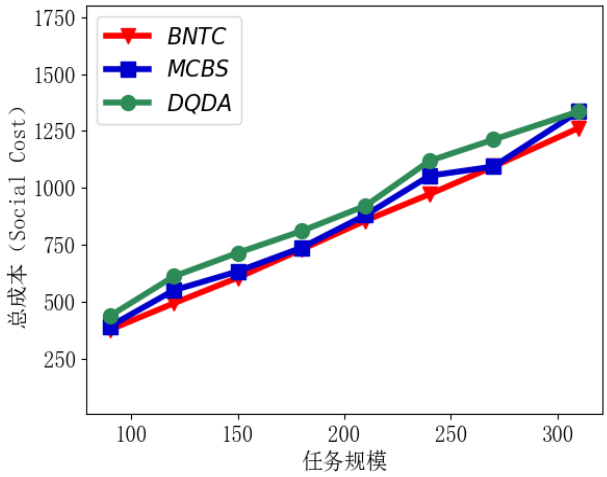

图 4-3　　三种算法的总成本对比

社会福利（Social Welfare）：社会福利的实验结果显示在图 4-4 中。根据图中显示，BNTC 算法达到的社会福利是三个算法中的最大值。社会福利公式最优的是首先满足成本最小；若成本最小再看超付最少；若超付相等，再看优胜团队

数量最少。因此，社会福利一定最优一定满足以上三个标准之一。

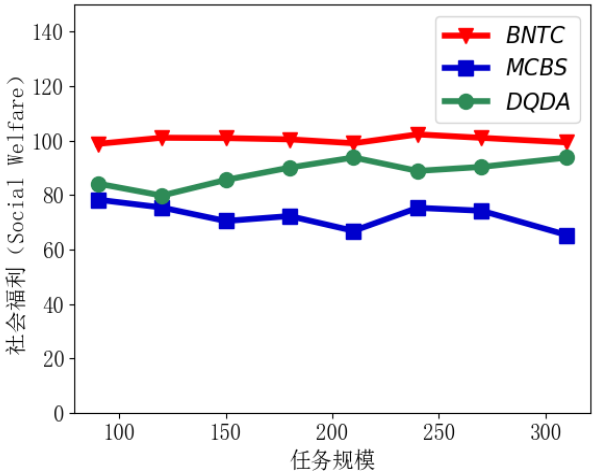

图 4-4　　三种算法的社会福利对比

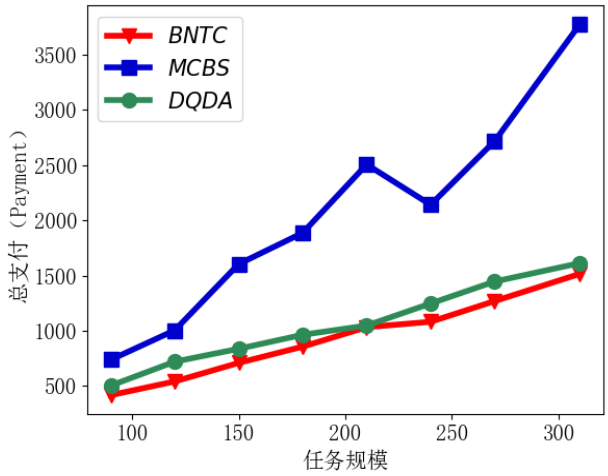

图 4-5　　三种算法的总支付对比

社会支付（Social Payment）： 任务发布者给选中的车辆团体制定支付奖励金额。实验结果如图 4-5 所示。实验结果表明，在相同目标规模任务下，BNTC总的支付奖励是三个算法中最少的。并且，支付奖励随着目标任务规模的扩大而上升。这里，实验中，MCBS 和 BNTC 的支付方式相似，都是根据算法 4 确定支付奖励金额，不同的是选取候选团队的方式。MCBS 选择团队考虑的是根据贪心算法选取最合适的效用率的团队得到局部最优而不是全局最优。在一些情况下，MCBS 如果除去该团队再重新选择获胜团队会获得更好的结果。因此，会出现 MCBS 比 BNTC 方案计算得出的社会支付更少的情况，正如图中 200-300 目标任务规模的情况。

超付率（OPR）：基于超付率的实验中表明，超付率与任务的数量并不相关。实验中得到的结果显示，BNTC 的超付率基本在 0.18 左右。MCBS 的超付率变化依然是因为贪心算法的再次选择可能会出现更优的策略。在某种情况下（任务规模是210），DQDA 的超付率是最优的，社会支付更接近真是成本。但是同时，DQDA 的社会成本和社会支付也是相当高的，只能说 DQDA 算法中，成本和支付奖励的差距不是很大。实验结果如图 4-6 所示。

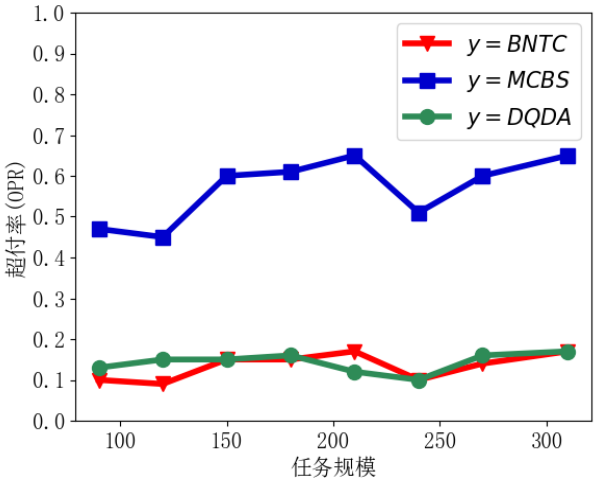

图 4-6　　三种算法的超付率对比

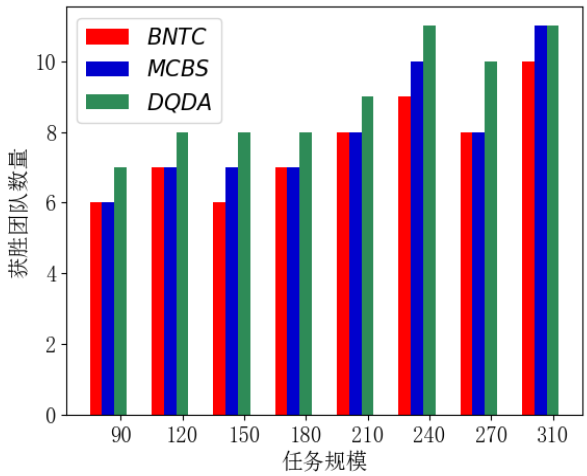

图 4-7　　三种算法的获胜团队数量对比

获胜团队数量（Winning Team Count）：通过算法选择出的获胜团队数量显示在图 4-7 中。在大部分情况下，根据 BNTC 中的两种算法得到的获胜团队数量比其他两种算法要好。然而，BNTC 中算法的基础是背包，不是贪心，因此在

团队规模上不一定总是获得最少的团队数量。贪心算法获得的团队数量有的时候要更少，如图中目标团队规模是 120 时的结果。

BNTC信誉值： 一个车辆团队的信誉值变化对超付率的影响如图 4-8 所示。在任务相同，分配结果相同的情况下，团队的信誉值研究，数值范围是[0-1]，团队获得的报酬随着该车辆团队信誉值的上升而上升，任务的超付率也随之逐渐上升。

车辆作恶、上传失败等会造成任务未能在规定时间内完成，车辆因此受到惩罚，信誉值改变，改变方式如前面公式（3-14）所示。多次任务成功才能使信誉值回升到失败之前的信誉值。如图 4-9 所示，红框表明任务失败。图中显示，当车辆节点参与执行任务的次数在 5-10 之间且信誉值为 1 的时候，两次失败，需要 4 次成功信誉值回升到 1。执行任务失败带来了连带损失。

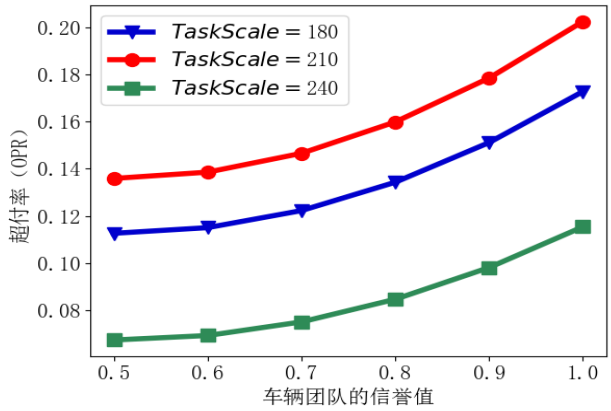

图 4-8　　BNTC 模型中超付比与信誉值的关系

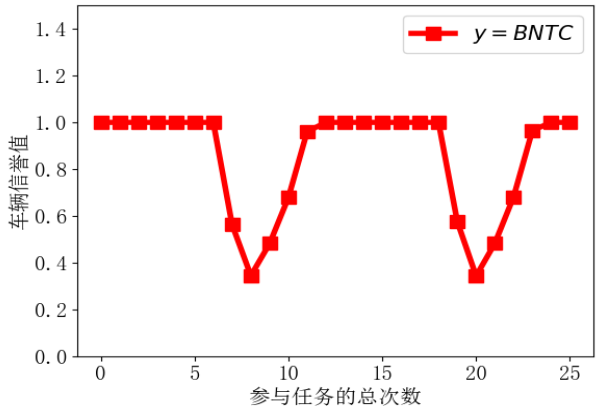

图 4-9　　BNTC 模型中车辆信誉值变化

本节主要对 WTS 算法和 CTP 算法进行实际的实验测试。对比 MCBS 算

法[11]和 DQDA 算法[14]，BNTC 有最低的社会成本和最低的奖励支付。超付率和社会成本关联性不是很大，因此，在某些情况下，BNTC 的超付率可能更高。

4.2 去中心化的 BNTC 系统实验测试

前面对 BNTC 系统中的两个主要算法进行模拟测试，定义并验证了社会成本最高的结论。众包机制在中心化平台中会带来一些安全隐患：高额的交易费用、一定概率的隐私泄露等问题。本章的实验要将算法真正部署到区块链中，用区块链建立可用的 BNTC 系统，并测试系统的效果。本节首先介绍选用的实验平台，再介绍智能合约以及部署的方案，最后测试实验效果。

4.2.1 实验环境

本文使用的区块链平台是用以太坊搭建的私有链，用三个树莓派和一台笔记本电脑模拟区块链中的节点，如图 4-10 所示。笔记本模拟发布任务节点。树莓派的配置和笔记本的配置如表所示。软件环境需要安装 golang.13.3，geth1.7.0 环境和以太坊钱包（V 0.9.2）。

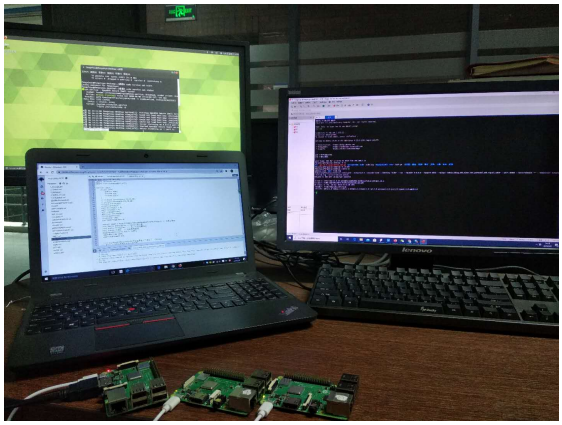

图 4-10 实验使用的基础设备

表 4-2 设备参数

设备	CPU	内存
树莓派	ubuntu16.04	8.00GB
笔记本	AMD 8700	16.00GB

本文使用智能合约自动执行数据收集与共享。首先，使用语言 solidity 在 Remix 上编写并测试智能合约。对于智能合约部分，无需安装任何软件，也无需本地调试测试，直接在 Remix 网站上运行即可。

4.2.2 智能合约执行流程

实验中，众包过程主要使用智能合约完成。众包过程的智能合约主要有三个：主调用智能合约、WTS 选择优胜团队算法智能合约和 CTP 确定支付算法智能合约。调用的系统实现如图 4-11 所示。任务的执行过程是由任务发布节点调用合约查看现有团队信息开始的。

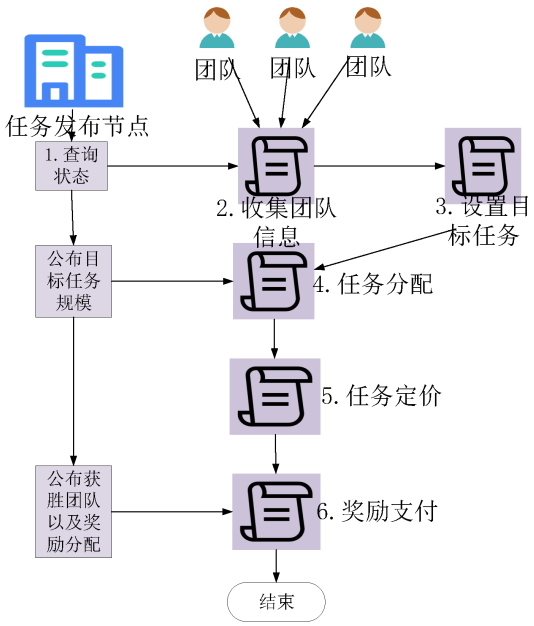

图 4-11　　智能合约调用过程

Init：云/边缘服务器首先调用 Init 函数。在 Init 函数中，智能合约定义了数据共享机制的所有相应变量，例如卖方列表 Slist，初始化后，智能合约在添加功能中经过验证后，智能合约将卖方添加到 Slist 中。在将智能合约部署在区块链网络中之后，平台和所有数据卖方都可以对其进行访问并开始数据共享。

第一步：任务发布节点调用智能合约中的 checkTeams() 函数，查看当前网络中团队在线以及规模费用情况，设置查看结束时间。并且调用 setTasker() 函数设置任务发布者。

这样做的原因有如下：

（1）调整适合的目标任务规模，为第三步做准备，以防信息不对等。如果现有网络无法完成目标规模任务，那么交易无法进行。因此，要让任务发布节点了解当前情况，做出正确的判断。

（2）任务发布节点需要了解当前的竞标价格。执行任务分配需要首先证明钱包中资金充足，任务发布节点发布任务需保证钱包中有足够多的金额支付任务的报酬。

第二步：在任务发布节点规定的时间段内，收集所有的参与竞标的车辆团队信息，调用 *addTeams*() 函数添加车辆团队信息。发布任务函数查看当前网络就设定了持续时间，在持续时间段内加入的团队为候选团队 $Teams$，超出该段时间加入的团队无效，无法参与竞拍。

第三步：任务发布节点根据查看的情况设置目标任务规模 $setTaskScale$，保证在线的车辆团队可以完成任务。

第四步：调用任务分配智能合约函数 *getWinner*()，计算出最佳的任务分配方式，如果可以执行，继续根据任务分配结果调用任务定价智能合约函数 *getPayment*()。再根据获胜团队计算出最佳定价方案。

第五步：任务发布节点将在本次竞拍中被选中的团队集合以及团队的奖励公布，并给各个团队发放奖励。该奖励是放在各个团队所在的RSU节点处的。当所属的车辆完成任务并通过检测，奖励再发放到各个车辆节点的账户中，执行批量转账的智能合约函数 $transferTokens$()。若车辆没有完成任务，资金将退回到任务发布节点的账户中。

4.2.3 资源消耗评估

4.2.3.1 注册性能评估

车辆节点、RSU 节点和任务发布节点在 PCA 进行离线注册，获取进入 BNTC 系统的资格。PCA 为每个车辆节点生成身份证书，为 RSU 节点和任务发布节点生成密钥。本实验评估离线 Golang 中身份证书和密钥对生成的性能。结果显示时间消耗以毫秒(ms) 为单位，是可以接受的，如表4-3 所示：

表 4-3　生成证书耗时

操作	实体	耗时(ms)
生成注册证书	车辆节点	166
生成密钥对	RSU 节点和发布任务节点	27

4.2.3.2 智能合约性能评估

上一小节介绍了用智能合约实现任务设置、任务分配以及任务定价等合约函数。为了展示智能合约的性能，实验中使用以太坊中的 gas 来衡量实现以及执行这些智能合约需要消耗的 gas。在以太坊联盟链中，gas 是用来作为智能合约资源消耗的计量单位。实验中设置 gas 价格为 0.000000001 (1 Gwei) /gas。2020年4月1 日，以太坊的价格大约在 141.53$ 左右，将智能合约消耗的 gas 换算成美元，大致的费用如表格 4-4 所示。两种算法仅花费1.419 $ （0.2304 + 1.189）即可获得分配和付款结果。资源消耗在合理范围内。

表 4-4 BNTC系统智能合约执行费用表

函数名	算法描述	transaction cost(gas)	execution cost(gas)
Init()	部署合约	3155990	2351810
setTasker()	设置任务发布者	65372	42180
addTeams()	添加候选团队	195379	172315
checkTeams()	查看现有候选团队	85837	64565
setTaskScale()	设置目标任务规模	42601	21137
getWinner()	获胜团队选择	1496032	1493960
getPayment()	获胜团队定价	4180347	4312675
transferTokens()	批量转账	39691	14643
总费用		6811607	8817915

4.3 本章小结

本章首先在基于算法性能对比实现了 BNTC 的 WTS 算法和 CTP 算法，以实现最大的社会福利。广泛的仿真表明，该模型的性能优于基线方法，并且实现了最大的社会福利。然后基于和系统应用，首先实现了第三方可信身份注册，并用智能合约实现两个算法。以太坊的实验表明 BNTC 模型可以在合理的成本内运行。

第 5 章 总结与展望

5.1 总结

车辆众包，作为物联网中的一个应用分支，在近几年的研究中尤为重要。先进的网络设备、传感设备和计算设备的支持，使得车辆拥有强大的计算能力，让车辆移动众包任务从理论像现实迈进一大步。交通堵塞已经成为大城市的标配，堵车造成资源能源浪费。对于聚集性现实计算力的有效利用车辆众包研究的一个方向。目前的车辆众包问题研究中，众包任务的分配具体到每一个设备的任务分配，任务对设备之间的关联性无要求，这种任务分配方式研究制约着大规模任务的分配，大规模任务可能需要多台位于同一局域网内的设备联合执行，这样的任务目前车辆移动众包模型没有考虑。本文提出了基于车辆团队为最小的任务分配单位的车辆众包模型，车辆团队的信誉、能力等根据团队中的每一位成员决定。在网络、传输、计算设备的支持下，利用团队组织形成的计算能力，以团队为最小分配单位分配大规模众包任务，可使移动众包任务可以利用相同局域网内部的联合计算资源，为大规模众包任务提供实现的可能。

移动众包任务会消耗能源、资源以及人为操作的成本。这些成本将成为众包任务的必要开销。因此，有效的激励方式对众包平台的发展具有重要的意义。由于目前模型中的车辆众包任务子任务分配到节点的模式，多任务节点多工人的分配，采用装箱算法的基本理念，以贪心算法为基础，设置分配机制。而本文设计的基于实时车辆网络模型中，实时性的短暂认为每一次只为一个大规模任务进行全网分配，因此提出基于有条件的背包算法可以找出最佳分配机制。在定价方案中，首先在原有的 VCG 模式中的定价方案基础上，加入信誉因子，对定价进行调节，进一步表明信誉对工人的影响。其次引入至关重要团队的概念，对完成任务不可缺的团队提高定价，激励团队的参与兴趣，提高任务的完成概率。

移动众包任务中，工人不仅考虑成本，还会考虑工人的隐私安全问题。中心化的平台隐私安全得不到最优的保障，车辆信息的传输泄露风险高，提高车辆移动众包的安全性能也是目前研究的一大热点。目前，区块链作为去中心化、保护隐私的基础平台，可达到安全保护的目的。本文使用区块链作为基础平台，拥有服务器的边缘设备和任务发布节点可进行记账，获取奖励，车辆节点作为轻节点对区块链提供验证服务。

以上是本文主要的研究内容，通过实验表明对车辆众包的发展有积极的作用。

5.2 展望

本文提出了对于车辆形成的团队进行众包分配的框架，但是也存在一些不足与解决方案提议：

1. 但对于团队内部如何进行任务分配，没有进行详细的设计。车辆团队内部任务的联合执行需根据设定不同的任务机制进行分配，这一部分需要更详细的规划与实验。由于车辆团队的实时组件，团队中红绿灯对车辆的离开与到达的影响从而改变团队的规模，这一部分展开详细分析与设计，用以提高车辆团队的稳定性与团队采集的准确性。

2. 文章中使用以太坊进行实验，但现实的 IoV 实验中，以太坊的硬件要求车辆设备无法达到，需要更轻量级的区块链平台进行。现有的 DAG 区块链平台是面对物联网设备开发的，但由于目前的 DAG 区块链的技术对于系统的安全性还需要进一步实验和验证。因此，适用于 IoV 的区块链平台是一个重要的开发方向。

3. 网络传感器的延迟对众包任务的完成速度也有一些影响，5G 技术的发展对 IoV 的发展起到积极的促进作用。制定在新的硬件设备上的任务传输协议策略，会对车辆众包起到积极的效果。

参考文献

[1] Yadav L, Kumar S, KumarSagar A, et al. Architechture, Applications and Security for IOV: A Survey[C]. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2018: 383–390.

[2] Qiu T, Liu J, Si W, et al. Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks[J]. IEEE/ACM Transactions on Networking, 2019, 27 (3): 1028–1042.

[3] Qiu T, Li B, Qu W, et al. TOSG: A topology optimization scheme with global small world for industrial heterogeneous Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2018, 15 (6): 3174–3184.

[4] Hu S, Su L, Liu H, et al. SmartRoad: A crowd-sourced traffic regulator detection and identification system[C]. In 2013 ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2013: 331–332.

[5] Ni J, Zhang A, Lin X, et al. Security, privacy, and fairness in fog-based vehicular crowdsensing[J]. IEEE Communications Magazine, 2017, 55 (6): 146–152.

[6] Li L, Liu J, Cheng L, et al. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19 (7): 2204–2220.

[7] Zhang Y, Lu Y, Huang X, et al. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69 (4): 4298–4311.

[8] Yang D, Xue G, Fang X, et al. Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones[J]. IEEE/ACM transactions on networking, 2015, 24 (3): 1732–1744.

[9] Jin H, Su L, Nahrstedt K. CENTURION: Incentivizing multi-requester mobile crowd sensing[C]. In IEEE INFOCOM 2017-IEEE Conference on Computer Communications, 2017: 1–9.

[10] Wang L, Yu Z, Yang D, et al. Collaborative Mobile Crowdsensing in Opportunistic D2D Networks: A Graph-based Approach[J]. ACM Transactions on Sensor Networks, 2019, 15 (3): 1–32.

[11] Gao G, Xiao M, Wu J, et al. Truthful Incentive Mechanism for Nondeterministic Crowdsensing with Vehicles[J]. IEEE Transactions on Mobile Computing, 2018, 17 (12): 2982–2997.

[12] Chen H, Guo B, Yu Z, et al. CrowdTracking: Real-Time Vehicle Tracking Through Mobile Crowdsensing[J]. IEEE Internet of Things Journal, 2019, 6 (5): 7570–7583.

[13] Yin B, Wu Y, Hu T, et al. An Efficient Collaboration and Incentive Mechanism for Internet of Vehicles (IoV) With Secured Information Exchange Based on Blockchains[J]. IEEE Internet of Things Journal, 2020, 7 (3): 1582–1593.

[14] Chen W, Chen Y, Chen X, et al. Toward Secure Data Sharing for the IoV: A Quality-Driven Incentive Mechanism with On-Chain and Off-Chain Guarantees[J]. IEEE Internet of Things Journal, 2019, 7 (3): 1625–1640.

[15] Taleb T, Sakhaee E, Jamalipour A, et al. A stable routing protocol to support ITS services in VANET networks[J]. IEEE Transactions on Vehicular technology, 2007, 56 (6): 3337–3347.

[16] Xu Y, Chen X, Liu A, et al. A latency and coverage optimized data collection scheme for smart cities based on vehicular ad-hoc networks[J]. Sensors, 2017, 17 (4): 888–901.

[17] 付溢. 区块链交易数据隐私保护研究与实现[D]. 北京: 北京交通大学, 2019.

[18] Xiong L, gen Li F, ke Zeng S, et al. A Blockchain-Based Privacy-Awareness Authentication Scheme with Efficient Revocation for Multi-Server Architectures[J]. IEEE Access, 2019, PP (99): 1–1.

[19] Lu Z, Wang Q, Qu G, et al. Bars: a blockchain-based anonymous reputation system for trust management in vanets[C]. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018: 98–103.

[20] Zhaofeng M, Weihua H, Hongmin G. A new blockchain-based trusted DRM scheme for built-in content protection[J]. EURASIP Journal on Image and Video Processing, 2018, 38 (4): 91.

[21] Yao Y, Chang X, Mišić J, et al. BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. IEEE Internet of Things Journal, 2019, 6 (2): 3775–3784.

[22] 张帅, 延安, 贾敏智. 基于区块链的众筹智能合约设计[J]. 计算机工程与应用, 2019, 55 (8): 220–225.

[23] Ali Z H, Badawy M M, Ali H A. A novel geographically distributed architecture based on fog technology for improving Vehicular Ad hoc Network (VANET) performance[J]. Peer-to-Peer Networking and Applications: 1–28.

[24] 郑灿健. 基于V2X通信的高能效传输技术研究[D]. 深圳: 深圳大学, 2018.

[25] Yu D, Ning L, Zou Y, et al. Distributed spanner construction with physical interference: constant stretch and linear sparseness[J]. IEEE/ACM Transactions on Networking, 2017, 25 (4): 2138–2151.

[26] 陈稼珅. 基于区块链智能合约的去中心化在线众包机制[D]. 杭州: 杭州电子科技大学, 2019.

[27] 张永棠. 一种移动众包系统在线激励机制优化算法[J]. 计算机应用研究, 2019 (9): 2588–2589.

[28] Yao H, Mai T, Wang J, et al. Resource Trading in Blockchain-Based Industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2019, 15 (6): 3602–3609.

[29] Li Z, Yang Z, Xie S. Computing Resource Trading for Edge-Cloud-Assisted Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2019, 15 (6): 3661–3669.

[30] Feng Z, Zhu Y, Zhang Q, et al. TRAC: Truthful auction for location-aware collaborative sensing in mobile crowdsourcing[C]. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications, 2014: 1231–1239.

[31] Vickrey W. Counterspeculation, auctions, and competitive sealed tenders[J]. The Journal of finance, 1961, 16 (1): 8–37.

[32] Clarke E H. Multipart pricing of public goods[J]. Public choice, 1971: 17–33.

[33] Groves T. Incentives in teams[J]. Econometrica: Journal of the Econometric Society, 1973: 617–631.

[34] Nakamoto S, Bitcoin A. A peer-to-peer electronic cash system[J], 2008.

[35] Maesa D D F, Mori P. Blockchain 3.0 applications survey[J]. Journal of Parallel and Distributed Computing, 2020, 138: 99–114.

[36] Gayoso Martínez V, Hernández-Álvarez L, Hernández Encinas L. Analysis of the Cryptographic Tools for Blockchain and Bitcoin[J]. Mathematics, 2020, 8 (1): 131.

[37] Zhu J, Li Q, Wang C, et al. Enabling Generic, Verifiable, and Secure Data Search in Cloud Services[J]. IEEE Transactions on Parallel and Distributed Systems, 2018, 29 (8): 1721–1735.

[38] Hong S. P2P networking based internet of things (IoT) sensor node authentication by Blockchain[J]. Peer-to-Peer Networking and Applications, 2020, 13 (2): 579–589.

[39] Yang Z, Yang K, Lei L, et al. Blockchain-Based Decentralized Trust Management in Vehicular Networks[J]. IEEE Internet of Things Journal, 2019, 6 (2): 1495–1505.

[40] Jiang Y, Lian Z. High Performance and Scalable Byzantine Fault Tolerance[C]. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2019: 1195–1202.

[41] Szabo N. Formalizing and Securing Relationships on Public Networks[J]. First Monday, 1997, 2 (9): 1050–1062.

[42] Wang Q, Qin B, Hu J, et al. Preserving transaction privacy in bitcoin[J]. Future Generation Computer Systems, 2017, 107 (10): 950–968.

[43] Li X, Han Y, Gao J, et al. Secure hierarchical authentication protocol in VANET[J]. Iet Information Security, 2020, 14 (1): 99–110.

[44] Pointcheval D, Sanders O. Reassessing security of randomizable signatures[C]. In Cryptographers' Track at the RSA Conference, 2018: 319–338.

[45] Yu Y, Zhao Y, Li Y, et al. Blockchain-Based Anonymous Authentication With Selective Revocation for Smart Industrial Applications[J]. IEEE Transactions on Industrial Informatics, 2020, 16 (5): 3290–3300.

[46] Liu D, Alahmadi A, Ni J, et al. Anonymous reputation system for iiot-enabled retail marketing atop pos blockchain[J]. IEEE Transactions on Industrial Informatics, 2019, 15 (6): 3527–3537.

[47] 孙玮. 基于动态群签名的隐私CA系统设计与实现[D]. 沈阳: 东北大学, 2015.

[48] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of cryptology, 2000, 13 (3): 361–396.

[49] Maxwell G, Poelstra A, Seurin Y, et al. Simple Schnorr Multi-Signatures with Applications to Bitcoin. 2018. https://eprint.iacr.org/2018/068.

[50] Bedogni L, Gramaglia M, Vesco A, et al. The Bologna Ringway Dataset: Improving Road Network Conversion in SUMO and Validating Urban Mobility via Navigation Services[J]. IEEE Transactions on Vehicular Technology, 2015, 64 (12): 5464–5476.

关于国际工程师学院人才培养模式情况说明

天津大学国际工程师学院借鉴法国工程师培养理念和模式，结合我国本土教育特色，积极探索工程教育改革路径，以多学科交叉融合为特色，聚焦科学技术前沿领域，服务国家重大战略需求，是天津大学研究生层面的工程教育改革试验区。

2017 年，国际工程师学院通过法国工程师职衔委员（ CTI ）授予的最高等级六年期认证和欧洲工程教育（ EUR-ACE ）专业认证。这标志着学院的办学模式、人才培养质量得到国际认可，学院毕业生也将获得由法国工程师职衔委员会授权颁发的法国工程师文凭。

国际工程师学院全面推进课程改革，总课时约 2000 学时，重新配置理论课、练习课和实践课比例，使得实践学时（练习和实践课）占到总学时的 2/3。教学内容与企业工程实际项目深度融合，累计 10 个月三阶段的渐进式实习，实现学校教育与企业需求的“无缝衔接”。

研究生在学期间着力加强工程实践能力、创新能力和解决实际问题能力的锻炼和提升，不强制要求发表学术论文。该培养体系和学位申请标准已于天津大学学位评定委员会第 97 次会议审议通过。特此说明。

发表论文和参加科研情况说明

（一）发表的学术论文

[1] Jianrong Wang, Xinlei Feng, Tianyi Xu, Huansheng Ning, Tie Qiu. “Blockchain based Model for Nondeterministic Crowdsensing Strategy with Vehicular Team-Cooperation”, IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3000048.

致 谢

时间过得非常快，三年的研究生生活收获满满，转眼间就要花上圆满的句号。回想本科四年研究生三年，七年的时光，最美的年纪，遇到最美的天津大学。在这期间，非常感谢我的老师，我的同学以及实验室的每一位同胞，让我在天大收获了很多。

首先我要感谢我的导师陈世展老师，做事严谨，认真负责，总大局出发，为了我们的未来着想。王建荣老师思维开阔，把握科学前沿方向，前瞻性十分强，给了我正确方向的指引，让我爱上了科研。邱铁老师对待科研的态度一丝不苟，严谨、科学、系统的掌握各个方面的知识，对待学生严格理性，在科研上给了我启示和指导，让我明白科研之路应该如何走。徐天一老师，在生活上、科研上，把自己知道的东西都教给我们，并且给予鼓励和爱护，像是科研生活上的领路者，带领我们前进。几位良师，让我发自内心的崇敬和感激。

在论文构思中，我要非常感谢我的两个师弟，胡登成和付钊，互相交流和讨论让我有了很多思路并且明白了很多，胡登成还给了我很多实验中的指导，再次非常感谢。实验中，因为疫情大部分在家进行，实验室的同学陶泽远、于庆洁、段文佳和刘贺，我们经常一起讨论并互相监督学习，感谢大家的陪伴。也是因为疫情在家，更要感谢父母的照顾，每日照顾我的饮食起居，让我更专心地投入论文工作。

感谢天津大学这个拥有百年历史的名校，让我得到了良师益友，得到了知识积累，得到了毅力和能力的锤炼，这是我生命中一段非常宝贵的财富。