****

**本 科 毕 业 论 文（设计）**

|  |  |
| --- | --- |
| 课题名称 | 基于区块链的网约车路径预警系统的设计与实现 |
| 学 院 | 计算机科学与网络工程学院 |
| 专 业 | 计算机科学 |
| 班级名称 | 计科174 |
| 学生姓名 | 李诗云 |
| 学 号 | 1706100092 |
| 指导教师 | 彭滔 |
| 完成日期 |  |

教 务 处 制

基于区块链的网约车路径预警系统的设计与实现

计科174 李诗云

指导教师:彭滔

摘要 本研究针对现有网约车平台安全事故频发的问题，旨在运用区块链技术特性，实现可靠的网约车路径预警系统。可以在杜绝人为因素影响的前提下，保证记录的真实性，并通过自动化且不可逆的预警机制，提高网约车模式的安全系数。文中的设计主要通过以太坊公链，实现不可篡改、公开透明的信息记录。Solidity智能合约自动进行核心逻辑的施行。Web3进行区块链与前后端的交互 。ReactNative结合高德地图API实现易迁移的移动端APP开发。

关键词 区块链；网约车；智能合约；

**ABSTRACT** Aiming at the frequent safety accidents of the existing ride-hailing platform, this study aims to realize a reliable ride-hailing path warning system by using the technical characteristics of block chain.The authenticity of the records can be guaranteed on the premise of eliminating the influence of human factors, and the safety factor of online car-hailing mode can be improved through automatic and irreversible early warning mechanism.The design in this paper is mainly through the Ethereum public chain to achieve tamper-proof, open and transparent information records.Solidity smart contracts automatically implement core logic.Web3 interacts with the blockchain and front and back ends.ReactNative is combined with Amap API to realize mobile terminal APP development that is easy to migrate.

**KEY WORDS** blockchian； online car-hailing；smart contract

目录

[1 前 言 2](#_Toc70451621)

[1.1 课题研究背景 2](#_Toc70451622)

[1.2 现有问题 2](#_Toc70451623)

[1.3 项目创新 3](#_Toc70451624)

[1.4 国内外研究现状 3](#_Toc70451625)

[2 相关概念和技术介绍 4](#_Toc70451627)

[2.1 区块链技术 4](#_Toc70451628)

[2.1.1 概念介绍 4](#_Toc70451629)

[图1 区块链分层架构模型 5](#_Toc70451630)

[2.1.2 技术特点 5](#_Toc70451631)

[2.2 智能合约 6](#_Toc70451632)

[2.2.1 概念 6](#_Toc70451633)

[2.2.2 部署原理 6](#_Toc70451634)

[2.2.3 运行原理 6](#_Toc70451635)

[2.3 网约车安全 7](#_Toc70451636)

[2.3.1 相关研究 7](#_Toc70451637)

[2.3.2 管理体制优化 7](#_Toc70451638)

[2.3.3 信用平台建设 7](#_Toc70451639)

[3 系统方案设计 7](#_Toc70451640)

[3.1 开发工具环境 7](#_Toc70451641)

[3.1.1 以太坊测试网Ropsten 7](#_Toc70451642)

[3.1.2 Remix-ide 7](#_Toc70451643)

[3.1.3 Metamask 7](#_Toc70451644)

[3.1.4 Solidity 7](#_Toc70451645)

[3.1.5 ReactNative 7](#_Toc70451646)

[3.1.6 高德地图API 7](#_Toc70451647)

[3.1.7 Web3Js 7](#_Toc70451648)

[3.2 移动端APP 7](#_Toc70451649)

[3.2.1 位置信息模块 7](#_Toc70451650)

[3.2.2 地图展示模块 7](#_Toc70451651)

[3.2.3 路径规划模块 7](#_Toc70451652)

[3.2.4 交易打包和事件监听模块 7](#_Toc70451653)

[3.3 区块链和智能合约模块 7](#_Toc70451654)

[3.3.1 坐标行程记录 7](#_Toc70451655)

[3.3.2 紧急联系人设置 7](#_Toc70451656)

[3.3.3 路径脱离判断 7](#_Toc70451657)

[3.3.4 发送脱离路径事件 7](#_Toc70451658)

[4 系统实现与测试 8](#_Toc70451659)

[4.1 系统实现 8](#_Toc70451660)

[4.2 系统测试 8](#_Toc70451661)

[4.2.1 测试环境配置 8](#_Toc70451662)

[4.2.2 测试方案 8](#_Toc70451663)

[4.2.3 操作流程 8](#_Toc70451664)

[4.2.4 功能测试 8](#_Toc70451665)

[5 结语 8](#_Toc70451666)

[6 参考文献 8](#_Toc70451667)

[7 致谢 8](#_Toc70451668)

基于区块链的网约车路径预警系统的设计与实现

* 1. 前 言
     1. 课题研究背景

近年来，城市化推进、基础交通设施的完善有利于孕育大量的出行需求；互联网技术的飞速发展也为出行行业的发展奠定基础。传统出行模式下，用户原地等待，司机沿途接客的出行方案，已经难以适应市场需求的发展。

在此背景下，网约车服务应运而生，并飞速发展，短短数年内已经完成了对传统出租车模式的反超。根据中国互联网络信息中心(CNNIC)的统计， 截至2020年6月，我国网约车用户规模为3.40亿。受疫情影响，较2019年中减少6415万。而在疫情前，网约车用户规模呈持续上升趋势，2019年6月网约车用户规模则一度达到4.04亿人，较2018年中增长约1600万人。其捷高效的服务模式已经在很大程度上改变了人们的出行习惯。

现代网约车平台同时集合了用户叫车，分配派单，行程结算，订单管理，支付管理，信用管理，综合运营等多种功能于一体。一站式为司机和用户解决营业和出行问题。较传统打车模式，有效匹配了司机和用户的需求，减少了司机空载率和乘客的等待时间，最大化的节省了双方的时间和沟通成本。成为了人们打车出行的首选模式。

* + 1. 现有问题

然而近年来多次发生的网约车抢劫杀人案、侵犯案、失踪案，动机卑劣，性质恶劣社会危害极大，引起了广泛的重视，将网约车推向了舆论的风口浪尖，对网约车业务发展造成了严重的打击。在此背景下保障网约车安全，完善相关法律，建设合理的监管体系的呼声越发响亮。

刑事案件外，平台管理方面也频频传出负面消息。2019年失信司机、报废车辆通过后门重新营业，却拒绝接受有合法营运资质的网约车公司接入事件。运营部门操作后台直接修改司机信用评分等被曝光出的事件，也在一次又一次地加剧网约车平台与用户之间的信任危机。如何平台数据的真实性，如何确保用户的知情权，如何建立良好的信任体系，也已成为了亟待网约车平台解决的问题。

* + 1. 项目创新

本文将立体式的运用区块链技术的优势特性，针对应用场景设计对应模式，以满足网约车模式中存在的安全需求。

区块链公链的特性完美符合网约车行程中对于订单坐标记录的需求。其具有任何人都可参与发送交易、确认交易、参与共识过程的架构；具有公开透明，去中心化，去信任成本的优势。采用公有链记录社会公示所需的重要信息，如司机信息，车辆情况，行程坐标等记录，在密码学上保证了其无法篡改，能够很好实现无需第三方机构信用背书的社会监督，同时做到减少成本及提高公信力。

同时创新性的辅以智能合约进行行程路径是否脱离的判断，较传统后台，智能合约部署在区块链中，拥有内容公开透明，不可篡改，一旦部署永久运行的特性。脱离了人为影响的判断机制，杜绝了平台暗箱操作的可能，保证了记录的真实性和判断的客观性，运用该种技术能够使网约车平台的具有相当的社会公信力。同时智能合约的内容由区块链执行，较传统后台，能够节省大量的服务端资源。

结合Web3监听智能合约中触发的路径脱离事件，第一时间对可能存在的威胁做出反应，自动触发应急机制。将区块链与APP立体结合，在模式设计的层面上，提供了一种有效的乘客安全保障方案。

* + 1. 国内外研究现状
       1. 网约车安全

对于网约车安全的探索也在一直进行中，现有的研究主要给出了两个方向的解决方案。

一是完善相关法律，通过国家立法，规范化网约车的经营管理流程。夯实平台责任提升合规率；同时完善监管平台，实现与网约车平台信息共享，进一步提高监管能力和水平，通过国家监管对平台进行督促和补充。

二是加速信用平台建设，根据《重庆市网络预约出租汽车经营服务管理暂行办法》第四十条规定：各有关部门应当按照职责建立网约车平台公司和驾驶员信用记录，并纳入全国信用信息共享平台。同时将网约车平台公司行政许可和行政处罚等信用信息在全国企业信用信息公示系统上予以公示。通过与信用挂钩，降低问题人士进入网约车行业的概率，同时大幅提高违规成本，以达到保障用户安全的目的。

而本文设计的基于区块链的网约车路径预警系统，将在技术层面为满足网约车模式中存在的安全需求提供新的思路。

* + - 1. 区块链技术

国外对区块链的探索大多来自于实务界的不断探索，强调数据编程应以法律为基础，这有利于区块链的智能合约与实际生活相结合，提供更好的服务。国外的许多企业开始认识到，区块链技术的兴起对网约车行业可能造成巨大冲击，开始研究区块链在网约车领域的应用，纷纷发布了区块链战略书。

2019年网约车领域的领头企业Uber，寄希望于使用区块链技术解决目前网约车行业缺乏安全标准，缺乏透明度，平台维护费用高昂的问题。通过Uber区块链提高司机与客户的联系效率，并使用区块链进行身份管理，同时解决目前存在的效率问题与信用问题。

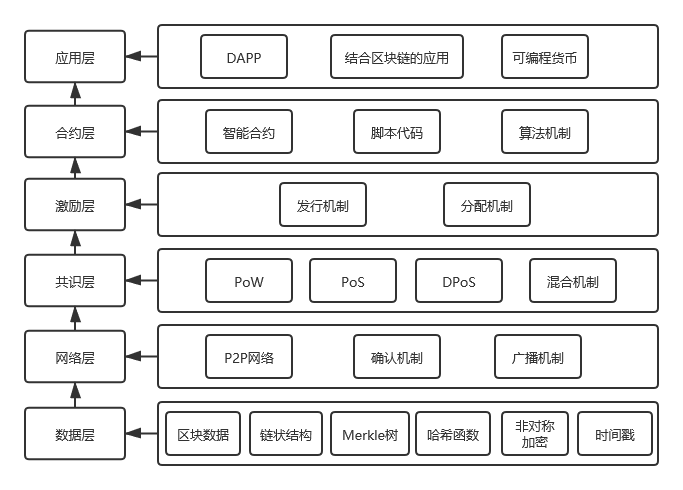
早在 2016年区块链就获得国内各行各业的关注，在网约车领域对于区块链技术应用也在不断进行探索。快的打车创始人陈伟星于2018年致力于打造以VV Share为核心的共享经济体，以区块链网约车应用VV Go打开相关市场，公布了详细的白皮书和模式设计。希望能形成囊括衣食住行的区块链生态。

杭州趣链科技有限公司在2017年申请了一项《一种基于区块链技术的智能网约车系统及网约方法》专利，该专利试图通过以一种基于区块链技术的智能网约车系统及网约方法，来打破目前中心化服务网约车平台的垄断。其中支付模块，评价模块，行程记录模块的设计与区块链密切结合，费用的计算逻辑，评价逻辑将通过智能合约实现直接部署在区块链上。

但遗憾的是，目前还没有完整的区块链网约车项目落地。

1. 1. 相关概念和技术介绍
      1. 区块链技术
         1. 概念介绍

区块链技术最早在2008年由中本聪团队以“区块”和“链”的概念提出，其本质是一个由节点共同维护的分布式账本。区块链技术为在一个分布式环境下保证数据透明度和可靠性提供了解决方案。

目前达成共识区块链的基础模型，自下而上分为六层，分别是数据层、网络层、共识层、激励层、合约层和应用层。数据层主要封装数据区块和哈希函数、时间戳等技术，保证区块链的基本结构，网络层主要包含分布式网络体系、数据广播机制和验证机制，共识层则是分布式网络中维持对数据的共识的各类机制，激励层主要包含经济激励的发行和分配机制，合约层主要包括智能合约、脚本代码和算法，应用层则是区块链技术的各类应用场景。

1. 区块链分层架构模型

区块链的数据结构是一种链式结构，由记录节点生成的符合规则的区块以类似链表的形式组成。区块由区块头和区块体组成，区块体包含交易信息和附加信息；区块头的生成规则较为复杂，对整个区块链系统的可靠性起着决定性作用。其必须通过上一个区块的hash值，再由哈希函数和区块链所使用的共识机制附加码构成。通过这样的链式生成规则，即可在密码学上保证其不可篡改，不可伪造的特点。

* + - 1. 技术特点

一、去中心化。区块链网络无需第三方管理机构或硬件设施进行管理和维护，所有节点都享有同等的权利，各个节点实现了信息自我验证、传递和管理。去中心化的特点使得人为因素对平台的影响被消除。同时平台的维护成本也因所有节点得以共同参与验证和维护工作，而得到了降低。

二、保障记录真实不可篡改。区块链技术通过加密算法、共识机制、时间戳等，保证每个区块的唯一性与可回溯性。每个区块都保留了上一区块的哈希值，并且每块的区块数据内容又与其哈希值唯一对应，这种遗传性使得诚实链上的区块相互关联，确保信息不可篡改。

三、公开透明。区块链使用去中心化的分布式账本，通过网络层中的信息广播机制，当交易发生时，将交易信息加密后向所有节点广播，所有节点均对交易进行记录，获取链上完整的交易信息。同时，后加入的节点也可通过区块链网络同步所有已存在的区块。该机制保障了区块链的公开透明性。

* + 1. 智能合约
       1. 概念

智能合约的定义是：一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。本文的中智能合约主要指以太坊中的智能合约。

以太坊中智能合约是一段依托于区块链网络运行的代码和数据的集合，即区块链分层架构模型中合约层负责处理的部分。以太坊的智能合约与早期区块链脚本的主要区别是其具有图灵完备，可以让我们像使用任何高级语言一样来编写几乎可以做任何事情的程序。提前制定规则并部署到网络后，即可在对应条件发生时自动执行所制定的规则。

* + - 1. 部署原理

部署智能合约到以太坊上时，以太坊客户端首先会调用SOLC智能合约编译器将合约编译成EVM字节码，之后通过RPC接口将字节码文件发送到以太坊网络进行广播，超过一半以上节点验证通过之后，编译后的字节码会被写入到区块链账本中，之后会通过一笔交易在区块链网络中创建出一个智能合约。该笔交易包含几个特殊信息，分别是创建者地址、智能合约内容、智能合约的部署地址。智能合约部署地址是由创建者地址和发送的交易数作为输入，通过Kecca-256加密算法重新计算生成的地址。

* + - 1. 运行原理

由于不存在中心节点，所以智能合约调用时，并不是由区块链直接执行。而是由试图记账的以太坊节点从区块链中取出合约代码，然后由本地的以太坊虚拟机（EVM）进行执行，将返回结果写入本次调用产生的区块中，完成整个调用的过程。之后进行广播，由整个网络的节点对运算结果相互认证，以保证智能合约执行的正确性。

* 1. 系统方案设计
     1. 开发工具环境
        1. 以太坊测试网Ropsten

本文主要在以太坊上进行区块链模块的开发。开发阶段将会使用以太坊测试网络Ropsten代替主网络(Mainnet)进行的交易和部署。

以太坊测试网（testnet）用于模拟以太网主网的行为。拥有几乎和以太坊等效的功能。在Ropsten测试网络中，用户可以在拥有小于四个eth时申请免费eth用于模拟交易和支付交易费用(gas)。因此可以在testnets上开发和测试自己的智能合约，测试发币等等，作为上链前的评估环境。当主网络进行任何重大改变时，其测试主要在这些测试网络上完成。测试网络上的代币只能在测试环境中使用。

* + - 1. Solidity

Solidity是以太坊官方推荐语言，也是目前最流行、版本最稳定的智能合约语言。Solidity运行在Ethereum虚拟机（EVM）之上，是一个图灵完备的成熟语言。用这种语言可以创建合约来编码任意状态转换功能，可以用简单的几行代码来实现系统逻辑。

* + - 1. Remix-ide

Remix-ide是一款在线ide，主要用于solidity和yul语言的在线编译，调试和部署。支持目前发布的所有solidity版本，同时提供虚拟机环境，web3注入环境和第三方web3Provider环境的多种部署功能。支持如单步调试在内的丰富插件。已经成为solidity在线开发的首选。

* + - 1. Metamask
      2. ReactNative
      3. 高德地图API
      4. Web3Js

Web3JS是一个轻量级的JavaScript库，用于连接以太坊网络的客户端。当Solidity合约编译好并且发送到网络上之后，可以使用以太坊的Web3API来调用它，使平台节点能与区块链网络节点进行交互，底层实现上，它通过RPC 调用与本地节点通信。Web3JS可以与任何暴露了RPC接口的以太坊节点连接。

web3中有eth对象 - web3.eth 具体来表示与以太坊区块链之间的交互。shh对象 - web3.shh表示Whisper协议的相关交互。

* + 1. 移动端APP
       1. 位置信息模块
       2. 地图展示模块
       3. 路径规划模块
       4. 交易打包和事件监听模块
    2. 区块链和智能合约模块
       1. 坐标行程记录
       2. 紧急联系人设置
       3. 路径脱离判断
       4. 发送脱离路径事件
  1. 系统实现与测试
     1. 系统实现
     2. 系统测试
        1. 测试环境配置
        2. 测试方案
        3. 操作流程
        4. 功能测试
  2. 结语
  3. 参考文献
  4. 致谢