

# 基于区块链的网约车安全风险规避模式

李青鹏,赵相福,陈中育,郑龙忠

(浙江师范大学 计算机系,浙江 金华 321004)

**摘要:**当前网约车系统对于风险的规避和应对还不是特别完善。网约车安全事件时有发生,安全事故给社会带来诸多不良影响,引起社会各界普遍关注。现有的网约车风险规避模式重在规避,而缺乏有效应对风险的方法,成为阻碍网约车发展的一大痛点。通过分析现有网约车风险规避模式的核心痛点和区块链技术去中心化、安全可信等特点,对比比特币节点间地址通信模式,设计出网约车节点间坐标通信模式,通过视图节点筛选找到附近司机,从而构架出新的网约车风险规避模式。通过对比两种风险规避模式的不同,分析出新风险规避模式的优点。最后,设定五种新风险规避模式的场景进行论证,证明新模式可以保证报警的有效性,风险解决的及时性,大大提高了乘客和司机的安全性。使网约车司机成为一个整体,互相监督互相保护。

**关键词:**区块链;网约车;风险规避;安全

**中图分类号:**TP311

**文献标识码:**A

**文章编号:**1673-629X(2019)09-0152-06

**doi:**10.3969/j.issn.1673-629X.2019.09.029

## Risk Avoidance for Safe Network Car System Based on Blockchain

LI Qing-peng, ZHAO Xiang-fu, CHEN Zhong-yu, ZHENG Long-zhong

(Department of Computer, Zhejiang Normal University, Jinhua 321004, China)

**Abstract:** The existing network car system is not particularly perfect for risk avoidance and response. There have been security incidents involving network vehicles, which have brought many adverse effects to the society and caused widespread concern in the community. The existing network risk aversion model focuses on avoidance, and the lack of effective methods to deal with risks has become a major pain point hindering the development of network vehicles. Through analysis of the core pain points of the existing network risk aversion model, and the decentralization of blockchain technology, security and credibility, comparing the address communication mode between Bitcoin nodes, we design a coordinate communication mode between the nodes of the network. The nearby drivers are searched through the view node to construct a new network car risk avoidance mode. By comparing the differences between the two risk aversion models, the advantages of the new risk aversion model are analyzed. Finally, the scenario of five new risk aversion models is set up to demonstrate that the new model can ensure the effectiveness of the alarm and the timeliness of risk resolution, which greatly improves the safety of passengers and drivers. Make the network car drivers become a whole, mutual supervision and mutual protection.

**Key words:** blockchain; network car; risk avoidance; safety

## 0 引言

随着科技的进步 5G 时代的到来,通信将变得越来越便捷<sup>[1]</sup>。作为新兴技术的区块链与物联网技术可以融合彼此的优点,更好地服务于人们的生活<sup>[2]</sup>。物联网安全研究还处于起步阶段,大部分研究成果还不能解决物联网发展中的安全问题<sup>[3]</sup>。区块链由于其去中心、去信任等优点,在信息安全等领域得到了很好的应用<sup>[4]</sup>。区块链共识的达成需要所有节点的参与,每

个节点都是对等的。如权益证明机制(PoS)<sup>[5]</sup>、股份权益证明机制(DPoS)<sup>[6]</sup>等,在一定程度上保证了每个节点在共识问题的正确性和一致性上有相同的参与权和投票权。随着社会的发展,城市交通压力越来越大,网约车作为“互联网+”的新型智能城市交通的产物,很好地利用了城市中过剩的交通资源,在一定程度上减缓了城市的拥堵,使得城市中交通资源得到更加合理的分配,在方便人们出行的同时,也缓解了城市的交

收稿日期:2018-10-27

修回日期:2019-02-28

网络出版时间:2019-04-24

基金项目:浙江省自然科学基金(LY16F020004)

作者简介:李青鹏(1992-),男,硕士生,研究方向为区块链共识算法;赵相福,博士,副教授,研究方向为基于模型的故障诊断、人工智能、区块链等;陈中育,博士,教授,通讯作者,研究方向为规范化软件开发技术;郑龙忠,博士,教授,研究方向为模式分类、机器学习。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20190424.1051.046.html>

通压力<sup>[7]</sup>。同时也促进了社会就业,对经济发展也有一定的贡献。从经济学角度看,网约车是共享经济的一种表现形式<sup>[8]</sup>。但由于网约车行业安全问题发生的随机性、安全事件的复杂多样性和监管的不规范性,使得原本适用于传统的出租车巡游安全监管方式,不能很好地适用于网约车的安全监管。据统计,国内网约车车主数量达到了600万人次,而且还在不断增加<sup>[9]</sup>。由于网约车行业入门简单,众多的网约车的出现,产生了许多新的安全问题。如网约车通过网络实现信息交互威胁到乘客的信息安全,网约车空间的封闭性,滋生出一些违法犯罪威胁到乘客和司机的人身安全。随着网约车的发展,乘客和司机的安全问题越发突出,适用于网约车服务安全风险的规避策略成为一个研究热点。通过分析现有网约车维护安全的方法和相关策略发现,现有的办法主要集中在对潜在的危险进行回避提高行业的准入门槛,但并没有一种有效地应对危险事件,解决事故的有效方法。

文中结合区块链的分布式去中心化思想,提出一种新的网约车安全模式设想,并对该模式进行完善,使其具有可行性。该模式旨在利用区块链的相关技术,使网约车变得更加安全。

1 现有的核心问题应用痛点

1.1 网约车的不安全性

在网络信息的大众化时代,网约车作为互联网+时代的新产物,要更好地服务于大众的生活,还有很多要完善的地方。的确网约车让大家的生活变得更加便捷,但当网约车安全事故产生时,往往会引发很大的社

会舆论,成为人们关注的焦点,这正说明网约车已经成为人们生活的一部分,谁也不想同样的事故发生在自己身上。网约车的安全问题,受到了普遍关注,人们对网约车往往是又爱又恨,既离不开,又对其潜在的安全问题十分担忧。

1.2 平台应对风险问题的无力性

如何让网约车变得更加安全和规范一直是许多网约车平台公司和国家相关部门的研究内容。2016年7月28日,交通运输部正式发布《网络预约出租汽车经营服务管理暂行办法》<sup>[10]</sup>。但是从现有的网约车规避途径来看,主要是提高网约车的准入门槛,多是侧重于对潜在的风险源进行回避。例如,潜在的风险司机,潜在的风险车辆的筛选剔除。这样做的确在一定程度上降低了危险事故的发生率,但危险事件没有杜绝。当平时表现正常的司机或者乘客犯罪时,并没有一种应对风险问题恶化,及时降低风险和解决风险问题的有效方案。现有的网约车一键报警机制具有不稳定性,并不能很好地保护乘客安全。由于网约车平台在应对风险事件方案的缺失,面对安全事故显得很无力。在安全事件发生时,只能寄希望于乘客自己报警成功和警察尽快到来。但是警察的到来往往存在一些不可抗性因素。例如,出警单位离事发地点太远,警察出警途中遇到堵车等不确定因素,还有网约车具有移动性,都会耽误救援的宝贵时间。

1.3 具体报警流程与安全漏洞分析

对现有相关网约车平台的风险规避和应对模式分析如图1所示。

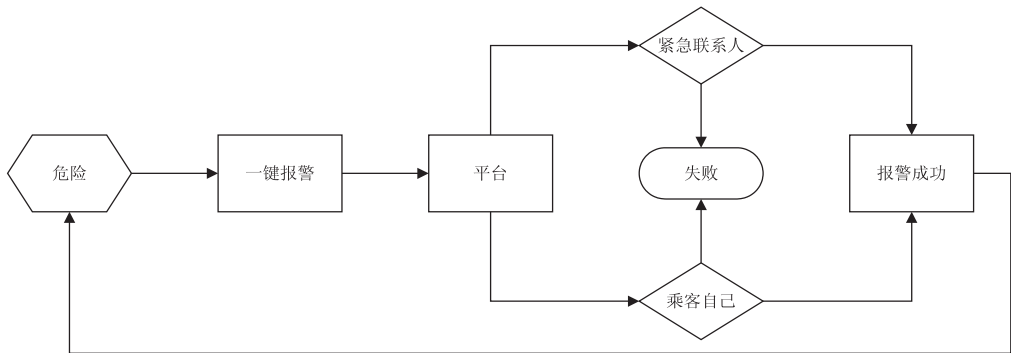


图1 现有网约车风险规避模式流程

在现有的网约车一键报警后,平台会将主要的报警信息进行打包,这些报警信息通过两个途径传递出去。第一种是传递给紧急联系人;第二种是通过平台提供的报警方式乘客自己通知警察。

通过图1可以看出,现有模式有如下不足:

- (1)紧急联系人可能没看到你的信息,错过报警,导致报警失败;
- (2)乘客在车上不方便报警,报警可能会激怒

- 司机;
- (3)存在紧急联系人和乘客都报警失败的可能;
- (4)警察出警地点距离事发地较远,或堵车等其他原因,到达报警地点时间较长;
- (5)危险车辆的移动性大,不好追踪。

可以看出,现有的网约车运行模式存在一些安全漏洞。其中紧急联系人在应对风险时也起到了非常重要的作用。紧急联系的选择一般是基于血亲的信任。

紧急联系人可以看成一种报警的有效选择,乘客可以平时在网约车平台上添加好自己的紧急联系人。在发生危险时,只要点击一键报警,自己报警的重要信息如地点路径、司机信息、车牌号等都会直接发送给紧急联系人。但紧急联系人这一要素存在一定的不稳定性,一旦错过信息将会导致报警失败。如果附近的人都能成为紧急联系人,在危险发生时那将起到更好,更稳定的作用。

因此,如何让这些在平台注册了的具有分布式节点特点的车辆,在安全问题出现时参与到事件中来,成为合理的紧急联系人,就是文中的主要研究点。

2 区块链技术特征

2008 年随着旨在避免金融危机的货币比特币的发行,其创立者中本聪的论文《比特币:一个 P2P 电子现金系统》<sup>[11]</sup>的发表,作为比特币的底层核心技术——区块链技术,就此诞生。区块链技术具有去中心化和点对点的特点,通过分布式节点间形成共识,从而实现数据的安全有效性<sup>[12]</sup>。

区块链技术的基础架构模型主要分为六个部分:网络层、共识层、激励层、数据层、合约层、应用层<sup>[13]</sup>。区块链是以加密机制、储存机制、共识机制等多种机制组成的分布式网络系统。可以在没有中心服务器的分布式节点系统间,进行可信的数据传递和交易。区块链具有去中心和可信化的特点,因而成为人们研究的热点。

共识算法保证节点间对收集到的数据和交易集合的共同确认,P2P 网络保证在一定时间内各节点的数据得到有效且一致的更新。共识算法和 P2P 网络共同组成区块链的共识机制如图 2 所示。

区块链网络中的分布式节点,通过点对点的模式进行连接,并且进行地址传播、数据通信和节点信息检测等来维持系统数据的正确性和一致性。

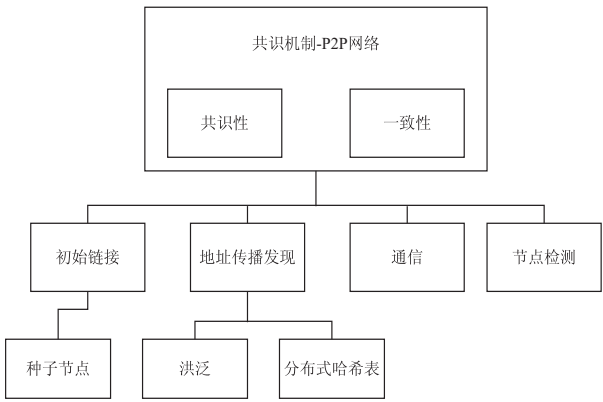


图 2 区块链的共识机制

2.1 数据的交互方式与发送传播机制

区块链系统中的节点具有高度分布式、自治性、进出自由的特点。主要采用 P2P 对等式网络来进行数据的接收和验证<sup>[14]</sup>。

P2P 网络有四种形式:中心化 P2P 网络、全分布式非结构化 P2P 网络、全分布式结构化 P2P 网络、半分布网络。

在中心化 P2P 网络中,当节点需要查找信息时,向中心服务器发送请求,中心服务器根据请求,反馈一个满足请求结果的目标节点地址,这样节点可以通过目标节点地址实现点对点的信息交换。这样的中心服务器有别于银行这类中心化机构,自己是不存储信息的。

P2P 网络中每个节点都是平等的,以扁平式拓扑结构联通和交互,保证了高度的去中心化。每个节点可以看作一个中心,有权参与每次共识区块的产生<sup>[15]</sup>。

区块链有新数据区块的产生有一系列的数据传播和节点间数据交互的协议,主要通过全网广播的方式达成,每个节点有新的数据都进行广播,同时每个节点也都可以接收广播内容并进行检测。

区块链技术的一种应用,比特币中各节点信息的更新如图 3 所示,两种方式分别为主动广播发送自己

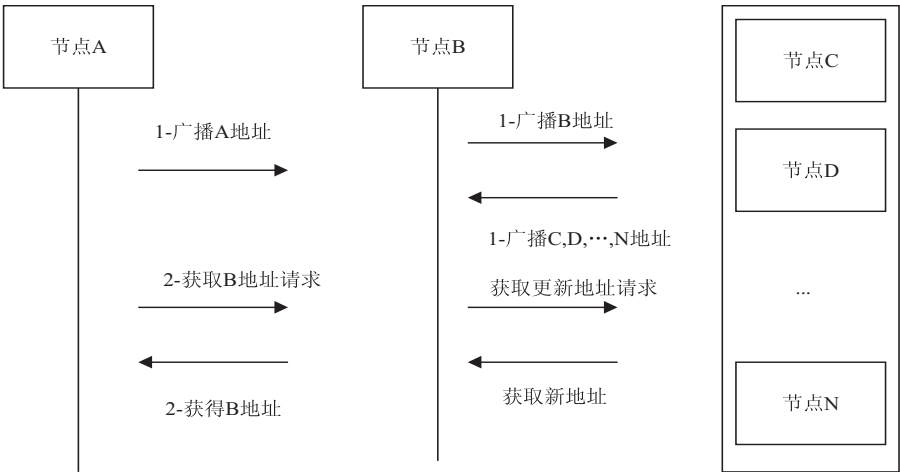


图 3 区块链应用比特币节点间通信模式

的地址和主动广播获取别人的地址。

比特币节点通信模式下广播和接收的都是节点的网络地址,该地址是比特币系统分配的一组代码,每个账户都不一样,可以看作节点的IP号。这样就将分布式节点联系起来,每个节点都可以知道其他节点的存在,也可以进行必要的通信。这样也使得节点可以自由进出,如果节点离开,将不再广播自己的地址。

### 2.2 节点的参与

中本聪在比特币的奠基性论文中设计了POW共识机制<sup>[11]</sup>,完美调动了各节点的积极性,让各节点充分发挥自己的计算能力,来解决系统设置的数学问题。其核心思想是让分布式节点通过算力竞争来保证共识数据的一致性和安全性。

在比特币系统中,各个分布式节点(矿工)通过各自本地的计算机的算力进行竞争,来解决一个求解复杂而验证简单的数学难题(即挖矿),最先解决的矿工将获得新区块的记账权利,同时获得系统奖励的比特币。

可以看出,区块链通信组网的方式以及奖励机制,对充分调动平台上各个分布式节点的积极性具有重要的意义,对分布式节点组成的系统也具有很强的启发意义。

## 3 区块链技术特征恰好可以解决网约车平台的现有问题

现有的网约车与区块链应用场景比特币有很多类似之处,区块链技术的相关优势特点完全可以应用到网约车平台,来解决网约车相关问题,弥补网约车的不足。详细分析如下:

(1)比特币是一个开放的平台,各个分布式节点(矿工)在这个平台注册。网约车同样是一个开放的平台,众多分布式的司机在其上注册。都具有高度的分布式特征。

(2)自治性。比特币平台上的节点,都拥有自己的计算机,独立解决系统的问题。网约车平台的司机同样拥有自己的汽车,独立进行接单服务。

(3)进出自由。比特币平台上的节点,自己决定是否参加到算力竞争中来,随时可以进入或退出。网约车平台的司机,同样可自由决定是否进入平台接单工作。

对现有的网约车报警流程的分析,不难发现,当前的报警模式比较粗糙,具有很大的安全漏洞,难以很好地保证乘客安全。根据比特币网络和网约车平台的相似性,恰好可以充分利用区块链技术的特征,为解决网约车平台的安全问题提供重要模式参考。

### 3.1 利用好平台数据的交互方式

区块链系统中的组网方式可以很好地对应到网约车平台,应用P2P网络让每个司机成为一个分布式节点,参与到解决安全事件中来。由于网约车司机都在一个平台,完全可以发挥定位和计算距离选择最近节点网约车的优势。

### 3.2 调动附近分布式网约车的积极性

POW共识机制中,通过一定数目的奖励来调动全网所有节点的积极性,参与到挖矿中来,从而获得奖励。在网约车平台同样可以设置这种奖励,但不是全网所有的网约车都参与进来,而是报警车辆附近的网约车司机,因为如果距离太远,不具备第一时间到达现场解决问题的条件。

第一,通过改进现有的组网方式,确保分布式的网约车司机知道其附近有危险问题网约车,而其可能是解决问题的最佳人选;

第二,通过设立一定的奖励机制,确保这些分布式节点司机自愿接单参与到事件的解决中来。

## 4 结合区块链技术的网约车安全风险规避模式

### 4.1 视图

可操作性拜占庭容错算法中提出了视图这一概念,当有客户提出共识问题请求时,所有要参与进来的分布式节点,将会被编号,看作一个视图整体。同视图下的分布式节点参与到共识问题中来,往往是对相关问题进行投票,并达成共识。当一定时间内视图中没达成共识,视图将会变化,重新召集新的分布式节点,并且重新编号,再重复上一轮计算并投票,一直到有新的共识达成<sup>[16]</sup>。

网约车平台都具有良好的定位系统,当人们需要打车时,可以看到自己附近有多少待客司机。因此,引入视图的概念,即将附近网约车看作当前视图中的节点。现有的网约车平台,都依托于GPS定位系统<sup>[17]</sup>。每辆网约车都有自己的经纬度坐标( $x,y$ ),通过运用比特币节点间地址通信的模式,设计出图4中的网约车间坐标通信模式。

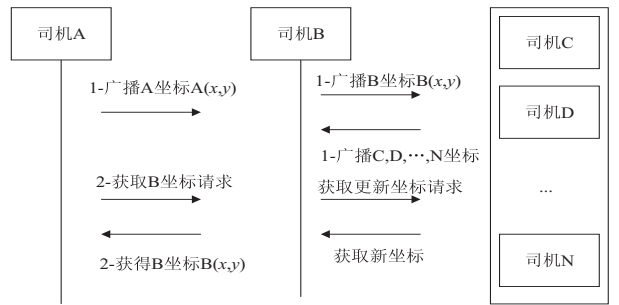


图4 网约车间坐标通信模式



在图 4 中,所有的网约车地址都进行广播,每个网约车节点,也可以搜索到所有的网约车实时地址信息。

当有乘客报警时,其附近一定范围就是一个视图,在该范围内的所有网约车司机都是该视图内的分布式节点。如图 5 所示,当节点  $O$  点击一键报警后,通过图 4 网约车间坐标通信模式可以获得平台上所有正在待客的网约车的地址。如何在众多的地址中刚好找到附近网约车节点的地址,就需要进一步筛选。

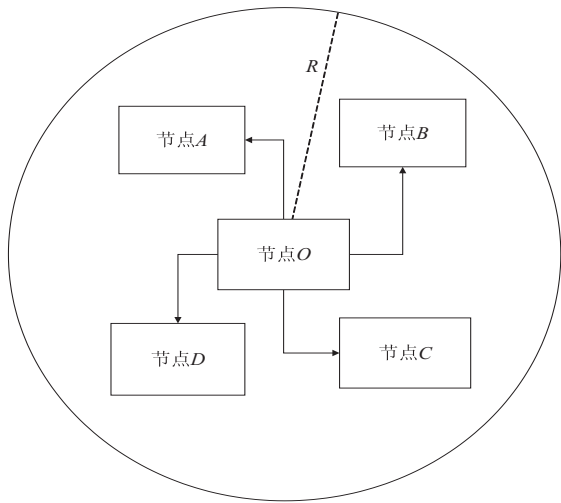


图 5 视 图

设报警节点坐标为  $O(x_1, y_1)$ , 被筛选节点坐标

为  $A(x_2, y_2)$ , 则 可 通 过 距 离 公 式  $|OA| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \leq R$  进行筛选,得到附近节点的集合  $P$ , 再在  $P$  集合中选出几个最小距离的节点,作为目标节点。

视图还具有可变化性,当一定范围内刚好没有节点存在,可以启动视图更换,也就是变换视图半径  $R$ , 确保一定会有节点存在。

共识机制: 当有乘客点击 APP 报警, 平台通过位置信息, 以及视图筛选锁定, 找到合适的视图并向其内的目标节点发送相关报警信息。通过这种模式, 让分布式节点间达到一种有节点出现危险, 需要解决的共识机制。

奖励机制: 适当奖励可以调动企业员工的积极性。如果设置一定的奖励, 该视图内的司机自己选择是否参与到问题的解决或者协调中来。通过紧急联系人到附近司机的转变, 也是一种信任的转变, 从血亲信任转变为货币信任, 起到的作用都是一样的, 但这种转变使得报警方式变得更加稳定, 同时附近的司机还具有离危险节点近的特点, 这是紧急联系人不具备的。

4.2 总体流程

在引入区块链的组网和奖励机制后, 设计新的风险规避和应对方案流程, 如图 6 所示。

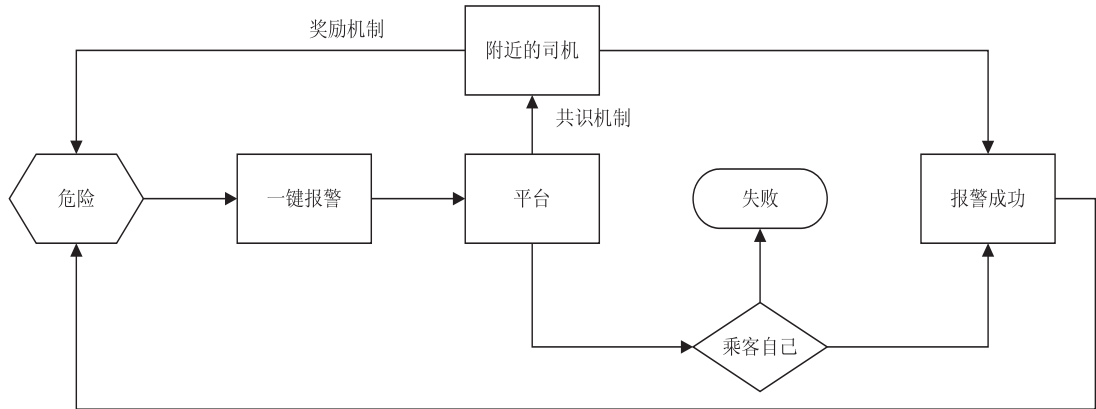


图 6 新构架的风险规避模式流程

这种模式下, 有两个途径可以解决风险。第一种途径还是警察处理, 第二种途径是附近的司机直接到达危险事件发生的地方进行适当处理, 同时不存在报警失败的情况。

这样可以节约时间, 降低风险, 甚至解决风险, 防止问题的进一步恶化。报警信息都会被附近司机收到, 不存在紧急联系人错过报警信息而导致报警失败的情况。

5 对比分析

通过对比现有模式下的风险规避途径流程和引入区块链相关概念的架构的风险规避途径模式流程可以

看出, 这种新模式具有以下特点:

- (1) 报警信息一定会被收到;
- (2) 解决了乘客在车上不方便报警的劣势;
- (3) 解决了危险车辆的高速移动性和不好追踪的问题;
- (4) 增加了一种解决危险的途径, 司机可以适当降低危险, 防止时间恶化;
- (5) 有很大概率在警察没到之前控制局面或解决问题;
- (6) 让分布的网约车司机, 变成一个自治的集体, 共同监督, 共同帮助;
- (7) 平台对乘客的安全保护更加有力。

6 场景分析与验证

构想实际当中的网约车场景,司机犯罪主要分为三个阶段:(1)有犯罪意图;(2)与乘客发生口角;(3)与乘客产生肢体冲突。基于这三个阶段,新模式下网约车风险事件可以分为以下几种情况。

第一种情况:司机有犯罪意图,但迫于乘客可以随时一键报警,通知附近司机,自己处于被监视的环境,而放弃犯罪。

第二种情况:司机有犯罪意图,并与乘客发生口角,乘客一键报警。司机发现乘客报警而放弃犯罪。

第三种情况:发生口角且乘客一键报警后,司机没有停止犯罪,附近司机赶到,司机停车,乘客脱离危险。

第四种情况:发生口角且乘客一键报警后,司机没有停止犯罪,附近司机赶到,司机没有停车,但开车中的危险司机不具备进一步犯罪的条件。开车中的司机没有多余的手脚攻击乘客。

第五种情况:理论情况下,司机停车,与乘客产生肢体冲突,乘客也有一定的自保能力,在乘客自我保护的这段时间,附近的司机完全可以赶到,使乘客脱离危险。

通过分析以上 5 种情况可以看出,在新模式下,乘客的安全性得到很大的提高,同时网约车司机成为了一个互相监督、互相保护的整体。

7 结束语

文中主要通过引入区块链应用比特币节点间地址更新的模式,设计出符合网约车节点间的坐标更新及通信模式,从而重新架构了一种更有力的网约车风险规避模式。充分调动网约车平台司机的积极性,使得他们互相监督和维护好平台的安全性。在风险事件发生时,网约车平台可以更有力地保护好乘客和司机的安全。当然现有的网约车风险规避途径还在完善当中,还需要更多更有效的规避模式补充。如节点间坐标等信息传递可以进一步进行加密,或者只在平台上用虚拟号进行信息的交互,从而更好地保护司机和乘客的隐私。随着 5G 的到来,通信变得更加便捷,相信网约车平台的安全模式将会得到极大的完善。

参考文献:

[1] 李章明. 5G 移动通信技术及发展趋势的分析与探讨[J]. 广东通信技术, 2015, 35(4): 44-46.

[2] 吴明娟, 陈书义, 邢涛, 等. 物联网与区块链融合技术研究综述[J]. 物联网技术, 2018, 8(8): 88-91.

[3] 张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017, 54(10): 2130-2143.

[4] 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7): 2092-2115.

[5] LARIMER D. Transactions as proof-of-stake[EB/OL]. [2018-10-10]. <http://7fvhfe.com1.z0.glb.clouddn.com/wp-content/uploads/2014/01/TransactionsAsProofOf-Stake10.pdf>.

[6] LARIMER D. Delegated proof-of-stake white paper[EB/OL]. [2018-10-10]. <http://docs.bitshares.org/bitshares/dpos.html>.

[7] 孙兴军. 网络约租车的风险及其规避[J]. 安徽行政学院学报, 2016, 7(4): 106-112.

[8] 李渊. 网约车安全风险分析及规避[J]. 湖北科技学院学报, 2016, 36(8): 10-14.

[9] 王静. 中国网约车的监管困境及解决[J]. 行政法学研究, 2016(2): 49-59.

[10] 李雅男. 网约车平台法律地位再定位与责任承担[J]. 河北法学, 2018, 36(7): 112-126.

[11] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2018-10-10]. <https://bitcoin.org/bitcoin.pdf>.

[12] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[13] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.

[14] 王安平, 范金刚, 郭艳来. 区块链在能源互联网中的应用[J]. 电力信息与通信技术, 2016, 14(9): 1-6.

[15] 张宁, 王毅, 康重庆, 等. 能源互联网中的区块链技术: 研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15): 4011-4023.

[16] CASTRO M. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer System, 1999, 20(4): 398-461.

[17] 樊杰. 基于 GPS 和 GPRS 的车载紧急报警系统的设计与实现[D]. 成都: 成都理工大学, 2014.