基于区块链和车联网的汽车租赁联盟的研究与实现

任 鹏[1], 徐晶晶[1], 王 意[1], 马小峰[1]

[1](同济大学 电子信息与工程学院,上海 嘉定 201804)

通讯作者: 马小峰, E-mail: xiaofengma@tongji.edu.cn

摘要: 区块链技术具有保证数据安全可信和实现快速同步的特性.随着区块链技术的发展,区块链技术开始在传统行业中得到应用.近年来,汽车租赁行业不断出现新的变化,但是传统的汽车租赁行业中汽车租赁企业投入资产规模大,市场准入门槛高,交易信息流通不畅等痛点仍然存在.本文针对这些问题通过车联网技术和区块链技术的结合,在车辆租赁者、车辆租赁服务平台、租赁车辆提供者、车辆保险机构和车辆维护机构之间设计了一个可信的汽车租赁联盟.这种汽车租赁联盟可以降低交易成本和市场准入门槛,提高汽车共享租赁经营的灵活性,促进相关业务的个性化创新.

关键词: 区块链;车联网;共享汽车租赁

Research and Implementation of Car Rental Alliance Based on Blockchain and Automotive Network

Peng Ren[1], Jingjing Xu[1], Yi Wang[1], Xiaofeng Ma[1]

[1](School of electronics and Information Engineering, Tongji University, Shanghai 201804, China)

Abstract: Blockchain technology has the characteristics of making data safe, reliable and keeping data synchronization. With the development of blockchain technology, blockchain technology has been used in a variety of traditional industries. In recent years, the automobile rental industry has been constantly undergoing new changes, but there still have some pain points, such as large-scale investment assets, high market access threshold, and poor flow of transaction information. Aiming at these problems, this paper designs a trustworthy car rental alliance among vehicle renters, vehicle rental service platform, rental vehicle providers, vehicle insurance institutions and vehicle maintenance institutions through the combination of automotive networking technology and blockchain technology. The car rental alliance can reduce transaction costs and market access threshold, improve the flexibility of car rental, and promote innovation of related business.

Key words: blockchain; automotive networking; sharing car rental

区块链技术诞生于比特币体系的设计中,2008 年最初提出的区块链技术仅仅是一种数据结构,用来存储比特币的交易历史,提供可信的交易验证[1].随着比特币交易网络的不断扩张,比特币体系以及背后的区块链技术受到越来越多的关注.比特币交易网络作为区块链技术在金融领域的首个应用[2],在经历了将近十年的稳定运行后,充分证明了背后起支持作用的区块链技术的可行性.随着区块链技术的不断演进,其具有的去中心化、稳定安全、不可篡改等特点[3,4,5], 使其脱离了加密数字货币范畴的束缚, 开始向供应链金融[6]、物联网[7]等领域不断扩展.

区块链技术的关键之一在于共识的达成.当前的区块链技术已经发展出了多种共识机制,其中比较有代表性的共识机制有 PoW, PBFT 和 Paxos 等,不同的区块链项目通常都采用这三种共识机制及其改进版本[8].根据区块链项目采用的共识机制的不同,可以将区块链项目分为公有链,联盟链和私有链三种类型.目前来看,单纯的私有链应用场景因为限于单一机构,应用范围较为局限,而以加密数字货币为代表应用场景的公有链和面向企业应用的联盟链的适配场景更为宽泛,本文提出的共享汽车租赁联盟采用的是基于联盟链的架构体系.

区块链技术的本质是通过技术方法保证数据的可信性,在没有强大中心机构提供信任机制的情况下,通过对技术方法的信任创造一种互信的交易环境,从而使交易变得可行.成熟的区块链系统设计的时候均考虑了对数据一致性的保证[9],并且对可能出现的各种恶意攻击行为进行预判,保证了系统具有一定的抗攻击性[10].本文提出的共享汽车租赁联盟的构建,在区块链服务系统设计中采用了当前较为成熟的 hyperleger fabric 架构,可以提供稳定可信的区块链系统服务.

随着物联网技术的不断发展,网络化和信息化不断渗透到生产生活的各个方面.车联网技术作为物联网技术的一种代表性应用,可以通过车载传感器、无线射频等技术,实现对车辆特性、运行状态等的实时追踪[11],并将数据通过信息网络平台上传到服务器进行进一步的分析处理.在以往的车联网技术研究中,通常希望能够利用车联网的数据进行车辆状态追踪[12],或者从交通管理的角度,通过对交通设施的使用情况进行分析,提供智能交通引导服务[13].本文提出的共享汽车租赁联盟,希望能够将车联网的数据和区块链系统结合起来,通过区块链系统赋予车联网数据可信性,进而建立一个可信的联盟.该联盟整合了车辆共享租赁商业场景中车辆所有者、车辆使用者、车辆租赁服务平台、车辆保险机构以及车辆维修服务机构等角色,通过区块链系统加快与车辆租赁相关的可信数据的流通,进而为参与各方提供个性化的服务,创造一种新型的汽车共享租赁服务模式.

1 区块链和车联网技术

1.1 区块链技术

区块链技术发展大致经历了三个阶段：依赖技术的理论储备阶段；以比特币交易体系为代表的数字货币试验阶段；支持复杂智能合约和分布式应用的扩展阶段.

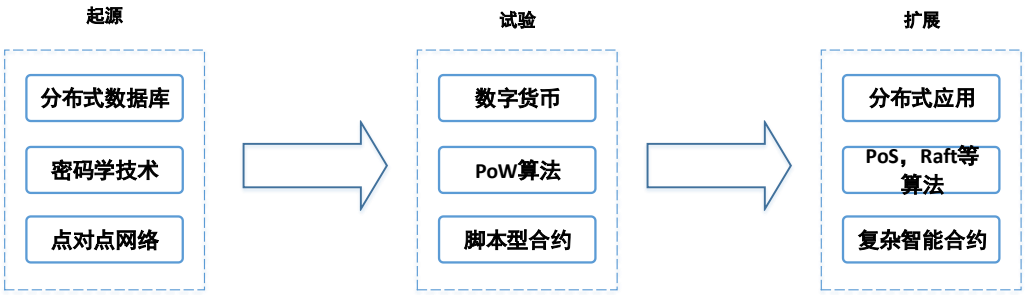

图 1 区块链技术演进

区块链技术的起源不同于传统的单点突破式创新,它采用了很多已经成熟的技术组件,通过巧妙的设计,构造了一个能够稳定运行的系统.其依赖的技术包括分布式数据库、非对称加密的密码学技术、点对点通信网络技术等.通过这些技术组合,可以打造一个没有中心化服务器的交易系统,系统中的每个参与者既是系统的使用者,也是系统服务的提供者.因为系统运行在明确的交易规则上,并且从技术层面上保证了交易的可靠性,所以参与的节点不需要依赖对其它节点的信任,而是依赖对整个系统的信任完成交易.

区块链技术第一次成功的试验当属比特币系统.在比特币系统的实践中,首次提出了 PoW 算法[1].PoW 算法设计了一个难以求解但易于验证的数学问题,理论上拥有更高算力的节点也有更大概率获得该问题的解.当某一个节点求得该数学问题的解并被其它节点验证之后,也就有拥有了为下一个区块创建提供服务的权利.节点通过完成对当前阶段交易内容创建区块的服务,可以获得一定的比特币奖励.PoW 算法是区块链技术中第一个真正具有实际意义的算法,具有很强的创新意义,但是其本身也有一些技术上的不足.不足之处主要有以下几点：

（1）PoW 算法本质上是通过消耗算力资源维持节点间的竞争状态,进而维持交易系统的运行.在算力竞争中有大量资源被浪费掉了,尤其是当前比特币交易网络规模不断扩大之后,这种高消耗资源的情况特别明显.

（2）随着比特币市值的不断攀升,专业的矿场组织大量先进的矿机作为节点参与竞争.这造成了目前比特币网络中的算力不断向

大型矿场中集合,最后造成了算力的中心化现象.

（3）PoW 算法数学问题的复杂度会随着网络算力的不断增强而增加,从而保证创建区块权利分配的时间稳定性.这种策略有助于系统的稳定性,但同时也限制了系统交易的确认速度.另外在竞争状态下,节点需要投入的算力资源也会不断扩大,没有尽头.

在 PoW 算法之后出现了 PoS 算法[14],通过引入权益证明一定程度上降低了计算的复杂度,解决了一些 PoW 算法中资源消耗过高的情况.以 PoW 算法和 PoS 算法为支撑的公有链架构类型的加密数字货币,经历长时间的运行试验,充分验证了区块链技术的可行性.在数字货币的发展阶段,因为交易逻辑相对比较简单明晰,所以区块链系统的设计中通常只支持简单的脚本型合约.

随着区块链技术的进一步发展,从加密数字货币的公有链架构中扩展出来了联盟链的架构体系.联盟链和公有链的最大不同在于,联盟链本身运行在一个具有一定信任基础的环境中,区块链体系的最大作用变成了交易数据的存证.因为很大程度排除了节点恶意构造虚假信息的攻击可能,在联盟链中的共识机制通常更为高效.典型的共识机制有 Paxos 算法[15,16]、Raft 算法[17]等,也有采用 Kafka[18]机制完成消息共识的策略.因为联盟链的设计面向企业应用,所以联盟链中的智能合约可以支持复杂的业务逻辑.随着区块链技术的进一步发展,一些新的密码学技术,例如零知识证明[19,20]、同态加密[21]等被不断尝试应用到区块链体系中,这也为更好的提高效率,保护用户隐私提供了可能.

1.2 车联网技术

物联网技术通常将用于数据采集的传感器和用于设备控制的控制器通过网络技术结合起来.在区块链技术诞生后,一直有学者研究将区块链技术与物联网技术进行结合[22,23].采用区块链技术能够降低物联网的成本,提升物联网设备的安全性[7].

车联网技术是物联网技术在交通领域的代表性应用之一,车联网可以通过车载传感器和无线网络通讯技术,对车辆的动态信息和静态属性进行提取,并进一步分析利用.随着传感器、云计算、移动网络通讯等技术的飞速发展,车联网技术已经可以完成车辆与车辆之间、车辆与道路基础设施之间、车辆与后台服务器之间的快速信息交换[24].

本文提出的基于区块链技术和车联网技术的共享汽车租赁模式,希望能够通过区块链技术保证车联网采集数据的可信性,进而通过可信的数据流通,在传统的汽车租赁场景下创造出更加灵活的商业模式.

2. 共享汽车租赁模式设计

2.1 汽车共享租赁联盟构建

随着我国汽车产业和旅游业的迅速发展,汽车租赁行业增长迅猛.但是相对于发达国家的汽车租赁行业,我国的汽车租赁行业发展无论是产业规模、技术管理、服务水平都存在着明显差距[25].当前我国的汽车租赁市场规模化效应较小,集约化程度较低,呈现比较分散的状态[26].

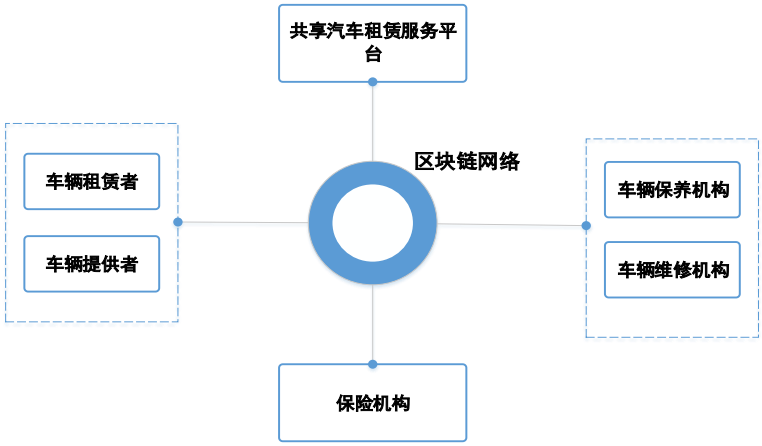

图 2 基于区块链的汽车共享租赁联盟构建

随着区块链技术和车联网技术发展,本文设计了基于这些新技术的汽车租赁联盟.如图 2 所示,通过区块链技术中的联盟链的架构,把汽车租赁产业相关的角色进行了抽象结合.租赁联盟中的角色包括:提供车辆保险的保险机构；提供租赁服务的租赁平台；提供车辆维护的维护机构；提供租赁车辆的车辆所有人和租赁车辆的车辆驾驶人.

车辆提供者提供的车辆在经过车辆维护机构的专业鉴定后,生成租赁车辆车况报告,包含车辆的品牌、行驶里程等基础信息.车况报告经由车辆租赁服务平台确认后写入区块链网络,租赁联盟中的成员均能获知车况信息.车辆租赁者的每一次租赁行为都会被区块链网络记录,记录的信息既包括租赁订单的时间、支付情况等信息,也包括由车联网系统采集的车辆在租赁期间的驾驶信息.共享汽车租赁服务平台根据车况报告和车辆租赁者的驾驶行为数据分析,可以对每次车辆租赁情况进行评估,提供个性化的订单服务.车辆保险机构根据车况报告、车辆租赁者的驾驶数据分析等可以提供个性化的保险服务.因为区块链网络数据的不可篡改性和可信性,联盟中

的各个角色可以放心的依赖网络中数据进行分析,从而显著提高商业模式中的信息流通速度,同时降低信息交换和信息监督审核的成本.因为能够在车辆提供者和车辆租赁者之间构建可信的关系,使拥有闲置车辆的车主方便进地进入租赁市场,从而可以充分发挥共享经济的精神,提高闲置车辆的利用率.这也在一定程度上改善了传统汽车租赁服务企业需要自有车辆,资产占用过重的情况.

2.2 车联网数据采集

传统的车联网系统可以通过车载传感器获取数据,然后通过无线通信网络将数据上传到服务器供管理者进一步分析[12].引入区块链系统之后,数据的存储和管理将由区块链系统负责.如图 3 所示,车载传感器对车辆的状态信息进行采集,然后通过车联网系统进行上传.数据上传之后的存储和管理由区块链系统中的智能合约负责,一旦数据写入区块链网络,则不能被更改,从而保证数据的可信性.

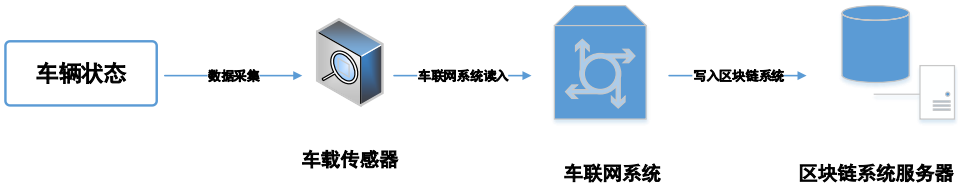

图 3 车联网数据采集写入区块链系统

因为数据的存储和管理由智能合约负责,所以智能合约的内容需要通过联盟中相关角色的审核.目前通过智能合约写入区块链系统的数据主要分为两类,一类是租赁平台提供的订单信息,一类是该订单期间车联网上传的驾驶数据,用于分析车辆租赁者的驾驶行为.

表 1 智能合约管理的主要数据

订单信息	驾驶数据
车主信息	GPS 轨迹
用户信息	速度信息（平均速度,最大速度）
车况信息	疲劳驾驶（疲劳驾驶次数,疲劳驾驶时间）
订单起始时间	夜间行驶（夜间行驶次数,夜间行驶时间）
保险信息	加速度（急加速次数,急刹车次数）
支付信息	其它车辆信息
其它运营信息	

3. 共享汽车租赁个性化业务设计

3.1 个性化租赁服务

本文提出的共享汽车租赁联盟中,汽车租赁平台起着信息撮合的作用.因为引入了区块链系统,联盟中的数据具有高可信性和高流通性,所以与传统的汽车租赁服务平台只起到中介作用相比,这里的汽车租赁服务平台可以简单的沟通各方,提供个性化的服务.

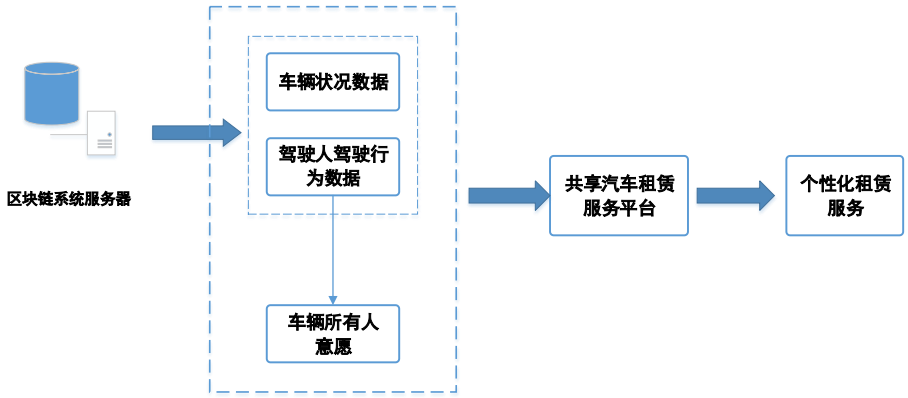

图 4 基于区块链系统的个性化租赁订单

如图 4 所示,因为区块链系统保存了租赁联盟中的车况数据和将要驾驶车辆的租赁人的驾驶行为数据,以这些数据进行分析可以进行个性化定制服务.例如通过驾驶行为数据分析可以获知驾驶人的驾驶技术和驾驶习惯优劣,对驾驶人的习惯进行评级.获得优异评级的驾驶人在租赁车辆中具有更大选择权,车辆所有人也乐于提供更大的优惠空间.通过对车况的信息评级,同时结合驾驶人的驾驶行为评级以及车辆所有人的意愿,汽车租赁服务平台可以对该订单进行差异化定价,提供差异化的服务响应.通过这种差异化的激励机制,可以有效引导车辆租赁者合理使用车辆,提高车辆供租双方的满意度,促进车辆供租双方的良好合作.

3.2 定制化车辆维护

车辆共享租赁联盟的商业模式中,安全性是保证正常运营的一个很重要因素.良好的车辆保养和高效的车辆救援维修服务是打造

高安全性的有效措施.通过区块链系统能够完整真实的记录车辆的维护信息,方便车辆保养机构和车辆维修机构通过历史记录定制维护计划.车辆保养和维修机构在参考了汽车租赁服务平台和车辆所有人的意愿之后,定制出个性化的车辆维护计划.车辆维护完成之后可以将维护情况直接写入区块链网络,供租赁服务平台和车辆所有人管理和查询,快速完成维护合同.

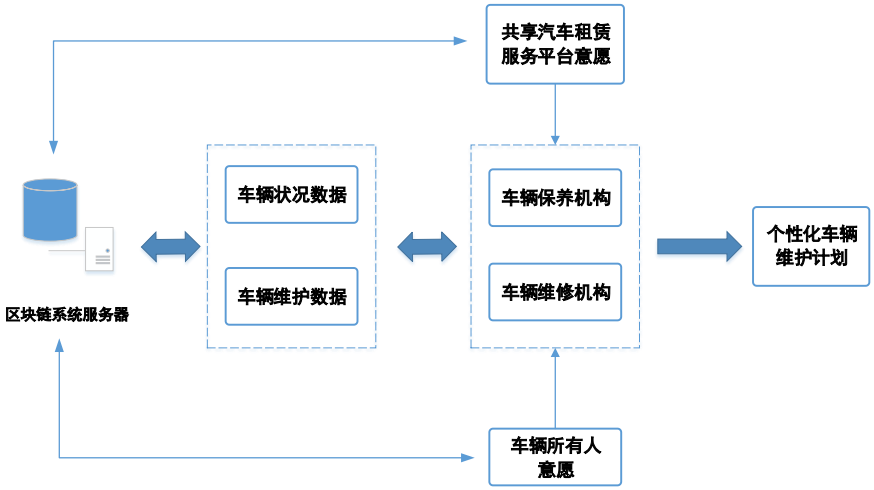

图 5 基于区块链系统的个性化车辆维护

3.3 精细化车辆保险

随着共享汽车租赁平台的发展,相关的汽车保险业务也应该同步展开.在相关的保险业务中,理赔时效是衡量保险服务水平的代表性指标,而在传统的保险业务中,存在着大量理赔时效纠纷问题[27].共享汽车使用过程中流动性较大,相对传统的汽车保险,责任更难认定.但是通过车联网系统和区块链系统将车辆状态及时记录存证,可以为后期的保险追溯提供很大的便利,提升保险服务的效率.

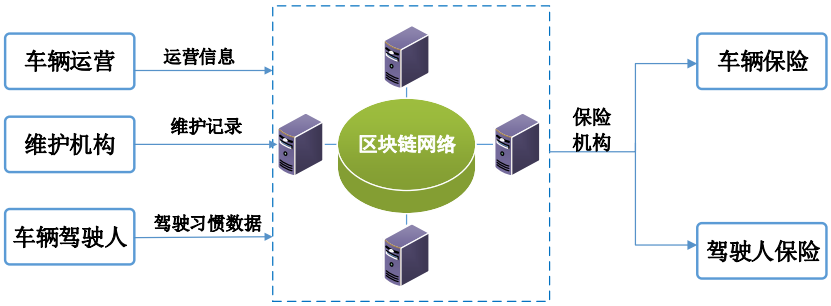

图 6 基于区块链系统的个性化车辆保险

随着物联网技术的发展和保险业务的不断创新,有研究者提出了车联网保险的概念[28].与本文提出的车联网系统作用定位相同,车联网保险通过车联网系统获取车辆静态属性和动态数据,进而分析驾驶人和车辆的安全等级,针对不同的等级提供差异化的保险费率和保险服务.本文在车联网保险的基础上,进一步引入了区块链技术.通过区块链技术,除了可以对车联网的数据进行记录以外,还可以记录车辆的维护信息和运营信息,既保证了数据记录的全面性,也保证了数据记录的安全性和可信性.通过对这些信息进行分析,保险机构可以获取更加详尽的参考,制定更加灵活的定价策略和服务策略,提供更加高效完善的个性化车辆保险和驾驶人保险服务.

4. 共享汽车租赁系统技术架构设计

共享汽车租赁系统架构设计上,底层是硬件系统.硬件既包括车联网设备、租赁车辆、车辆维护设备,也包括区块链系统服务器、传统的网络服务器和文件服务器.在底层系统之上,可以构筑文件服务和网站服务,用于对外提供业务服务.整个系统可以通过移动应用和网页应用与用户层进行交互.用户层可以通过前台系统就行业务查询和操作.

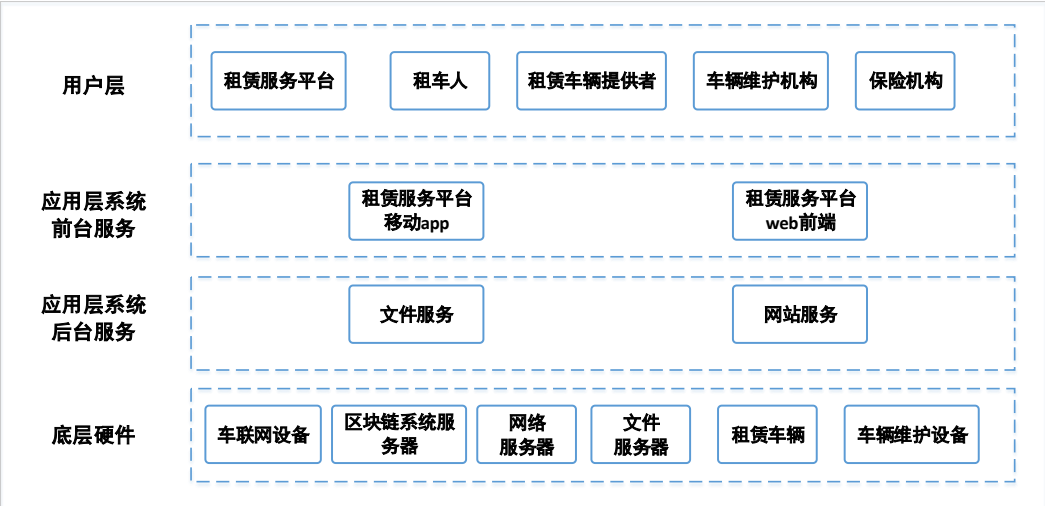

图 6 共享汽车租赁系统总体框架

需要说明的是,车联网设备采集的数据较为详尽,在长时间的运行中,会积累大量运营相关数据.由于区块链系统分布式账本的特性,这些数据需要在多个节点同步,直接存储原始数据会占用大量存储空间.所以在实际应用中,我们在区块链系统中存储的通常是数据块的哈希值.当我们需要对一些数据进行确认验证的时候,可以取得该数据块的哈希值,然后到文件服务器中进行比对验证.具体步骤如下所示:

(1) 每一个订单中通过车联网设备获取车辆数据,与联盟中成员提交的运营数据作为一个单位存储在传统的文件服务器上.这些原始数据为 M.原始数据 M 将会按照传统的存储技术进行管理,保证数据的安全性.

(2) 对原始数据的内容进行 hash,同时加上数据存储位置以及写入区块链系统的时间戳,组合成区块链系统的存储内容 B.生成的存储内容 B 将会区块链系统中进行广播存储.

$$\mathrm{B} = \mathrm{Hash}(M) + \mathrm{Url(M)} + timestamp(M)$$

(3) 客户端需要读取数据的时候,首先从传统的文件服务器获取原始数据 M,然后从区块链系统中获取相应的 B,按照上面公式进行计算,只有匹配正确的才能被客户端认可.

(4) 当联盟成员根据验证过的数据 M 分析得到自己的提案 C 写入区块链网络时,会在 B 后加上自己的私钥签名和签名时间,供其它成员验证.

$$\mathrm{C} = \mathrm{B} + \mathrm{signature}(role) + timestamp(role)$$

5. 结束语

本文提出的共享汽车租赁联盟的构建,在传统汽车租赁的基础上,引入了区块链技术和车联网技术,并由这些新技术推动了业务创新.通过共享汽车租赁联盟的构建,可以在车辆租赁者、车辆提供者、车辆租赁服务平台、车辆维护机构和车辆保险机构之间构建可信的数据连通渠道,实现相互之间高效可信的合作.同时,基于区块链系统和车联网系统的数据可信分析,可以提供个性化的定制业务.包括定制化的车辆租赁订单服务,定制化的车辆维护服务和定制化的车辆保险服务.但是目前系统设计中也存在一些不足,主要是采用开源的 fabric 架构,系统定制化程度较低,同时对一些用户数据隐私的问题没有进行充分的考虑.下一步可以参考一些新的密码学技术,例如同态加密等方法,对用户数据隐私进行更加完备的管理.

References:

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Cheah E T, Fry J. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin[J]. Economics Letters, 2015, 130: 32-36.

[3] Ober M, Katzenbeisser S, Hamacher K. Structure and anonymity of the bitcoin transaction graph[J]. Future internet, 2013, 5(2): 237-250.

[4] Bohannon J. Why criminals can't hide behind Bitcoin[J]. Science, 2016.

[5] 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.

[6] 马小峰, 杜明晓, 余文兵, 等. 基于区块链的供应链金融服务平台[J]. 大数据, 2018, 4(1): 13-21. 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理: 问题与方法[J]. 软件学报, 2018, 29(1): 150-159.

[7] 王云, 何明久. 区块链与物联网的应用案例分析[J]. 集成电路应用, 2018, 35(3): 70-74.

[8] 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理: 问题与方法[J]. 软件学报, 2018, 29(1): 150-159.

[9] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487.

[10] 叶聪聪, 李国强, 蔡鸿明, 等. 区块链的安全检测模型[J]. 软件学报, 2018, 29(5): 1348-1359.

[11] 王建强, 吴辰文, 李晓军. 车联网架构与关键技术研究[J]. 微计算机信息, 2011, 27(4): 156-158.

[12] 郭文倩, 谢健骊, 汪洋. 基于物联网技术的兰州市公交车工况数据采集系统研究[J]. 自动化与仪器仪表, 2018, 3: 013.

[13] 诸彤宇, 王家川, 陈智宏. 车联网技术初探[J]. 公路交通科技 (应用技术版), 2011, 5: 266-268.

[14] Larimer D. Transactions as proof-of-stake[J]. 2013.

[15] Lamport L. The part-time parliament[J]. ACM Transactions on Computer Systems (TOCS), 1998, 16(2): 133-169.

[16] Lamport L. Paxos Made Simple, Fast, and Byzantine[C]//OPODIS. 2002, 3: 7-9.

[17] Ongaro D, Ousterhout J K. In search of an understandable consensus algorithm[C]//USENIX Annual Technical Conference. 2014: 305-319.

[18] Garg N. Apache Kafka[M]. Packt Publishing Ltd, 2013.

[19] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on computing, 1989, 18(1): 186-208.

[20] Micali S, Pass R. Local zero knowledge[C]//Proceedings of the thirty-eighth annual ACM symposium on Theory of computing. ACM, 2006: 306-315.

[21] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of secure computation, 1978, 4(11): 169-180.

[22] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things[J]. Ieee Access, 2016, 4: 2292-2303.

[23] Bahga A, Madisetti V K. Blockchain platform for industrial internet of things[J]. Journal of Software Engineering and Applications, 2016, 9(10): 533.

[24] 刘小洋, 伍民友. 车联网: 物联网在城市交通网络中的应用[D]. , 2012.

[25] 董伟栋, 霍潞露. 发达国家汽车租赁业对我国的启示[J]. 汽车与配件, 2013 (7): 44-47.

[26] 夏鸿文, 赵侃, 刘应吉. 我国汽车租赁发展现状及管理对策研究[J]. 交通节能与环保, 2015, 11(6): 43-47.

[27] 郗宏伟, 褚红宽. 关于汽车保险理赔时效纠纷的研究[J]. 现代商业, 2018, 2: 117.

[28] 彭江琴. 基于 GID 的车联网保险 UBI 费率与驾驶行为评分研究[D]. 南京邮电大学, 2016.