

# 基于区块链的高速联网收费数据传输应用研究

于欣海<sup>1</sup>, 黄欣哲<sup>2</sup>, 梁海<sup>2\*</sup>, 丁勇<sup>2</sup>

(1. 安徽省高速公路联网运营有限公司, 安徽 合肥 230031;

2. 桂林电子科技大学, 广西 桂林 541004)

**摘要:**自高速公路取消省界收费后, 跨省车辆通行的数据在多个省份之间存在的分散存储、数据共享流程繁琐和隐私泄露等问题日益凸显。为解决上述问题, 该文提出一种基于区块链的高速公路联网收费数据共享方案, 基于区块链链接省部两级联网中心, 使其共同维护同一个账本。并采取对称加密和非对称加密相结合的方式对链上数据进行处理, 以实现数据的安全存储和用户的隐私保护。同时利用智能合约实现跨省结算和数据的实时共享。为提高链上数据的检索效率, 基于数据表加密技术实现链上链下数据的安全同步存储和访问。实验结果表明, 该方案不仅能够满足高速公路车辆通行数据共享的一致性、安全性、可信性要求, 而且其区块链存储和查询 TPS 完全满足安徽省高速公路联网收费场景下的实际需求。未来随着通行数据不断增长的情况, 可采用增加节点的方式提升业务处理能力, 性能和功能优势更加突出。

**关键词:**区块链技术; 智能合约; 联网收费; 数据共享; 隐私保护

中图分类号: TP31; U491.1

文献标识码: A

文章编号: 1673-629X(2023)10-0051-08

doi: 10.3969/j.issn.1673-629X.2023.10.009

## Data Sharing Scheme for Expressway Networking Charging Based on Blockchain

YU Xin-hai<sup>1</sup>, HUANG Xin-zhe<sup>2</sup>, LIANG Hai<sup>2\*</sup>, DING Yong<sup>2</sup>

(1. Anhui Expressway Network Operation Co., Ltd., Hefei 230031, China;

2. Guilin University of Electronic Technology, Guilin 541004, China)

**Abstract:** Following the elimination of provincial boundary tolls on expressways, the concerns of decentralized storage of inter-provincial vehicle traffic data among numerous provinces, burdensome data sharing protocols, and privacy breaches have become more prevalent. Therefore, we propose a blockchain-based expressway network toll data sharing system that connects provincial and ministerial two-level networking centers using blockchain technology so that they can maintain the same ledger collectively. The combination of symmetric and asymmetric encryption is used to process data on the blockchain in order to guarantee safe data storage and user anonymity. Simultaneously, smart contracts are utilized to realize real-time interprovincial settlement and data sharing. To improve the retrieval efficiency of data on the blockchain, secure synchronous storage and access to data on and off the blockchain are implemented using data table encryption technology. The experiments demonstrate that it not only meets the consistency, security, and credibility requirements for the exchange of expressway vehicle traffic data, but its blockchain storage and query TPS also meet the actual requirements of the Anhui Province expressway networking toll scene. When traffic data continues to increase in the future, the capacity of data storing and processing can be expanded by adding nodes, and its performance and functional benefits will increase.

**Key words:** blockchain technology; smart contract; online charging; data sharing; privacy protection

## 0 引言

2020年1月1日, 全国29个联网省份的487个省界收费站全部取消, 同年5月, 实现了“一次行程、一张账单、一次扣费、一次告知”的总体目标, 高速公路出入口的收费站拥堵缓行的状况得到全面缓解<sup>[1]</sup>, 有效改善了人民群众的出行体验, 助力节能减排、降本增

效, 取得了明显的社会效益和经济效益。

而车辆跨省出行传统收费清算共有三个阶段: 首先, 省部两级联网中心相互通信启动行车计费服务。其次, 由部联网中心根据各省联网中心上传的信息拟合数据并计算通行费用。最终, 由省联网中心将通行费用返回至结算收费站。

收稿日期: 2022-12-29

修回日期: 2023-04-28

基金项目: 国家自然科学基金(62172119); 广西自然科学基金(2019GXNSFGA245004)

作者简介: 于欣海(1978-), 男, 高级工程师, 研究方向为交通信息化; 通信作者: 梁海(1982-), 男, 讲师, 硕士, 研究方向为区块链。

在这一过程中,各省级联网中心不仅要跨省请求数据,而且还依赖中心化服务器的计算结果,不仅导致收费结算流程繁琐,降低收费站的通行效率,同时跨省结算请求数据时可能会造成隐私泄露和数据篡改等问题,带来极大的信息安全隐患。

针对这一问题,国内外研究人员开展了大量研究并提出了不同的解决方案。闫卫喜等人<sup>[2]</sup>对区块链技术在交通运输业的应用指出数据资源共享程度不足、数据价值挖掘深度不足和隐私保护不够的问题,为后续研究指明了方向。为了解决高速公路车辆通行数据零散(资源共享)问题,王若华等人<sup>[3]</sup>提出一种基于超级账本的高速公路通行数据区块链,使用链码对通行数据上链,同时快速完成数据共识的判断。为了深度分析数据价值,张利华等人<sup>[4]</sup>提出双链数据存储模型来对历史数据进行分析,解决恶意伪造、篡改数据等问题。

为解决高速收费中的隐私保护问题,王秀丽等人<sup>[5]</sup>提出一种应用区块链的数据访问控制与共享模型,利用属性基加密对企业数据进行访问控制与共享,达到细粒度访问控制和安全共享的目的。王士成等人<sup>[6]</sup>利用属性加密技术和智能合约技术,实现了自动化安全数据共享。张正昊等人<sup>[7]</sup>提出了一种支持监管的敏感数据可控共享方案,通过使用动态累加器技术实现敏感数据的访问控制,实现数据拥有方对数据的可控性。

然而,现有场景中很少有对高速路收费进行隐私保护,大多数的数据传输方案不能满足高速收费场景,并且当数据量足够大时可能造成数据阻塞,降低数据的共享效率。因此,有必要针对高速联网收费场景设计一种基于分布式支持隐私保护的数据传输共享方案。

为了解决高速联网收费场景所面临的挑战,提出一种基于区块链的高速联网收费数据共享方案。其中通过区块链将省部两级联网中心全部链接在一起以维护一个共同的账本,并通过智能合约实现高速跨省结算的自动化,以此实现数据的实时共享;对于隐私保护,结合非对称加密和对称加密实现链上数据的密文存储;对于数据高效的检索,设置了链上链下数据库同步机制,采用表加密的形式存储数据,任何未获得权限的用户都会被拒绝访问。

在具体功能上,相比于传统的高速收费系统,基于区块链实现了车辆通行数据的分布式存储和访问,保证了数据的实时共享。同时为保护用户隐私,对链上敏感数据进行加密处理,使其具有更高的安全性;对于检索模块,相比于纯链上数据存储的方式,采取链上链下数据库同步机制,降低对链上的访问开销,同时优化

数据存储结构,进一步提高检索效率,并同步降低存储开销。

在性能上,对 2 000 000 笔存证交易(存证数据大小 200 Bytes),分别对持续时长为 10 分钟左右和 5 分钟左右,并发数为 180 增加到 300 进行测试。实验结果表明:区块链存储 TPS 均值、查询 TPS 均值完全满足安徽省高速公路联网收费需求,在通行数据不断增长的情况下,可以采用增加节点的方式提升业务处理能力。

## 1 相关技术

### 1.1 区块链技术

区块链是一种去中心化的分布式账本技术<sup>[8]</sup>,是分布式数据库、密码算法<sup>[9]</sup>、共识机制<sup>[10-11]</sup>和智能合约<sup>[12-14]</sup>等技术的有机结合。

区块链数据由去中心化网络上的多个对等节点共同维护的相同副本组成。数据副本又将所有数据以区块的形式进行存储,区块之间则利用哈希指针串联成链。每个区块由区块头和区块体组成,区块体由具体数据组成,区块头由前块哈希、时间戳、版本号等系统性信息和当前块哈希组成。通过默克尔树的方式将区块内全部交易的哈希值计算出区块哈希。由于哈希所具有的极难碰撞的性质,因此任何人可以通过某一交易哈希值及其兄弟路径的哈希值求出一个区块哈希,通过该区块哈希判断交易是否被修改,若求出的区块哈希与区块本身的哈希不同,则说明交易被修改或是不存在。

由于每个区块的区块头中都包含了前块哈希,这就使得区块之间关系紧密,并且单个区块的更改会因为无法匹配头部哈希值和后续块中的前块哈希值而验证失败。在去中心网络和这种区块链存储的模式下,少部分节点的更改和外部恶意篡改都能因为与大部分节点数据不一致而被识别出来,因此链上数据具有不可篡改、可追溯、可信的特点。

除此之外,区块链系统中的共识机制确保了上链数据的正确性和一致性,智能合约则使得开发者能够在区块链上进行应用的开发。

### 1.2 数据隐私技术

区块链上记录的数据在上链过程中,需要经过各区块链节点达成共识,所有数据必须公开给区块链网络中的所有节点,这将会导致区块链出现隐私泄露风险<sup>[15]</sup>。为了解决这个问题,需要对必要的数据进行加密,再上链,最终以密文的形式存储在链上,从而保证数据的隐私性和安全性。

目前已经有多种区块链数据隐私保护方案,如交易数据加密<sup>[16]</sup>、零知识证明<sup>[17]</sup>、同态加密<sup>[18]</sup>等,均是

依托于密码学算法。但是不同的方案在安全性和实用性上各有优劣。针对高速公路联网收费涉及多方参与的业务特点,以及对于安全性和实用性的权衡,在数据存储与共享过程中除了实现交易上链,重点还在交易产生的记录数据的上链存储、上链运算,由于高速公路联网收费数据包含通行用户的隐私信息,因此如何在链上安全存储,且实现数据访问权限的控制尤为重要。

该文将采用链上数据库表加密技术,利用非对称密码算法及对称密码算法的方式,任何未被授权的账

户无法解密表交易操作。

## 2 高速公路联网收费及清算现状

### 2.1 联网收费系统架构

全国联网收费系统框架由收费公路联网结算管理中心(以下简称“部联网中心”)、省(区、市)联网结算管理中心(以下简称“省联网中心”)、省内区域/路段中心、ETC 门架、收费站、ETC 车道、ETC/MTC 混合车道等组成,如图 1 所示。

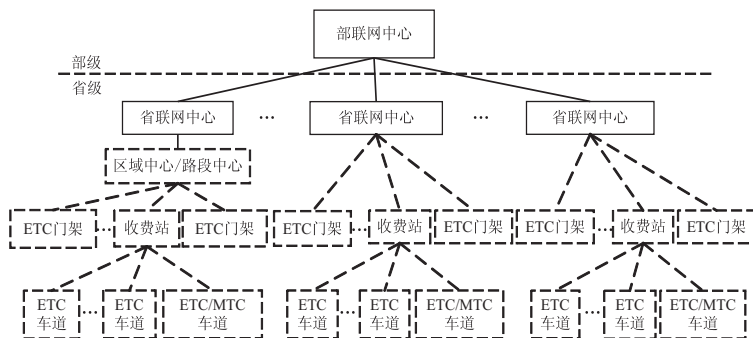


图 1 全国联网收费系统框架

其中部联网中心主要实现跨省 ETC 清分结算和跨省其他交易拆分结算、全网费率管理等功能;省联网中心主要实现本省(区、市)ETC 清分结算和其他交易拆分结算、本省(区、市)路段费率管理功能。

### 2.2 收费与清分流程

#### 2.2.1 车辆收费流程

高速公路通行车辆收费方式主要有电子不停车自动收费(ETC)和人工半自动车道收费(MTC)两种。

(1)ETC 车辆通过 ETC 门架系统实现分段计费,通过车载单元(OBU)和后台记账形式自动完成扣费。

(2)MTC 车辆采用 5.8 GHz 复合通行卡<sup>[15]</sup>(CPC 卡)为通行介质,辅以车牌图像识别,在入口将计费车型信息写入 CPC 卡,通过 ETC 门架系统实现分段计费,在出口进行人工收费。

#### 2.2.2 清分结算流程

清分结算业务采用部、省两级模式,部联网中心主要完成跨省 ETC 通行费清分结算以及跨省 MTC 通行费拆分结算,省联网中心主要完成省(市、区)内 ETC 清分结算和 MTC 通行费的拆分结算。

##### (1)ETC 车辆交易清分结算流程。

ETC 车辆交易流水通过省联网中心实时上传至部联网中心,发行服务机构下载交易数据进行记账。记账确认后,部联网中心生成清分结算通知书,各收费方省联网中心和发行服务机构对清分结算通知书进行确认,部联网中心按照清分结算结果进行资金归集和划拨。省联网中心完成省(市、区)内 ETC 清分结算。

##### (2)MTC 车辆交易拆分结算流程。

部联网中心接收各省联网中心上传的 MTC 车辆通行交易数据,每日根据实际通行省(区、市)对交易数据进行拆分结算,并下发结算通知书由各省联网中心确认,部联网中心根据轧差金额进行资金归集和划拨。省联网中心完成省(市、区)内 MTC 通行费的拆分结算。

#### 2.2.3 存在的问题

##### (1)数据同步过程繁琐。

数据同步过程繁琐主要体现在以下两个方面。一是两级清分模式涉及部联网中心、省联网中心、ETC 卡发行服务机构、银行等多方参与,需要多个省联网中心分别与部联网中心进行数据对账和结算通知书确认,受数据合规性、及时性、准确性影响,容易出现数据补充同步和结算通知书反复确认情况,使得清分结算周期变长效率降低。二是由于需数据同步更新的省联网中心和收费站众多,一旦出现交易数据、计费参数更新不及时、不完整等情况,将导致不同路段、省份之间出现清算争议。

##### (2)数据隐私的泄漏。

由于数据原本是保存在独自的省联网中心,当需要跨省结算时,需要共享数据,在共享过程中数据的完整性和安全性难以得到保证,因此可能存在用户数据泄露的问题。

## 3 基于区块链的高速联网收费数据共享方案

### 3.1 总体系统架构

为了解决现有的高速跨省收费与清分系统的数据



同步过程繁琐和数据隐私安全的问题,提出一种基于区块链的高速联网收费数据共享方案。在不改变高速公路原有联网收费业务系统的前提下,引入区块链进行数据存储来实现各省联网中心间数据的同步,当车辆进出高速路口以及高速上途径 ETC 门架时,车辆信息会被自动采集并上链,区块链各节点之间会同步这些信息。

设计一套基本的通用的数据库表来解决传统方式下,不同省联网中心数据格式不同,交易数据与计费参数不完整可能导致的问题。将分别设计跨省的和省内

的交易清分结算方案,并以智能合约形式写到链上,当车辆通过高速出入口以及 ETC 门架时,会自动调用智能合约将对应信息自动采集,并自动完成跨省和省内的交易清分结算。同时设计一套加密解密以及访问控制机制,在保护用户隐私数据安全的基础上,实现车辆通行数据以及清分结算数据的多方共享。另外,为了保证系统的效率,会在外置一个传统数据库,通过访问控制的接口将链上数据保存下来,方便查询。整体架构如图 2 所示。

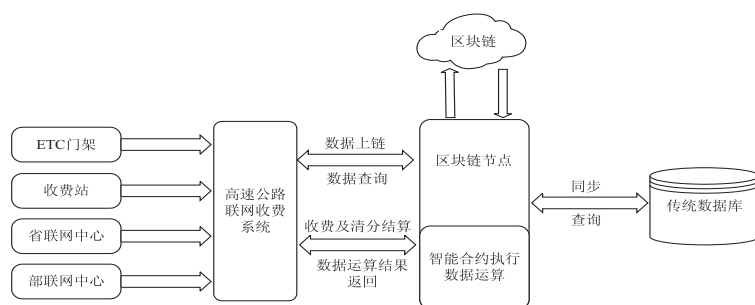


图 2 方案整体架构

为此,首先需建立区块链网络,省联网中心、部联网中心作为区块链的节点对数据进行存储,高速公路联网收费系统与区块链网络的对接,当有车辆驶入时,调用智能合约将驶入信息存入到链上,当车辆通过收费系统驶出时,自动调用智能合约去链上检索对应车辆的驶入信息,自动计算扣费。车辆交易流水、通行记录、清分结算等数据以交易记录的形式记录到区块链上,并通过链上数据库表访问控制机制授权给对应的省部中心,将数据同步到传统数据库中,方便对数据的查询,在必要时能结合链上数据进行验证。

### 3.2 数据库表设计

为了解决不同省联网中心数据格式不同,交易数据、计费参数不完整可能导致的问题,设计一套通用

的、基础的数据库表用来保存车辆通信信息。

针对高速公路联网收费的实际业务场景,需要将 ETC 门架、收费站采集的车辆 ETC 交易流水、ETC 通行记录、CPC 卡通行记录、收费站、收费车道、抓拍时间、车牌号、车型等收费关键信息,以及省部联网中心经过计算生成的清分结算数据上链存储。

表中数据分为普通数据表和加密数据表两种存在形式,区别在于表操作具体内容在链上是否以密文形式存储,加密表操作在 SDK 中进行加密,然后以密文形式存储在区块链上,并且以密文的形式存储到实体数据库中。

高速公路联网收费数据库表以及对应的访问权限控制如图 3 所示。

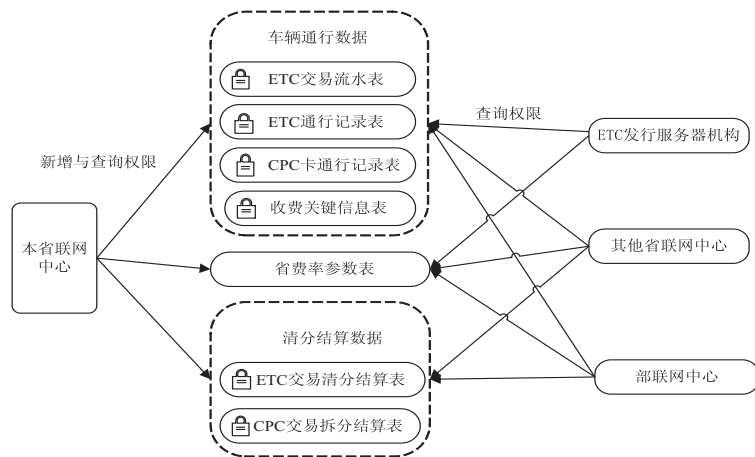


图 3 数据库表授权共享

ETC 交易流水表、ETC 通行记录表、CPC 卡通行记录表等为加密数据表,由省联网中心创建,授权给其

他省联网中心和部联网中心查询权限,省联网中心仅限于查询与本省相关的跨省通行数据,部联网中心可

以查看所有跨省车辆通行数据。

省费率参数表为普通数据表,由省联网中心负责创建和维护,授权给所有链上用户查询权限。

ETC 交易清分结算表和 CPC 交易拆分结算表为加密数据表,由省联网中心负责创建,授权给其他相关的省联网中心、部联网中心、ETC 发行服务机构等查询权限,省联网中心仅限于查询与该省相关的跨省清分结算数据,部联网中心可以查看所有的跨省清分结算数据。这不仅使得资源可以得到合理的配置,而且管理水平也得到一定的提高,对不同路段的协调工作也更加高效。

### 3.3 跨省交易清分结算方案

针对 ETC 车辆跨省交易,当车辆经过收费站出口车道完成交易时,即触发跨省清分结算智能合约,基于部级链上该车辆在各省的 ETC 交易流水(或通行凭证)、ETC 通行记录等信息,按照预先设定的交易清分规则,自动执行对本次 ETC 交易的清分结算,并将 ETC 交易清分结算结果在部级链上存储,同时为相关的省联网中心、ETC 发行服务机构、银行设置共享访问权限。针对 MTC 车辆跨省交易,将基于部级链上该车辆在各省的 CPC 卡通行记录、通行流水、交易日志等信息,按照预先设定的交易拆分规则,自动执行对本次交易的拆分结算,并将 MTC 车辆交易拆分结算结果在部级链上存储,为相关的省联网中心、ETC 发行服务机构、银行设置共享访问权限。

部联网中心每日通过智能合约自动完成当日所有单笔跨省 ETC 车辆交易清分结算结果汇总,形成当日跨省 ETC 车辆交易清分结算结果,并按照此清分结算结果进行资金归集和划拨;通过智能合约自动完成当日所有跨省 MTC 交易拆分结算结果汇总,形成当日跨省 MTC 车辆交易拆分结算结果,并按照此拆分结算结果,根据轧差金额进行资金归集和划拨。

### 3.4 省内交易清分结算方案

针对 ETC 车辆省内交易,当车辆经过收费站出口车道完成交易时,即触发省内清分结算智能合约,基于省级链上该车辆在省内的 ETC 交易流水(或通行凭证)、ETC 通行记录等信息,按照预先设定的交易清分规则,自动执行对本次 ETC 交易的清分结算,并将 ETC 交易清分结算结果在省级链上存储,同时为相关的收费站、ETC 发行服务机构、银行设置共享访问权限。针对 MTC 车辆省内交易,将基于省级链上该车辆在各省的 CPC 卡通行记录、通行流水、交易日志等信息,按照预先设定的交易拆分规则,自动执行对本次交易的拆分结算,并将 MTC 车辆交易拆分结算结果在省级链上存储,为相关的收费站、ETC 发行服务机构、银行设置共享访问权限。

省联网中心每日通过智能合约自动完成当日所有省内 ETC 车辆交易清分结算结果汇总,形成当日省内 ETC 车辆交易清分结算结果,并按照此清分结算结果进行资金归集和划拨;通过智能合约自动完成当日所有省内 MTC 交易拆分结算结果汇总,形成当日省内 MTC 车辆交易拆分结算结果,并按照此拆分结算结果,根据轧差金额进行资金归集和划拨。

### 3.5 数据存储与授权共享流程

由于区块链是在去中心网络下由多个对等节点共同维护的,区块链中的数据对所有用户都是公开的,因此存在对特定数据进行加密的需求。在有些场景下即需要区块链以维护数据的可靠与可信,又不希望泄露链上的用户信息。因此,可以对必要的数据进行加密保存,同时在链上保存访问权限控制信息,当有节点或者用户需要访问链上加密数据时,必须先验证链上的访问权限控制信息,通过验证后智能合约会对所访问数据自动进行解密。其流程如图 4 所示。

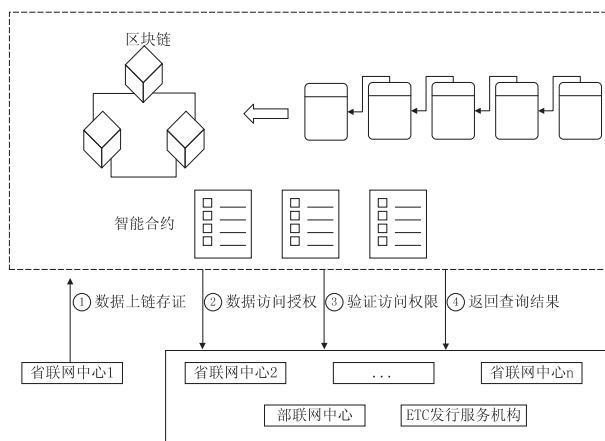


图 4 高速公路车辆通行数据共享示意图

当车辆驶入高速,信息被记录上链时,先由本地的省联网中心(图中的省联网中心 1)对数据信息进行加密上链,即数据上链存证;省联网中心在上链时会对数据的访问等权限赋予不同的用户或节点,即数据访问授权;当不同的用户或者节点需要访问数据时需要先对自己的身份信息进行验证,以判断是否有对应数据的访问权限,即验证访问权限;在对访问发起方的身份进行验证并确认其具有相应权限之后返回查询结果。

为了实现以上流程,设计了一套数据加密流程,主要包含六个部分:身份密钥初始化,创建加密表,加密表授权,插入数据,授权数据给用户,用户读取数据。身份数据初始化是生成对应节点和用户的公私钥身份信息;创建加密表则是将车辆信息表格进行加密;加密表授权会对创建者以外的身份授予权限,使其能够读取表格信息;插入数据则是对加密表的信息进行修改,添加车辆新的信息;授权数据给用户则是将加密表权限授予给用户;用户读取数据则是用户读取链上加密

的数据。

数据存储及共享主要包含五个部分:初始化,创建加密表,加密表授权,授权数据给用户,用户读取数据,其目的和具体细节如下:

### (1) 身份密钥初始化。

在身份密钥初始化阶段,按照高速公路收费的组织架构,在区块链上为各个组织注册合法账户,每个用户生成一对公私钥  $(Pk_i, Sk_i)$  由用户自身保存,其中对公钥进行哈希运算得到身份 id 并上链,其过程可由算法 1 表示。

算法 1:

1. 对任意用户  $account_i$ , 使用椭圆曲线算法生成公私钥  $(Pk_i, Sk_i)$

2. 生成用户  $account_i$  身份 id,  $account_i\_id = sha256(Pk_i)$

在实际中使用 Ed25519 算法生成公私钥,使用 sha256 算法对公钥进行哈希运算得到身份 id。

### (2) 创建加密表。

创建加密表是将数据以加密的方式进行保存,由各省联网中心负责创建,各省联网中心默认对加密表具有管理权限,其流程可由算法 2 表示。

算法 2:

1.  $account_i$  发送创建表交易:  $T = \{table\_name, table\}$ ,  $Sig_i = SignatureECC(T, Sk_i)$

2. 使用 AES 算法随机生成对称密钥  $K$

3. 使用  $K$  对创建表语句加密,得到密文  $C = EncryptAES(table, K)$

4. 使用公钥  $Pk_i$  对  $K$  加密,得到加密令牌  $X_i = EncryptECC(K, Pk_i)$

5. 将  $X_i$  和  $C$  保存至链上,保存的格式为数组  $\{Pk_i, table\_name, X_i, C, Sig_i, R \mid U \mid D\}$

其中,  $R$  代表读取权限;  $U$  代表修改权限;  $D$  代表删除权限。

### (3) 加密表授权。

当数据以加密表的形式存储之后,省联网中心负责将加密表授权给其他相关的省联网中心、部联网中心、ETC 发行服务机构等查询权限以便进行相关的业务操作,而未被授权的用户将不能访问加密表,具体流程可由算法 3 表示。

算法 3:

1. 用户  $i$  根据  $account_i\_id$  和  $table\_name$  从链上获取  $X_i$  和  $C$

2. 使用  $Sk_i$  对  $X_i$  解密,得到 AES 算法密钥:  $K = DecryptECC(X_i, Sk_i)$

3. 使用  $K$  对  $C$  解密,  $table = DecryptAES(C, K)$

4. 使用  $Sk_i$  对  $T = \{table\_name, table\}$  签名,  $s = SignatureECC(T, Sk_i)$

5. 验证  $s$  和链上  $Sig_i$  是否一致,如果不一致,退出;否则进入步骤 6

6. 使用  $account_j$  的公钥  $Pk_j$  对  $K$  加密,得到加密令牌  $X_j =$

$EncryptECC(K, Pk_j)$

7. 发出邀请给  $account_j$  账户对  $T$  进行签名:

$Sig_j = SignatureECC(T, Sk_j)$

8.  $\{Pk_j, table\_name, X_j, C, Sig_j, R \mid U \mid D\}$  记录保留至链上

(4) 插入数据。

当跨省通行车辆在高速出口完成收费后,自动触发存证智能合约进行车辆通行数据上链存证,这就需要修改链上保存的加密表。在这个过程中存证智能合约首先会判断用户是否具有对应权限,如果没有权限,则会退出,如果有权限,则继续对新增数据进行加密并插入到加密表中,具体流程可由算法 4 表示。

算法 4:

1. 账户  $account_i$  发起插入表记录交易:  $\{table\_name, (fields, values)\}$

2. 通过  $account_i\_id$  和  $table\_name$  获取记录  $\{Pk_i, table\_name, X_i, C, Sig_i, R \mid U \mid D\}$

3. 判断是否有  $U$  权限,如果没有退出;否则进入步骤 4

4. 使用  $Sk_i$  对  $X_i$  解密,得到 AES 算法密钥:  $K = DecryptECC(X_i, Sk_i)$

5. 使用  $K$  对  $C$  解密,  $table = DecryptAES(C, K)$

6. 使用  $Sk_i$  对  $T = \{table\_name, table\}$  签名,  $s = SignatureECC(T, Sk_i)$

7. 验证  $s$  和链上  $Sig_i$  是否一致,如果不一致,退出;否则进入步骤 8

8. 使用 AES 算法随机生成对称密钥  $K_2$

9. 使用  $K_2$  对记录进行加密,得到记录密文:  $R = AES(\{fields, values\}, K_2)$

10. 使用  $Pk_i$  对  $K_2$  加密,得到加密令牌  $X_{2i} = EncryptECC(K_2, Pk_i)$

11. 计算  $record\_id = sha256(\{table\_name, fields, values\})$

12. 计算记录的签名,  $RSig_i = SignatureECC(record\_id, Sk_i)$

13. 将记录  $\{record\_id, Pk_j, table\_name, X_{2i}, R, RSig_i, R \mid U \mid D\}$  记录至区块中

14. 返回  $record\_id$

(5) 将数据授权给用户。

用户完成数据插入后,随即触发授权智能合约,自动为车辆通行数据途径的各省联网中心、部中心等用户设置数据访问权限,具体流程可由算法 5 所示。

算法 5:

1. 通过  $record\_id$  从链上获取记录,  $\{record\_id, Pk_i, table\_name, X_{2i}, R, RSig_i, R \mid U \mid D\}$

2. 查看是否有  $R \mid U \mid D$  权限,如果没有则退出,否则进入步骤 3

3. 使用  $Sk_i$  解密  $X_{2i}$ ,  $K_2 = DecryptECC(X_{2i}, Sk_i)$

4. 生成签名  $s = SignatureECC(record\_id, Sk_i)$

5. 验证  $s$  和链上的  $RSig_i$  是否一致,如果不一致退出,否则进入步骤 6

6. 使用  $account_j$  账户的私钥  $Sk_j$  对  $record\_id$  签名,  $RSig_j =$



SignatureECC(record\_id, Sk<sub>j</sub>)

7. 使用 Pk<sub>j</sub> 对 K<sub>2</sub> 进行加密, 得到加密令牌 X<sub>2j</sub> = EncryptECC(K<sub>2</sub>, Pk<sub>j</sub>)

8. 将记录 { record\_id, Pk<sub>j</sub>, table\_name, X<sub>2j</sub>, R, RSig<sub>j</sub>, R | U | D } 记录至区块中

(6) 用户读取授权数据。

用户读取区块链上的共享数据, 将会触发智能合约, 智能合约首先对用户的身份进行验证, 判断是否具有访问控制权限, 如果没有权限则退出, 如果有权限, 则可以进行数据的解密供用户访问, 具体过程可由算法 6 所示。

算法 6:

1. 账户 account<sub>i</sub> 发起读取记录交易: { record\_id, Pk<sub>i</sub>, table\_name, X<sub>2i</sub>, R, RSig<sub>i</sub>, R | U | D }
2. 查询是否存在标志 R; 如果没有则退出, 否则进入步骤 3
3. 计算 s = SignatureECC(record\_id, Sk<sub>i</sub>)
4. 判断 s 和 RSig<sub>i</sub> 是否相等, 不相等则退出; 否则进入步骤 5
5. 使用 Sk<sub>i</sub> 解密 X<sub>2i</sub>, K = DecryptECC(X<sub>2i</sub>, Sk<sub>i</sub>)
6. 使用 K 解密 R 记录, record = DecryptAES(R, K<sub>2</sub>)

## 4 安全性分析

### 4.1 数据存储安全

区块链上的数据由按时间顺序各个区块组成, 数据上链以后将不能被篡改。由于采用去中心化数据存储架构, 因此对任何一个节点的攻击都无法使整个网络瘫痪, 也无法控制整个链上的数据。基于智能合约数据存储与共享, 保证数据使用过程安全, 同时将每笔交易都上链存储, 数据有据可查, 可以进行溯源审计。以上的区块链技术特点, 保证了数据的安全性。

### 4.2 用户隐私保护

在用户数据隐私上, 采用了基于非对称和对称密码学算法的加密表技术, 数据在上链之前进行加密, 并且加密令牌也是密文上链, 只有数据上链的操作者能够进行解密。

假设恶意用户获取区块链的访问方式, 开始遍历区块链交易, 但是获取到的链上表操作交易内容均是密文, 在没有表拥有者私钥或者未被授权情况下, 是无法解密数据的; 而且即使恶意用户自己运行一个节点, 也无法将链上创建的加密表同步到自己运行的节点的

数据库中, 因为无法解密就无法知道当前数据库操作内容。

### 4.3 访问权限控制

高速公路联网收费业务涉及多方参与, 各参与方所需数据以及访问权限各不相同, 采用链上数据库表的授权机制, 基于非对称密码学算法, 对加密令牌进行转加密, 并在链上记录权限, 不可篡改。将加密表及链上权限控制相结合, 实现链上数据的授权访问控制。

假设恶意用户真的伪装为监管方, 获取了数据访问权限, 并且在本地运行一个节点同步了数据, 但是因为加密表授权机制的精细控制, 对于监管方只授予查询权限, 因此恶意用户只能获取到历史数据, 而无法对链上数据进行修改, 保障区块链以及链上数据安全不被篡改。

## 5 实验与结果分析

### 5.1 实验环境搭建

实验选择 ChainSQL 去搭建区块链, 并模拟出高速收费系统, 编写两类智能合约, 一类是存证类合约, 用来记录车辆信息, 进行收费和清分, 另一类是查询类合约, 用来查询链上数据。调用存证类合约会往链上增加数据, 查询类合约不会往链上新增数据。搭建的链包含 4 个共识节点, 并有 4 台压测机共 8 台硬件设备, 硬件配置均为戴尔 R730 服务器, 2 \* CPU 英特至强 E5-2620 v3, 2.4 GHz, 15 M 缓存, 内存 8 \* 16 G RDIMM, 2133 MT/s, 硬盘 10 \* 1.2 TB 10 k RPM SAS 6 Gbps 2.5 英寸热插拔硬盘, 万兆网卡。区块链节点操作系统为 Ubuntu 18.04.5 LTS。

### 5.2 实验过程与结果分析

进行三类实验去测试系统性能能否满足高速公路收费场景, 分别是普通场景下存证交易的性能测试, 高并发场景下存证交易的性能测试和高并发场景下查询交易的性能测试。采用交易吞吐量 (TPS) 和确认交易吞吐量 (CTPS) 作为性能衡量指标。

对于普通场景下的存证交易性能测试, 4 台压测机共发送 2 000 000 笔存证交易 (存证数据大小 200 Bytes), 持续 10 分钟左右, 并发数为 180, 测试结果如图 5 所示。

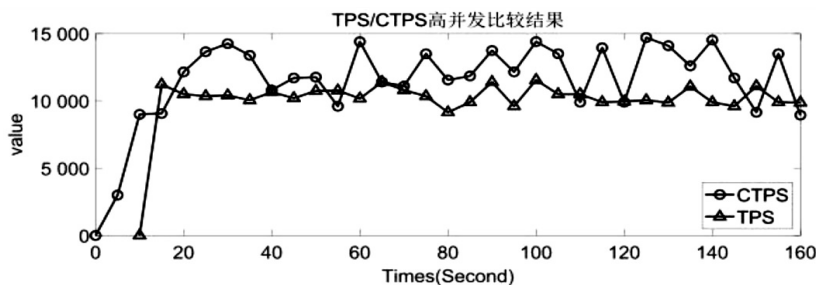


图 5 高并发压力测试

结果显示 TPS 均值 10 034, CTPS 均值 11 393, TPS 峰值 11 410, CTPS 峰值 14 542, 交易成功率 100%。

对于高并场景下的存证交易性能测试, 4 台压测机共发送 2 000 000 笔存证交易(存证数据大小 200 Bytes), 持续 5 分钟左右, 并发数为 300, 测试结果如图 6 所示。

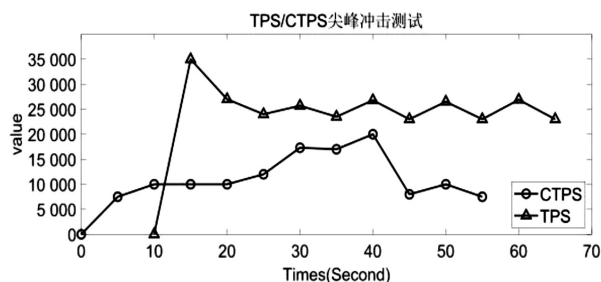


图6 存证尖峰冲击测试

测试结果: TPS 均值 23 624, CTPS 均值 10 791, TPS 峰值 34 975, CTPS 峰值 20 000, 交易成功率 100%。

对于高并发场景下的查询交易性能测试, 4 台压测机共进行 2 000 000 交易查询, 持续 5 分钟左右, 并发数 300, 测试结果如图 7 所示。

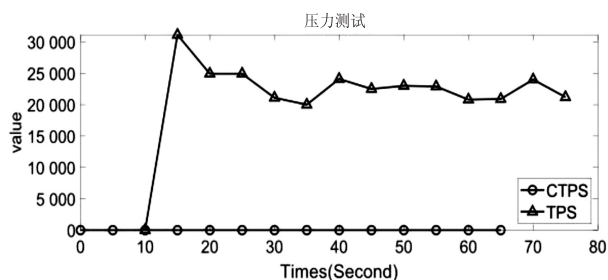


图7 单节点查询压力测试

测试结果: TPS 均值 21 389, TPS 峰值 31 127, 时间 15 时 38 分 ~ 15 时 40 分。

实验结果表明, 测试环境区块链存储 TPS 均值、查询 TPS 均值完全满足安徽省高速公路联网收费需求, 在通行数据不断增长的情况下, 可以采用增加节点的方式提升业务处理能力。

## 6 结束语

提出了基于区块链的高速公路联网收费数据共享方案, 利用区块链技术实现车辆通行数据的分布式存储, 通过链上数据库表加密技术结合智能合约技术, 实现车辆通行数据上链加密存储和自动化授权共享, 同时将数据共享过程上链存证, 利用区块链不可篡改的技术特点, 实现对数据共享过程的可追溯。该方案有利于实现车辆通行数据的跨地区、跨部门共享, 对于简化高速公路联网收费以及清分结算业务流程, 提高业务协同效率具有重要意义。实验结果表明, 该方案在

数据链上存储与多方共享方面能够满足隐私保护要求, 并且具有较高的性能, 能够满足高速公路联网收费数据共享需求。在后续的研究中, 将在数据高效共识上链以及跨链传输等方面做更加深入的研究与探索。

## 参考文献:

- [1] 中国网, 新闻中心. 交通运输部: 全国高速公路 ETC 使用率超 65.98% 收费站缓行拥堵缓解[EB/OL]. [2020-10-28]. [http://news.china.com.cn/txt/2020-10/28/content\\_76852695.htm](http://news.china.com.cn/txt/2020-10/28/content_76852695.htm).
- [2] 闫卫喜. 浅谈区块链技术在交通运输行业的应用[J]. 中国交通信息化, 2020(2): 132-134.
- [3] 王若华, 焦健, 石晋平. 一种基于超级账本的高速公路通行数据区块链[J]. 北京信息科技大学学报: 自然科学版, 2021, 36(2): 69-75.
- [4] 张利华, 蒋腾飞, 姜攀攀, 等. 基于区块链的高速铁路监测数据安全存储方案[J]. 计算机工程与设计, 2020, 41(4): 933-938.
- [5] 王秀利, 江晓舟, 李洋. 应用区块链的数据访问控制与共享模型[J]. 软件学报, 2019, 30(6): 1661-1669.
- [6] 王士成, 史述云, 文义红, 等. 基于区块链的装备数据安全共享方案研究[J]. 国防科技, 2021, 42(5): 52-57.
- [7] 张正昊, 李勇, 张振江. 可控可追责的敏感数据共享方案[J/OL]. 计算机研究与发展: 1-12 [2021-12-27]. <http://kns.cnki.net/kcms/detail/11.1777.TP.20211214.1531.002.html>.
- [8] 李燕, 马海英, 王占君. 区块链关键技术的研究进展[J]. 计算机工程与应用, 2019, 55(20): 13-23.
- [9] 张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
- [10] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
- [11] 刘懿中, 刘建伟, 张宗洋, 等. 区块链共识机制研究综述[J]. 密码学报, 2019, 6(4): 395-432.
- [12] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展[J]. 自动化学报, 2019, 45(3): 445-457.
- [13] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.
- [14] 范吉立, 李晓华, 聂铁铮, 等. 区块链系统中智能合约技术综述[J]. 计算机科学, 2019, 46(11): 1-10.
- [15] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.
- [16] 张奥, 白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报, 2020, 31(5): 1406-1434.
- [17] 王瑞锦, 唐榆程, 裴锡凯, 等. 基于轻量级同态加密和零知识证明的区块链隐私保护方案[J]. 计算机科学, 2021, 48(S2): 547-551.
- [18] 代闯闯, 栾海晶, 杨雪莹, 等. 区块链技术研究综述[J]. 计算机科学, 2021, 48(S2): 500-508.