计算机应用
Journal of Computer Applications
ISSN 1001-9081,CN 51-1307/TP

《计算机应用》网络首发论文

题目：基于区块链和零知识证明的高速公路自由流收费方法
作者：王一帆，林绍福，李云江
收稿日期：2024-01-02
网络首发日期：2024-03-22
引用格式：王一帆，林绍福，李云江．基于区块链和零知识证明的高速公路自由流收费方法[J/OL]．计算机应用．
https://link.cnki.net/urlid/51.1307.TP.20240320.1013.004

Journal of Computer Applications ISSN 1001-9081
计算机应用 CODEN JYIIDU http://www.joca.cn

doi:10.11772/j.issn.1001-9081. 2023121830

基于区块链和零知识证明的高速公路自由流收费方法

王一帆，林绍福*，李云江，
(北京工业大学 信息学部软件学院，北京 100124)
(*通信作者电子邮箱 linshaofu@bjut.edu.cn)

摘要：针对目前智慧交通中高速公路自由流收费方案里因车辆套牌导致的车辆逃费和数据集中式存储可能引起的用户隐私泄露至集中式实体的问题，提出了一种基于区块链和零知识证明的高速公路自由流收费方法，首先设计视频监控逃费检测机制确保高速公路上车辆的合规性，其次设计区块链中的智能合约将车辆位置证书以及付费数据加密存储至分布式账本中，并引入零知识证明技术在保护隐私的情况下确保支付的正确性，同时在零知识电路中设计根据车辆行驶里程收费的算法。理论分析与模拟实验表明，该方法在正常情况下实现位置隐私零知识的实际行驶里程正确收费，异常情况下能及时预警并记录至区块链上；该方法平均收费时间相较于传统人工收费方法由原来的 38 秒降低至 1.8 秒，相较于基于 5G 和电子不停车收费系统（ETC）结合的收费方法，减少了约 0.1 秒；对于相同的入站与出站口，不同路线的信息网络可信第三方信息采集点（ICP）数量重合度越低，根据行驶里程的收费越精准。

关键词：高速公路；自由流收费；隐私保护；区块链；零知识证明
中图分类号：TP391.9 **文献标志码：**A

Highway free-flow tolling method based on blockchain and zero-knowledge proof

WANG Yifan, LIN Shaofu*, LI Yunjiang
(Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China)

Abstract: In response to the issues of vehicle toll evasion caused by license plate cloning and potential user privacy leaks due to centralized data storage in the current intelligent transportation highway free-flow tolling schemes, a highway free-flow tolling method based on blockchain and zero-knowledge proof was developed. Initially, a video surveillance mechanism for toll evasion detection was designed to ensure the compliance of vehicles on highways. Subsequently, smart contracts within the blockchain were designed to encrypt and store vehicle location certificates and payment data in a distributed ledger. Zero-knowledge proof technology was introduced to ensure the correctness of payments while protecting privacy, and an algorithm for charging tolls based on the vehicle's mileage was designed within the zero-knowledge circuit. Theoretical analysis and simulation experiments demonstrated that under normal conditions, the method achieves accurate toll collection based on the actual driving mileage with zero-knowledge of location privacy, and in the event of exceptions, it can provide timely warnings and record anomalies on the blockchain. The average toll collection time has been reduced from 38 seconds to 1.8 seconds, a decrease of about 0.1 seconds compared to the methods combining 5G and Electronic Toll Collection (ETC). For the same entry and exit points, the lower the overlap in the number of Information Collection Point (ICP) on different routes, the more accurate the mileage-based tolling.

Keywords: highway; free-flow tolling; privacy protection; blockchain; zero-knowledge proof

0 引言

我国的高速公路收费从人工到自动化再到联网，收费模式随着技术的更新发展愈加多样便捷，道路使用者的满意度和便利感受随之提高。国家从政策层面积极推动公路自由流收费的发展，在《关于推动交通运输领域新型基础设施建设的指导意见》中提到，探索推进卫星定位系统与车路协同、电子不停车收费系统（Electronic the collection，ETC）等技术融合应用，研究北斗自由流收费技术。《公路“十四五”发展规划》中提出，积极探索“ETC＋北斗”开放式自由流收费等新技术的智慧应用试点。然而实体收费站的存在，尤其在车流量大的收费站点依然拥堵频发，收费站建设、运营

收稿日期: 2024-01-02; 修回日期: 2024-02-21; 录用日期:2024-02-28。
基金项目: 国家重点研发计划资助项目(2020YFF0305400)。
作者简介: 王一帆(2000—)，男，河北邯郸人，硕士研究生，CCF 会员(N2157G)，主要研究方向：区块链与数据治理、面向时空数据的隐私保护；林绍福(1967—)，男，北京人，教授，博士，CCF 会员(75651D)，主要研究方向：智慧城市时空大数据、大数据计算与智能、区块链与数据治理、物联网与感知智能；李云江(2001—)，男，江苏盐城人，硕士研究生，CCF 会员(P6605G)，主要研究方向：区块链与数据治理、面向时空数据治理的隐私保护。

管理成本仍较高，出行者在少人化、无人化收费以及无感通行方面的需求越来越迫切[1]。随着经济的发展，高速公路给人们带来了很多便利，但同时在高速公路发展中也存在着许多问题：

1.由于实体收费站的存在，收费站出口需要缴纳通行费，收费过程漫长且复杂，由于过度拥挤的车辆在收费站口，车流速度会受到很大的影响[2]。

2.由于套牌车、遮挡号码、ETC 的漏洞等问题，给稽查带来很大的影响。

3.由于现在的收费制度，无论行驶多少里程数与时间，人们都支付相同的费用，这样的收费制度并不公平。

4.中心化收费实体收集了大量的用户的个人隐私数据，并采用大数据分析和人工智能技术以获得有关其客户的宝贵知识，这将导致垄断、隐私泄露等问题。

针对高速公路自由流的收费方式，国内外已经做了许多探索与应用。中国已经在全国范围内推广了 ETC，这是一种自由流收费的形式。通过 ETC 系统，车辆不停车或短暂的降速也可完成收费，大大提高了通行效率。中国在一些地区也在试验无人收费技术。例如，通过车牌识别技术和移动支付技术，车辆无需人工干预即可完成收费。同时，政府积极推进发展自由流收费，中国交通运输部已经提出了“取消省界收费站，实现高速公路全网自由流”的目标。总的来说，我国高速公路自由流收费系统正在逐步发展和完善，未来有望实现更高的通行效率和服务质量[3]。

在美国，许多州都采用了电子收费系统。例如 E-ZPass 是美国最大的电子收费系统，覆盖了 17 个州的高速公路、桥梁和隧道。用户可以通过预付费账户支付通行费而无需停车或慢行。在悉尼，所有的收费路都使用电子收费系统，用户可以选择安装一个电子标签在车辆上，或者注册一个账户，通过车牌号码识别系统支付通行费。新加坡的电子道路定价系统（electronic road pricing，ERP）是一个先进的城市交通管理系统，它使用电子收费技术来管理城市的交通需求。ERP 系统通过收取通行费来控制车辆的数量，从而减少交通拥堵。法国的 Telepeage 系统允许驾驶员在高速公路上以正常速度行驶，而无需停车支付通行费。用户可以通过一个预付费账户支付通行费，该账户可以在线充值[4]。

国内外高速公路自由流收费系统的实施虽然取得了一定的成效，但也面临着一系列难题与挑战。首先，技术问题是一个主要的挑战，包括车辆识别的准确性、系统的稳定性和可靠性等。其次，数据隐私也是一个重要的问题，因为自由流收费系统需要收集和处理大量的个人和车辆信息，如何保证这些数据的安全和用户隐私的保护是一个全球性的挑战。此外，法规和政策问题也不能忽视，不同的国家和地区可能需要根据当地的法规和政策来调整自由流收费系统的设计和运行方式。用户接受度也是一个问题，虽然自由流收费系统可以提高交通效率，但是需要用户适应这种新的收费方式，这可能需要一段时间。对于跨国或跨地区的高速公路，如何设计和实施一个公平、有效的自由流收费方法是一个挑战。最后，基础设施的建设和改造也是一个重要的问题，一些国家和地区可能需要进行大规模的基础设施建设和改造，以适应自由流收费的需求。这些问题和挑战需要各国政府、企业和社会各方共同努力，通过技术创新、政策调整和用户教育等方式来解决。

自由流高速公路收费是近年来的现实问题与热点问题，已有学者进行了很多研究，Goutham 等[4]设计了基于 GPS 的电子收费站系统，实现了根据里程数支付但其未考虑恶意用户不主动打开 GPS 以及中心实体所涉及的隐私问题；PENG 等[2]提出使用基于北斗的高速公路收费系统，使用北斗定位与 ETC 进行收费，刘继等[5]开展基于 5G 的 ETC 无杆准自由流收费系统建设方案研究，王哲等[6]实现了基于北斗导航定位的自由流收费系统，较好地解决了高速出行过程中出现的路线二异化、高速公路收费站拥堵问题，但都忽略了安装北斗硬件的各方面成本以及隐私泄露问题；Keshav 等[7]实现了基于 GPS 和图像处理的区块链无收费站收费系统，使用摄像头与 GPS 作为双重车辆身份验证，并使用区块链进行分散支付，提升支付安全性，但并未考虑链上隐私泄露的问题；VeerasekharReddy 等[8]开发了一种使用计算机视觉技术的新型收费系统，使用摄像头捕捉收费站的过往车辆，使用自动车牌识别算法进行处理，系统再进行扣费；Sonali 等[9]根据 GPS 与智能合约实现了一种尽可能透明的方式建立自由流收费系统；Guo 等[10]基于区块链与零知识证明实现了基于区块链的基于位置的车辆服务的隐私保护支付方案，使用区块链与零知识证明基于收费站进行了收费方案的研究，但并未设计逃费以及根据里程数支付的问题，以上工作都尚未同时很好地解决现存的一系列问题。

为此，本文基于研究现状以及现实问题与挑战设计了一种基于区块链和零知识证明的高速公路自由流收费方法，本文采用高速入口监控摄像头以及高速路中的摄像头以及信息网络可信第三方信息采集点（Information Collection Point，ICP）的采集车辆位置信息，本文的主要工作如下：

1.针对高速公路自由流逃费等场景逃费情况，设计了一套综合稽查预警机制。

2.本研究采用区块链技术构建一个去中心化支付方案。在此基础上，本研究开发并部署了智能合约，自动执行付费流程。

3.为了在不泄露用户隐私的前提下验证支付的正确性，本研究引入了零知识证明技术。本研究设计了一种创新的支付验证协议，它允许用户证明其支付金额与实际行驶里程、车型相符，同时不会暴露任何额外的个人位置隐私。

本文第一节介绍了高速公路收费服务和收费证明、区块链、以及零知识证明算法的相关理论，第二节介绍了此方法的基于区块链与零知识证明的高速公路自由流收费模型、基于零知识证明的高速公路收费验证算法，第三节介绍了进行的本方法的技术实验与功能实现，第四节是小结。

1 基本原理

1.1 高速公路收费服务和收费证明相关理论

位置服务（Location-Based Services，LBS）是指在移动环境下，利用地理信息系统(Geographic Information System，GIS)、定位技术和网络通信技术，提供基于移动对象的空间位置信息的服务技术体系[11]。LBS 的基本模式包括位置获取、位置验证和信息服务三个关键步骤。典型的 LBS 应用场景包括实时人车流量监控、基于位置的访问控制、特定商户的折扣促销以及电子选举等。在实际应用中，存在着恶意用户可能伪造其位置信息以谋取个人利益的风险，这可能对 LBS 的判断和 LBS 的最终结果产生严重负面影响。为应对这一威胁，LBS 要求用户在获取服务之前能够提供关于其当前或历史位置的验证信息，这些验证信息被称为位置证明。

位置证书[12]是数字证书，用于验证用户在特定时间的位置。它包括用户的身份标识、时间信息和空间信息。从定位方式的角度来看，位置证书获取分为两种类型：基础设施依赖型和基础设施独立型。基础设施依赖型位置证明依赖于商户安装的硬件设备来收集用户的位置信息。通常，这需要结合物联网技术，例如使用 Wi-Fi 接入点（AccessPoint，AP）或低功率广域网络（Low-Power Wide-Area Network，LPWAN）等基础设施来获取位置信息。这种方法产生的位置信息通常更可靠，但管理和部署特定的硬件设备可能具有挑战性。基础设施独立型位置证明则是由用户的移动设备生成位置信息，或者通过邻近用户的协助来获取位置,一般是通过全球卫星导航系统（Global Navigation Satellite System，GNSS）来实现，其中最常用的是全球定位系统（Global Positioning System，GPS）。这种方法简单而高效，但在实际使用中可能会面临位置伪造的问题。

1.2 区块链

1.2.1 基本原理及其特点

区块链是一组通过密码学方法链接在一起的数据块,其中包含了一定时间内交易信息的哈希值。区块按时间顺序连接成链条,链中区块内容通过哈希指针串联。区块链网络由多个节点共同维护组成，节点使用公私钥来对交易信息进行签名，同时广播到区块链网络。其他节点验证交易的有效性后，达成共识将其存入新区块。新区块广播到全网后加入区块链。区块链技术涵盖多种关键技术元素，包括加密、共识机制、激励机制、分布式存储和智能合约。

从本质上来说，区块链是一种使用密码学方法确保其不可破坏和不可篡改的链式数据结构，也被称为公共账本。这个账本由一系列区块组成，每个区块通过包含前一个区块的加密哈希值，通过加密哈希值进行前后的连接。每个区块还包含时间戳、随机数、交易数据等信息，区块链的一个关键特征是其共识算法，例如工作量证明（Proof of Work，PoW）和权益证明（Proof of Stake，PoS）[13]。这些算法确保网络中的所有对等点能够达成共识，以确定哪个对等点有权将新区块添加到链中。获得记账权的对等节点随后成为“矿工”，负责打包交易并添加到区块中。一旦数据被写入区块链，就无法修改，这样就确保了数据的不可篡改，整个过程通常被称为挖矿，因为参与记账权竞争的对等节点需要解决复杂的数学问题来证明其工作或权益，从而有资格添加新区块。这种过程是区块链网络的核心，同时也是激励机制的一部分。对于公共区块链，获得记账权的矿工通常会获得代币奖励，这一机制鼓励矿工参与网络并保持其正常运行。区块链技术可以分为不同类型的网络，包括公共链、私有链、联盟链和混合链，以满足不同应用场景和需求。这些类型的区块链在访问权限、共识机制和控制权方面有所不同。本文介绍的区块链网络是私有链，提供更高的隐私性，安全性和控制性。

区块链的核心特征包括以下几个方面：

1） 分布式账本：区块链是一种分布式账本技术，数据被公平的分布在各个节点上，而不是集中在单一的中央服务器上。每个节点都包含一份完整的账本副本，这确保了数据存储的去中心化。

2） 不可篡改性：一旦数据被添加到区块链上，因其分布式账本的特性，几乎不可能被篡改。每个区块都包含前一个区块的散列值，以及时间戳，这样任何的数据修改都会在整个网络上被检测到。

3） 去中心化：区块链网络通常没有单一的中央权威，而是由多个节点一起进行维护和管理。这降低了对中心化机构的依赖，使决策更加分散。

4） 共识机制：区块链网络通过共识算法来确定数据的有效性

区块链在高速公路自由流收费研究中的解决方法是利用分布式共识、不可篡改的交易记录、智能合约和去中心化管理等原理，来确保收费方式的安全性、可信度和公正性。这些原理的结合可以为自由流收费提供更安全、高效和可信的解决方案。

1.2.2 智能合约

智能合约是以太坊应用的基石，是存储在区块链上的计算机程序，能够将传统合约转换成数字化合约。智能合约是一种自动执行的计算代码，运行在去中心化的区块链上，旨在自动执行合同条款而无需中介。这些合约具有不可篡改性和透明性，使用加密技术确保安全性，并在没有中间商的情况下自动化完成业务流程。它们适用于多个领域，从金融领域到供应链管理以及不动产交易等，为降低交易成本、提高可信度提供了潜在解决方案。一旦智能合约执行，通常是不可逆转的，从而增加了对合同的信任度。

在本文高速公路自由流收费方法中，智能合约可以作为用于实现自动化的收费和管理的解决方案。智能合约可以根

据预设的规则和条件自动执行交易和操作，同时根据设定的规则和费率，自动计算和收取用户的费用。当用户通过高速公路时，智能合约可以根据行驶距离、车型和时间等因素，自动计算出应收取的费用，并从用户的账户中扣除相应金额，可以将收费数据记录在区块链上，确保数据的完整性和不可篡改性。每笔交易和收费记录都会被永久地存储在区块链上，可以随时进行查阅和核对[14]。

智能合约的原理基于区块链技术和编程逻辑，通常使用智能合约编程语言进行编写，并在区块链上部署和执行。智能合约可以被多个参与方访问和执行，但其执行结果是公开可验证的。通过使用智能合约[15]，高速公路自由流的收费可以实现自动化的收费和管理，提高效率和减少人为错误。同时，智能合约的执行结果可以被验证和审计，增加了该收费方法的透明度和可信度。

1.3 零知识证明算法

零知识证明是一种由证明者、验证者双方交互的密码学协议，对于一个可描述的论断，证明者可通过零知识证明令验证方确信该论断正确，但除此以外验证方无法获取任何额外信息。零知识证明具有如下三条核心性质：

1)完备性：如果结论为真，证明方一定可以向验证方证明论断的正确性。

2)可靠性：如果结论为假，证明方无法说服验证方论断的真实性。

3)零知识性：除了论断的真假以外，验证方无法得知其他有效信息。

零知识证明需要建立在数学假设之上，如离散对数问题（Discrete Logarithm Problem，DLP）或指数知识（Knowledge of Exponent，KoE）等，不同的假设会对证明的安全性和计算性能产生不同的影响。例如，非交互式简洁的零知识证明（Zero Knowledge Succinct Arguments of Knowledge，ZK-SNARKs）零知识证明方法以 KoE 假设为其安全基础，证明生成的时间复杂度为$O(n\,log^{n})$，其中n表示证明约束中的门数量，而证明验证的复杂度是常数级的，通常只需要数毫秒来完成一次零知识互动，这表现出卓越的计算性能。然而，ZK-SNARKs 的一个缺点是，在该方案中，需要提前进行一次可信设置以生成证明方和验证者共享的公共参数（Common Reference String，CRS），但这个 CRS 只适用于一类证明，且如果攻击者获取了 CRS 生成时使用的随机值τ，就有可能生成虚假证明，存在一定的安全风险。

与之不同，Bulletproofs 零知识证明方法以离散对数问题为其安全基础，证明生成和验证的时间复杂度均为$O(n)$，但在电路门数量较高的情况下性能表现不佳。然而，该方案的优势在于无需提前的可信设置，使证明生成更加灵活。另一方面，零知识透明可扩展知识论证（Zero-Knowledge Succinct Transparent Argument of Knowledge，ZK-STARKs）采用抗碰撞哈希函数（Collision Resistant Hash Functions，CRHF）作为其安全基础，尽管证明生成的时间复杂度达到了$O(n\,log^{n})$，但远超过上述两种方法，表现出较差的算法性能。然而，ZK-STARKs 不需要可信设置，并且被证明可以抵御量子攻击。

综上所述，不同的零知识证明方法基于不同的数学假设和安全性基础，具有不同的性能特点和安全风险，选择合适的方法取决于具体的应用需求和威胁模型。算法具体参数比较如表 1 所示。

表 1 不同零知识证明算法的性能参数

Tab. 1 Performance parameters of different zero-knowledge proof algorithms

证明方法	证明生成复杂度	证明验证复杂度	证明大小	安全假设	可信设置
ZK-SNARKs	$O(n\ \log\ n)$	$O(1)$	$O(1)$	KoE	需要
Bulletproofs	$O(n)$	$O(n)$	$O(\log\ n)$	DLP	不需要
Plonk	$O(\log\ n)$	$O(1)$	$O(1)$	DLP	需要
DARK	$O(1)$	$O(\log\ n)$	$O(\log\ n)$	DDH	不需要
Groth’16	$O(\log\ n)$	$O(1)$	$O(1)$	LWE	需要
ZK-STARKs	$O(n\ \log_2\ n)$	$O(\log_2\ n)$	$O(\log_2\ n)$	CRHF	不需要

零知识证明可以作为一种解决办法，用于确保用户隐私的同时验证其支付费用的资格。零知识证明是一种密码学协议，允许证明者向验证者证明某个陈述的真实性，而不泄露具体信息。在该方法中，用户可以使用零知识证明向收费节点证明其具备支付费用的资格，而无需透露身份和行驶路径。这种解决办法保护用户隐私，确保收费方的安全性和可信度。零知识证明的安全性建立在密码学基础上，防止伪造和欺骗，并且证明过程是可验证的，任何人都可以对证明进行验证，确保其真实性和可信度。零知识证明在高速公路[14]自由流收费中的应用提供了一种保护用户隐私和验证支付资格的解决方案。

在研究高速公路自由流收费方法时，结合零知识证明和区块链技术具有重要的必要性。区块链是一种分布式数据库，具有去中心化、共同监管、防篡改等特点。但区块链的去中心化和高透明度导致交易者隐私数据的泄露，交易者隐私信息的安全性得不到保障。因此，区块链隐私保护问题也是区块链数据安全研究的重点和难点。零知识证明可以实现车辆通过收费站时无需透露具体身份和行驶路径的情况下完成收费验证，保护用户隐私。区块链技术可以提供去中心化的数据存储和不可篡改的交易记录，所有的收费交易都会被公开记录在区块链上，任何人都可以查看和验证。这种特性使得收费的过程更加公平和公正，确保收费数据的安全性和可信度。区块链技术可以自动化处理收费交易，无需人工干预，大大提高了收费的效率。同时，零知识证明技术也可以自动化处理隐私保护，无需车主手动操作。通过结合这两种技术[16]，可以建立一个安全、隐私保护且可信的自由流收费方法，为用户和监管机构提供更好的服务和保障。

2 方法

2.1 基于区块链与零知识证明的高速公路自由流收费模型

2.1.1 基于区块链与零知识证明的高速公路自由流收费模型总体架构

在基于区块链与零知识证明的高速公路自由流收费模型总体架构中，区块链上的节点分为视频监控节点、车辆用户节点、高速公路收费节点、区块链平台如图 1 所示：

视频监控节点在总体架构模型中，首先进行套牌车检测，于链下在全国车牌检测数据库以及区域车牌检测数据库和时空矛盾检测数据库依次进行检测，当都通过检测后进入高速公路零知识证明收费阶段，否则异常预警并上链存储记录异常的信息。在高速公路零知识证明收费阶段，针对车辆用户节点视频监控节点负责向车辆发送入站出站信息 S_{in} 和 S_{out}、车型类别 Ty、以及可作为 ICP 并发送路途中间的位置证书(Location Certificate，LC)；针对区块链平台，视频监控节点同时将车辆加密证书(Encrypted Location Certificate，ELC)、S_{in} 和 S_{out} 以及个人标识上传至区块链上进行存储。

车辆用户节点进入高速公路时，收到视频监控节点信息同时车辆调用智能合约发起预付款向其发送F'的金额，出站时收到视频监控节点信息后整合路途中收到的付费相关信息结合入站出站信息以及路中的信息网络可信第三方信息采集点（Information Collection Point，ICP），同时查询链上自己的证书以及相应的哈希加密后的信息，作为零知识电路的私密输入与公共输入，最终得到付费零知识的证明π以及费用 F 后上链进行存储。

区块链平台负责记录明文异常信息、加密位置证书以及其他加密付费信息，通过区块链可追溯以及不可篡改特性同时利用智能合约保证可信的付费以及零知识的验证过程。

高速公路收费节点根据区块链智能合约付费验证结果进行收费同时针对区块链上记录的逃费情况进行稽查。

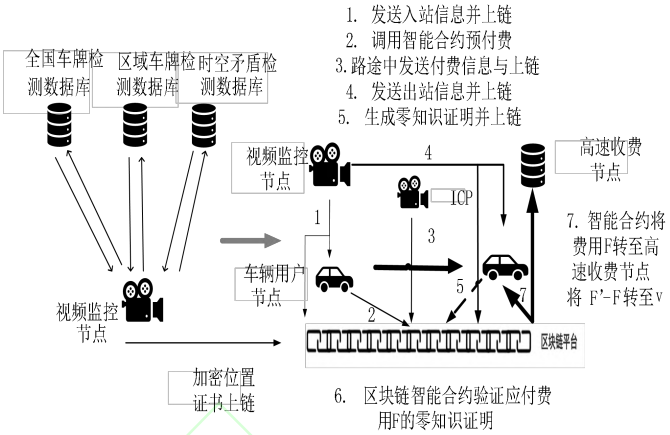

图 1 基于区块链的零知识证明高速公路自由流收费总体架构模型

Fig. 1 Blockchain-based zero-knowledge proof highway free-flow toll overall architecture model

在套牌车检查模块中如图 2 所示，以海南高速公路自由流收费为例，视频监控节点检测到车辆信息后可向全国车牌检测数据库查询，证明目前的车辆的车牌是存在的。由于海南的地理特点，进入海南的车辆都有信息备份，此时验证是否在海南区域数据库登记过，若不通过则证明是套牌车。若通过但在同时或不久存在时空矛盾情况，即相同的车牌在距离较远处出现则证明是套牌车。

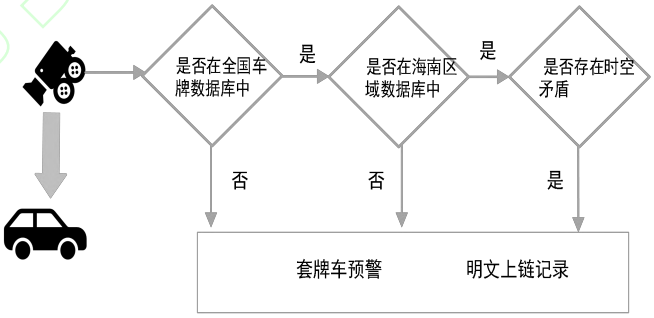

图 2 套牌车检测模块

Fig. 2 Counterfeit license plate vehicle detection module

2.1.2 基于区块链与零知识证明的高速公路自由流收费实现过程

在零知识证明的通用框架中，通常包括证明者、验证者、见证者三种角色，协助完成隐私保护的证明过程，零知识证明的证明关键的参数分为内置电路中与外部输入[17]两种方式，在本收费方法中，通过内置与证明相关的关键数据以及特殊电路算法的设计实现隐私保护的高速公路根据里程自由流收费。在基于区块链与零知识证明的收费过程中如图 3 所示，由于视频监控节点的监控功能所具备的主动性，证明者无需像传统零知识证明交互机制中的证明者主动向见证者申请寻求生成证明所需参数。

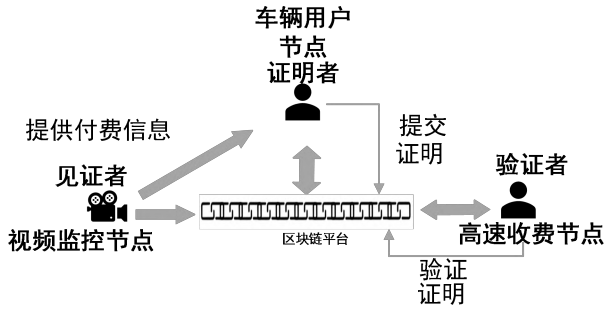

图 3 基于区块链与零知识证明的高速公路自由流收费验证模型主体单元关系图

Fig. 3 Main Unit Relationship Diagram of High Speed Free Flow Toll Verification Model Based on Blockchain and Zero Knowledge Proof

视频节点作为见证者，当监控到车辆用户节点进入高速入站口时，向其发送相应付费信息，同时路途中间的视频监控节点同样可作为 ICP 传输收费验证参数并存储至链上。由于内置电路的参数，故不需要验证者与证明者进行通信发送约束，证明者从见证者与区块链收集到收费参数后直接构造付费证明并上传至区块链上。验证者调用智能合约进行零知识的收费验证。在此过程中，总共减少两次交互，效率也因此提高。

零知识付费证明协议流程由两部分组成，分别是收集参数预支付和费用验证协议。其中，收集参数预支付协议主要用于规定车辆如何与视频监控节点交互，进入高速路请求签发 *LC*，并规定视频监控节点上传相应信息；费用验证协议主要用于规定车辆如何产生应交费用 *F* 的零知识证明以及高速公路收费节点如何验证费用的合法性。协议流程如图 4 所示。收集参数预支付阶段，视频监控节点监控到车辆后向其发送入站信息以及车型信息。车辆在路途中向 ICP 视频监控节点请求签发 *LC*，视频监控节点在收到请求后，验证请求的有效性，验证通过则返回 *LC* 参数；同时视频监控节点结合用户请求中包含的信息，生成 *ELC* 并将指纹广播至整个区块链网络，等待网络中其他视频监控节点挖矿保存指纹。而车辆在收到视频监控节点返回的 *LC* 参数后，生成 *LC* 保存至本地，留待请求付费时使用。费用验证阶段车辆使用本地保存的 *LC* 与链上的信息生成应交费用的零知识证明。然后以远程通信方式将应交费用 *F* 的零知识证明发送给视频监控节点，请求付费。高速公路收费节点在收到应交费用 *F* 的零知识证明后，调用智能合约验证应交费用 *F* 的零知识证明的有效性，验证通过则返回验证结果；同时，高速公路收费节点生成支付费用或退回费用 *F-F'* 并请求将服务记录保存至区块链网络。

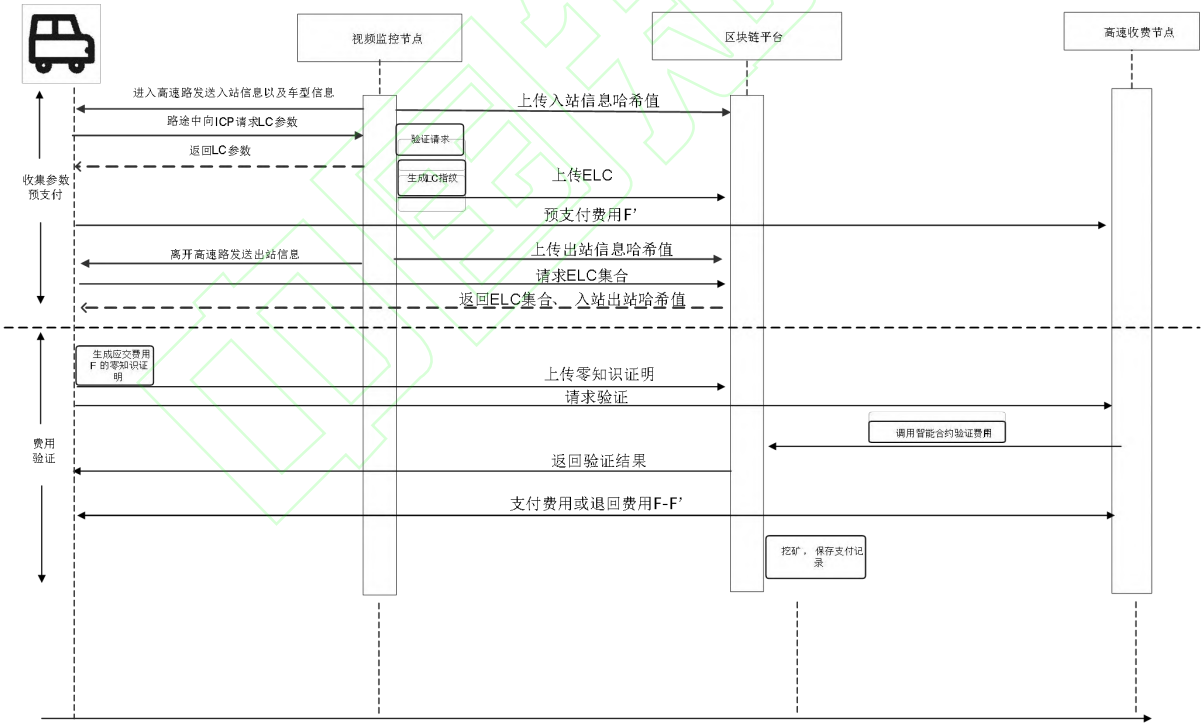

图 4 零知识付费证明协议流程

Fig. 4 Zero-knowledge location proof protocol process

2.1.3 基于智能合约的高速公路收费验证算法

1) 合法车辆证书上传合约

合法车辆证书上传合约用于上传和验证合法车辆证书的有效性。这样的合约可以用于确保车辆证书的真实性和有效性，以便在车辆交易、保险索赔、车辆维修等方面提供可靠的证明。定义车辆证书结构 VehicleCertificate，结构信息包含证书类型，证书数据，证书日期，证书上传者。智能合约中的 uploadVehicleCertificate 会将证书信息上传并存储在区块链上，以供将来的查询和验证。合法车辆证书上传合约可

以提供查询和验证服务，允许其他相关方在需要时查询车辆证书的有效性，以确保交易的合法性。

2) 收费验证智能合约

a) 分发公私密钥功能体

分发公私密钥智能合约（KeyDistributionContract）主要是创建一个安全的方式来生成、存储和分发密钥对。首先定义公钥和私钥变量，PublicKeyDistributed 事件用于记录公钥的分发，随机生成私钥或从可信的随机源中获取，getPublicKey 函数用于获取公钥，然后接下来 distributePublicKey 函数用于分发公钥给其他地址，signdata 函数使用私钥对数据进行签名。

b) 位置信息上链功能体

初始化合约状态，便于在一个用户付费完之后合约状态的变更。其中 N 为加密位置证书的数量，加密位置证书中包含位置信息、车辆类型信息，*userHash* 为用户个人 ID 的哈希标识，便于后续零知识证明电路中验证链上客户端存储数据的一致性，H_{in} 与 H_{out} 为入站与出站口的哈希值。

Function：UploadCertificates//位置信息上链

struct LocationCertificate

userHash; // 用户的唯一哈希标识符

spacetimeHash; //结合地理位置和时间戳以及车辆类型哈希值

H_{in};

H_{out};

For (i = 0; i <N; i++) // 存储每个位置证书

push(LocationCertificate(*userHash*, *_spacetimeHashes*[i]));

c) 位置信息查询功能体

userHash 为用户个人 id 的哈希标识，根据个人标识返回位置证书。

Function：GetCertificates//位置信息查询

return userCertificates[*userHash*];

d) 初始化功能体

初始化合约状态，*state* 用于记录合约的状态，便于在一个用户付费完之后合约状态的变更。

Function：Init//初始化

state=INIT;

e) 预付费功能体

当视频监控节点检测到车辆进入后，向区块链上传其位置证书之后向车辆用户节点发送参数，此时车辆用户节点应向高速公路收费节点 Charger 预付费用 F’并转至智能合约，此 F’按照入站后的所有道路平均里程数费用计算得出。

Function：Pre-fee//检测到车辆进入进行预付费

("Pre-fee",F’)→ contract;

f) 零知识收费验证功能体

当车辆用户节点提交证明后，智能合约验证证明π，通过后进入退费结算阶段。

Function：Verify//验证收费

Assert *state* = DEPOSIT:

state = UPLOAD;

If Verify (π) =1:

state = TRUE;

Refund;

Else:

state = FALSE;

Refund;

g) 收费结算功能体

当证明通过后收取应付费用 F，同时退去相应费用。若证明无法通过，则扣去预付款费用 F’。

Function：Refund//费用结算

If *state* = TRUE:

Transfer F→ Charger;

Transfer (F’-F)→V;

Else:

Transfer F’→ Charger;

state = FINISHED;

2.2 基于零知识证明的高速公路收费验证算法

2.2.1 基于零知识证明的高速公路收费算法

零知识证明实际上是一种多方参与的协议，由于智能合约在位置验证算法中的应用，验证者可以对证明者的身份、时间、位置等多维度信息进行验证，而不侵害证明者的个人隐私。本模型中，高速公路收费节点即为验证者，车辆用户节点为证明者，而视频监控节点以及 ICP 作为见证者，见证其位置信息以及确认其轨迹里程数。需要特别强调的是，本研究采用 ZK-SNARKs 构建零知识位置证明算法。与大多数零知识证明方法一样，ZK-SNARKs 允许证明计算语句，但无法直接应用于计算问题。因此，必须使用算术电路来对计算语句进行建模。然而，算术电路的算法表现更为复杂，例如，无法简单地表示条件语句等。为了确保文章的可读性，本文的伪代码仍采用常见的编码表现形式。

由于零知识证明的特殊性，每个算法输入都分为两部分：验证者提供的公共输入和证明者提供的私密输入。值得强调的是，证明在本地生成，不会将私密输入透露给任何人，发送至验证者处的证明也不包含任何证明者的隐私信息。

1)信息一致性验证

本算法对视频节点上传的其位置信息证书是否与区块链上的加密证书保持一致以及其他信息一致性进行判断，公开输入为链上存储的加密证书 *ELC*、入站出站信息哈希值 H_{in} 和 H_{out}，其中：

$$ELC = \left\langle PubKey_P, Hash\left(PubKey_s, PC_p, Ty\right)\right\rangle$$

私密输入为车辆用户节点公钥 $PubKey_P$、记录本条位置证书的视频监控节点公钥 $PubKey_s$、车辆接收到的时空信息 PC_p、车辆的类型 Ty、ICP 的数量 N 和入站出站信息 S_{in} 和 S_{out}，输出结果为 True 时则车辆用户节点持有真实的私钥，同时说

明车辆用户节点接受的信息与链上保持一致，即车辆用户节点持有真实的位置信息证书。具体算法和过程如下所示。

算法 1: IsConsistency ()

公共输入:ELC,H_{in},H_{out},H_N

私密输入: $PubKey_P,PubKey_s,PC_p,Ty,N,S_{in},S_{out}$

输出: True/False

$H1$ = Hash($PubKey_s$,PC_p)

$H2$ =Hash(S_{in},S_{out});

$H3$ =Hash(N);

if((<$PubKey_P$, $H1$>,$H2$,$H3$) == (ELC,< H_{in},H_{out} >, H_N))

return True;

else

return False;

2)车型费率验证

本算法对视频节点上传的车型计算其费率，私密输入为车型 Ty，输出为费率 $Tyfee$，根据一类客车 Ty1，二类客车 Ty2，三类客车 Ty3，四类客车 Ty4 匹配费率。

算法 2: Typefee()

公共输入:

私密输入: Ty

输出: $Tyfee$

if (Ty==Ty1):

$Tyfee$=Ty1fee;

else if（Ty==Ty2）:

$Tyfee$=Ty2fee;

else if（Ty==Ty3）:

$Tyfee$=Ty3fee;

else $Tyfee$=Ty4fee

return $Tyfee$;

3)距离验证

本算法私密输入参数为入站 S_{in}，出站 S_{out}，收到的 ICP 数 N, 公共输入参数为入站与出站信息哈希值 H_{in} 和 H_{out}，输出信息为行驶里程 Dis 与入站出站联合哈希值存入 out 数组中。为方便计算，在此算法中 S_{in} 和 S_{out} 都抽象为每个入站口所代表的数值，而在 Dis[]数组中存储着两者相乘的乘积。匹配入站口与出站口后在符合匹配的 m 条道路中，每条道路有着不同 ICP 数，distance[i][N]代表匹配的 S_{in} 和 S_{out} 出入站口中 ICP 数为 N 的那条路的里程数，编写电路时某些语言语法不可以使用二维数组进行输入，故可以转化为 $roadnum$ 个数量的一维数组实现，而一维数组的匹配可通过条件语句进行匹配。其中 $roadnum$ 为入站口出站口的自由组合的数量，例如若有 4 个站口，则有 $roadnum$=$C_4^2=6$。

算法 3: Distance（）

公共输入:

私密输入: S_{in},S_{out},N

输出: out

for(i=0,i<$roadnum$,i++)

if(S_{in}*S_{out}==Dis[i])break;

out=distance[i][N];

return out;

4)费用计算

本算法综合以上算法，其公共输入为入站口与出站口哈希 H_{in} 和 H_{out}、加密证书 ELC 的集合，ICP 数量 N 的哈希值 H_N，计算出应付费用 out[0]，入站出站哈希值 out[1]，以及总的约束是否通过 out[2]。

算法 4: Computefee（）

公共输入: ELC[N],H_{in},H_{out},H_N

私密输入: S_{in},S_{out},N,LC[N],$PubKey_P$,Ty

输出: out[2]

verify=True；

for (i = 0; i < N; i ++)

if(IsConsistency(ECL[i],H_{in},H_{out},H_N,$PubKey_P$,LC[i].$PubKey_s$, LC[i].PC_p,Ty, S_{in},S_{out},N)!=1)

verify=False;

if(verify)

out[0]=Typefee(Ty)*Distance(S_{in},S_{out},N);

out[1]=True;

else out[1]=False;

return out;

2.3 证明计算

在完成零知识证明算法的设计后，需要进行“验证算法多项式转化”以及“可信设置”两项准备工作，在准备完成后进行多项式承诺生成证明，证明者发送证明给验证者进行验证。

上述算法无法直接用于证明的生成，根据 Schwatz-Zippel 定理[18]可知，多项式上任意点的计算结果有极大概率是其唯一身份的表示，可以显著增加验证过程的简洁性与可靠性，因此本文需将电路转化为变量多项式。本研究将使用 BN-254, BLS12-381 椭圆曲线构建生成器，可信设置的关键一步是创建结构化参考字符串（Structured Reference String，SRS），参考字符串是由随机生成的秘密数字参数化的椭圆曲线点列表 s，任何电路只要有足够的元件就可以使用任何类似的 SRS，电路 n 门需要一个 SRS 至少 n+5 要素如下：

SRS:

$$1\cdot G1, s\cdot G1, s^2\cdot G1\cdots, s^{n+2}\cdot G1$$
$$1\cdot G2, s\cdot G2$$

根据电路可以将每个门的约束写成方程，在 PLONK 中，这些方程的设置如下。每个方程都具有以下形式（认为：L=左，R=右，O=输出，M=乘法，C=常数）：

$$\left(Q_{Li}\right)a_i+\left(Q_{Ri}\right)b_i+\left(Q_{Li}\right)c_i+\left(Q_{Mi}\right)a_ib_i+Q_{Ci}=0 \quad (1)$$

然后将这组方程转换为单个多项式方程:

$$\begin{aligned}&Q_L(x)a(x)+Q_R(x)b(x)+Q_O(x)c(x)\\&+Q_M(x)a(x)b(x)+Q_C(x)=0\end{aligned} \quad (2)$$

之后生成多项式的承诺，通过 SRS，乘以多项式的系数，最终可以得到多项式的承诺，验证者发送随机γ，证明者计算多项式承诺证明：

$$h(x)=\sum_{i=1}^{t}\gamma^{i-1}\frac{f_i(x)-f_i(z)}{x-z} \tag{3}$$

证明者将承诺发送给验证者，验证者构造 H(x)多项式，并得出与多项式相关的 SRS 的关联点值，然后验证者验证多项式的值是否等于承诺值验证者计算 F_v 和 V_v，其中 cm_i 为多项式承诺，z_i 为多项式值，s_i 为多项式结果：

$$F_v=\sum_{i=1}^{t}\gamma^i\cdot cm_i \quad V_v=\sum_{i=1}^{t}\gamma^i\cdot s_i \tag{4}$$

验证者通过椭圆曲线配对函数验证函数多项式承诺值与多项式值：

$$e(F-v,[1]_2)\cdot e(-W,[x-z]_2)=1 \tag{5}$$

验证者通过 H（x）获取证明者的知识，通过 SRS 的设置，验证者不会泄露任何有关多项式的信息。

2.3.1 基于零知识证明的高速公路收费验证算法安全风险分析

为防止证明者的隐私遭到泄露，本算法主要通过 Kate 承诺与安全多方计算确保 SRS、费用证明的生成过程中的安全性。

1)本文使用的零知识证明结构为 PLONK ZK-SNARKs，因此验证算法的安全性基于椭圆曲线配对的 Kate 承诺，在 Kate 承诺方案中，假设 P(*fee*)是对多项式 P(X)的承诺，攻击者能否在不知道秘密 *fee* 的情况下找到 $Q(fee)=P(fee)$ 且 $Q(X)\neq P(X)$，由于攻击者不知道 *fee*，其只能构造 $Q(X)-P(X)=0$ 的方程求解，众所周知，任何非常数次多项式最多可以有 n 个零点，因此获取 *fee* 的概率极其小，因为 n 远远小于椭圆曲线的阶数 p，假设使用 $n=2^{28},p\approx 2^{256}$，其概率为 $\frac{2^{28}}{2^{256}}\approx 2*10^{-69}$，这是一个非常低的可以忽略的概率，因此该费用验证方案具有足够的安全性。

此外，证明的安全性也依赖于椭圆曲线的安全性，算法采用了 110 位安全级别的 BN128 曲线，即攻击者需要进行 2110 次操作才能攻破，兼顾了证明生成性能与可靠性[19]。

2) 初始的可信设置采用安全多方计算（Multiparty Computation，MPC）实现，对于一个秘密 *fee*，采用安全多方计算使用一组计算机来创建群元素，其中没有任何单一计算机能知道秘密 *fee*，所有计算机都不诚信才会泄露 *fee*。因此算法选择安全多方计算对 ZK-SNARKs 的 SRS 第一阶段生成提供安全可靠的电路参数，该过程随机熵源来自于环境数据（天气、地震活动等）、天然放射物体最新值等难以预料的数值，且该过程只要任何一个参与方能诚实参与，那么最终得到的 SRS 就是可信的。

3 实验

3.1 实验环境

本研究通过 Snarkjs 实现了提出的方案，具有可移植性强、证明实现便捷高效等优点，并使用了 Circom 实现了零知识证明电路，它是一种专门用于编写算术电路的语言。在这之后，本文使用 Solidity 语言开发零知识高速公路中费用证明的验证合约，并采取 Truffle 平台测试方案，这是一个在以太坊进行 DAPP 开发的环境与测试框架。最终，将验证合约部署在私有区块链 Ganache 进行测试。实验环境如下：主机型号 LENOVO Legion R9000X、AMD Ryzen 7 6800H with Radeon Graphics@3.20 GHz。此外，测试数据来自于模拟数据。

3.2 费用验证实验过程

如图 5 所示，其中“a,b,c,d”分别为站点名称，“1,2,3,4”分别为站点编号，其中黑色圈为中间的视频 ICP 节点。

如图 6 和图 7 所示为电路编译过程，依据上述零知识证明算法的设计使用 circom 于 zkrepl 平台中进行编译，其编译时间为 1.3s，其中有 4 个公开输入，5 个私密输入，1 个输出，其中 S_in 与 S_out 别是入站与出站口的编号，H_in 与 H_out 为入站出站编号的哈希值，Pubk 为公钥，*ELC* 为证书，pC 为位置编码的十进制表示，N 为 2 个 ICP 数，ty 为第二类车型，在 LOG 中算出的 fee 是 100 元，行驶里程数是 50 公里即图示中 a 到 b 中 2 个 ICP 的路段，假设第二类客车每公里 2 元，结果正确。本研究进行了 100 次的证明生成实验，如图 8 所示统计证明生成的平均时间为 1.5092 秒。

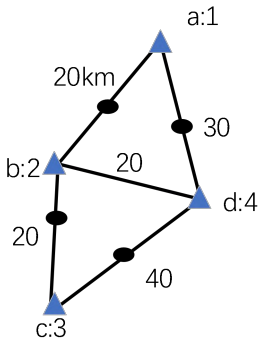

图 5 高速站点图

Fig. 5 high-speed station map

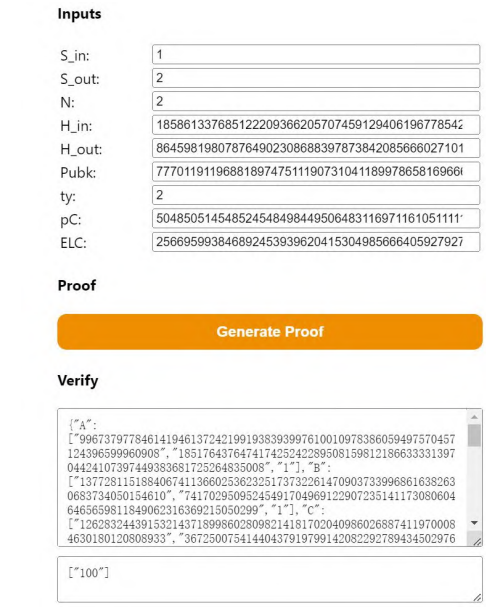

图 6 证明验证界面

Fig. 6 Proof verification interface

图 7 circom 电路编译

Fig. 7 circom circuit compilation

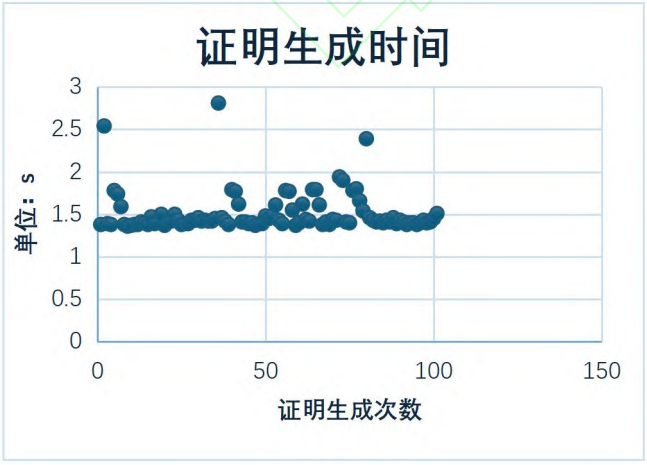

图 8 证明生成时间

Fig. 8 Proof generation time

如图 6 为证明生成过程，其中 Verify 中的内容为生成的证明，图 9 为通过验证的验证结果。

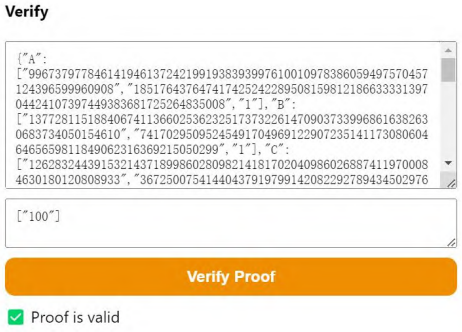

图 9 验证结果

Fig. 9 Validation results

本实验对基于区块链的零知识费用验证合约进行了 1000 轮调用测试。理论上，合约的验证效率主要受到配对函数的影响，在区块链网络未遭受重大网络攻击时，能够保证毫秒级的响应时间。如图 10 所示，验证合约的调用效率呈现出一定波动，生成时间在 3.9 至 12 毫秒的区间内波动，这是由于网络环境不稳定等原因引起的。测试结果表明，合约调用的平均时长为 5.156 毫秒，这证实了该合约能够满足验证者在高速公路收费场景中对费用信息的需求。

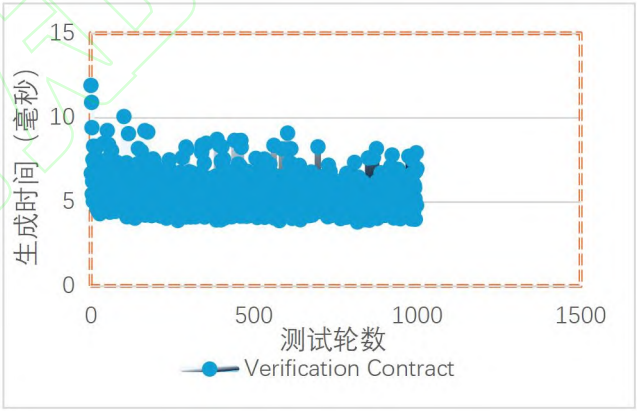

图 10零知识费用证明合约调用测试

Fig. 10 Zero-knowledge fee proof contract call test

在此方法中，收费时间的计算包括合约调用时长约 0.005156 秒、证明生成时间 1.5092 秒、网络传输延迟平均 0.3 秒，收费平均时长为 1.8 秒，通过查阅文献资料[5,10,20]收集图中收费方式的收费时间数据进行进行实验对比分析，最终如图 11 所示，与传统人工收费方式相比，平均 38 秒的收费时间在本研究方法中减少到了 1.8 秒，收费效率提升了约 95 个百分点。与结合 5G 和 ETC 的收费方法相比，此方法的收费时间减少 0.1 秒，收费效率表现出了约 5 个百分点的提升，相比于同样使用零知识证明方法的 ZK-GSIGPROOF，收费时间减少了 2.5 秒，提升约 58 个百分点。

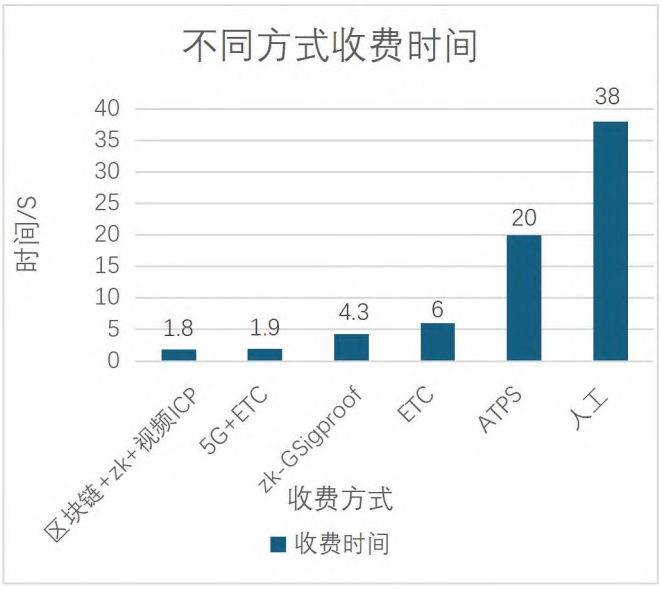

图 11不同方式的收费时间

Fig. 11 Charging time for different methods

3.3 区块链实验过程

实验以以太坊开源平台 Ganache 作为底层开发平台，使用 Solidity 作为智能合约编程语言，通过将合约部署至私有区块链测试网络进行验证，本文主要以 PlonkVerifier 合约的部署等过程为例，具体实验步骤如下所示：

步骤 1：合约部署模块

合约部署是将智能合约在区块链或智能合约平台上创建和激活的过程。这包括选择合适的合约平台，编写合约代码，将其编译成字节码，上传到区块链网络并支付 gas 费用以部署合约。该 PlonkVerifier 合约是在 VScode 使用 Solidity 编写合约代码，以以太坊开源平台 Ganache 作为底层开发平台，将合约部署至私有区块链测试网络进行验证。在部署前，通常建议进行测试以确保功能和逻辑无误，随后可以通过 Ganache 或其他用户界面与合约进行交互和管理。安全性和成本考虑至关重要，因此在部署之前需要仔细审查合约代码，并了解所选平台的规则和最佳实践。图 12 表示了合约部署的过程。

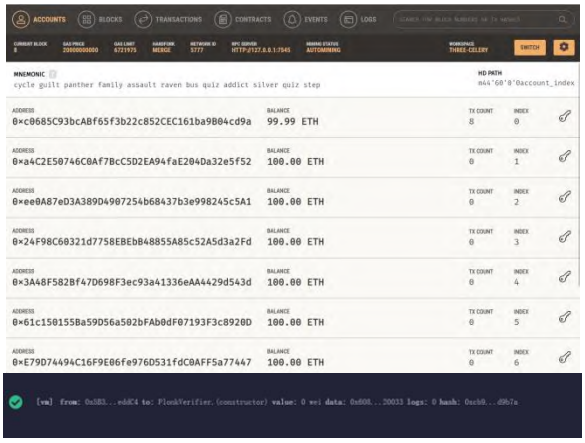

图 12合约部署过程

Fig. 12 Contract deployment process

步骤 2：合约调用模块

合约部署后，与合约相关的另一个重要方面是合约调用。一旦智能合约成功部署到区块链或智能合约平台上，其他用户或智能合约可以与之交互，执行合约中定义的功能和逻辑。用户或其他智能合约可以通过事务或函数调用来与已部署的合约互动。事务通常用于触发合约中的状态变化，而函数调用用于查询数据或执行合约中的某些操作。事务是一种用于改变区块链上数据状态的操作。用户可以发送事务来执行合约中定义的功能，这些事务可能包括向合约发送数字资产、修改合约状态或执行其他操作。事务通常需要支付一定的 gas 费用，以覆盖网络上的计算和存储成本。图 13 和图 14 分别表示了合约调用的过程和结果。

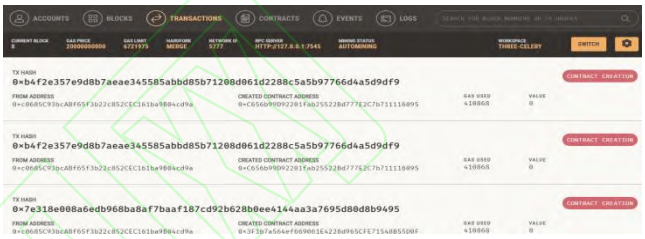

图 13合约调用过程

Fig. 13 Contract call process

图 14合约调用结果

Fig. 14 Contract call result

步骤 3：合约交易模块

根据前面合约部署，合约调用两个步骤的完成，在以太坊开源平台 Ganache 会形成以 BLOCKS 模块，上面记录了合约交易的相关情况。图 15 表示了 BLOCKS 模块上合约交易的记录结果。

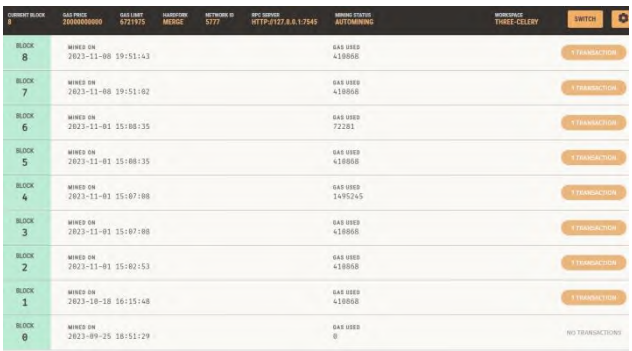

图 15合约交易记录结果

Fig. 15 Contract transaction record results

4 结语

本研究描述了一种基于区块链和零知识证明的高速公路自由流收费方法，首先通过检测套牌车模块保证高速公路上车辆的合规性，采用区块链技术实现的去中心化机制将改变传统的中心化收费体系，同时使用零知识证明的技术意味着用户可以在无需透露身份信息的情况下进行支付，从而更好地保护隐私。通过本研究，也展伸一些相关改进，该方案中逃费检测模块有望运用到零知识证明，预付费方面需要选择一个合适的预付款的费用，在获取车辆用户的位置信息定位方面可以融合北斗以及其他的定位方式，以免极端情况监控节点无法获取位置信息的发生。总的来说，基于区块链和零知识证明的高速公路自由流方法具有能在多个领域带来重大变革的潜力，在提高高速公路费用支付效率的同时能保护用户隐私。

参考文献

[1] 孙婧.自由流收费向往的未来[J].中国交通信息化,2023,16(08):18-22.(SUN J. Free flow tolling, the longing for the future [J]. China Transportation Informatization, 2023,16(08):18-22.)

[2] PENG X, DI Z, MING G. Freeway free-flow payment system based on beidou[C]// Proceedings of the 19th International Computer Conference on Wavelet Active Media Technology and Information Processing. Piscataway:IEEE, 2022: 1-5.

[3] 门小骅,柴洪峰,才华,等.基于定位技术的自由流收费系统研究[J].交通企业管理,2021,36(05):83-85. (MEN X H, CHAI H F, CAI H, et al . Research on free flow toll collection system based on positioning technology [J]. Transportation Enterprise Management, 2021, 36(05): 83-85.)

[4] GOUTHAM K, GOWTHAM M. GPS Based E-Toll Gate collection System[C]// Proceedings of the 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies. Piscataway:IEEE, 2023: 1-6.

[5] 刘继,郭晓春,周洁,等.基于 5G 的 ETC 无杆准自由流收费系统[J].中国交通信息化,2023,01(06):68-71. (LIU J, GUO X C, ZHOU J, et al. ETC roadless quasi-free flow tolling system based on 5G [J]. China Transportation Informatization, 2023,01(06):68-71.)

[6] 王哲,于静,王聘.基于北斗卫星定位的自由流收费系统[J].中国交通信息化,2022,32(11):104-105. (WANG Z, YU J, WANG P. Free-flow tolling system based on Beidou satellite positioning [J]. China Transportation Informatization, 2022,32(11):104-105.)

[7] THOSAR K, SINGH H, CHATTERJEE S, et al.Blockchain-based booth-less tolling system using gps and image processing[C]// Proceedings of the IEEE World AI IoT Congress. Piscataway:IEEE, 2023: 0380-0383.

[8] VEERASEKHARREDDY B, THATHA V N, MAANASA A, et al. An anpr-based automatic toll tax collection system using camera[C]// Proceedings of the 3rd International Conference on Pervasive Computing and Social Networking. Piscataway:IEEE, 2023: 133-140.

[9] PATIL S, KUKARNIL M, DESALE S, et al. Smart toll booth system using smart contract[C]// Proceedings of the 2023 IEEE 8th International Conference for Convergence in Technology (I2CT). Piscataway:IEEE, 2023: 1-6.

[10] GUO Y, WAN Z, CUI H, et al. Vehicloak: a blockchain-enabled privacy-preserving payment scheme for location-based vehicular services[J]. IEEE Transactions on Mobile Computing, 2023,22(11): 6830-6842.

[11] 柳林,张继贤,唐新明,等.LBS 体系结构及关键技术的研究[J].测绘科学,2007,32(5):144-146.(LIU L, ZHANG J X, TANG X M, et al. Research on LBS architecture and key technologies[J]. Surveying and Mapping Science, 2007, 32(5): 144-146.)

[12] GAMBS S, KILLIJIAN M O, Roy M, et al. PROPS: a privacy-preserving location proof system[C]// Proceedings of the 2014 IEEE 33rd International Symposium on Reliable Distributed Systems. Piscataway:IEEE, 2014: 1-10.

[13] 吴梦宇,朱国胜,吴善超.基于工作量证明和权益证明改进的区块链共识机制[J].计算机应用,2020,40(08):2274-2278. (WU M Y, ZHU G S, WU S C. Improved blockchain consensus mechanism based on workload proof and equity proof [J]. Computer Applications, 2020, 40(08):2274-2278.)

[14] 王勇,陈莉杰,钟美玲.基于零知识证明的区块链方案研究进展[J].信息网络安全,2022,22(12):47-56.(WANG Y, CHEN L J, ZHONG M L. Research progress on blockchain solutions based on zero-knowledge proof [J]. Information Network Security, 2022, 22(12): 47-56.)

[15] 宋杰,刘晓媛,孙树垚.关于区块链技术在高速公路收费领域应用的研究与思考[C]//第十七届中国智能交通年会.北京:机械工业出版社,2022:68. (SONG J, LIU X Y, SUN S Y. Research and Reflection on the Application of Blockchain Technology in the Field of Expressway Tolling [C]// Proceedings of 17th China Intelligent Transportation Annual Conference. Beijing:China Machine Press, 2022:68.)

[16] 宋英齐,冯荣权.零知识证明在区块链中的应用综述[J].广州大学学报(自然科学版),2022,21(04):21-36.(SONG Y Q, FENG R Q. Review of the application of zero-knowledge proofs in blockchain [J]. Journal of Guangzhou University (Natural Science Edition), 2022, 21(04): 21-36.)

[17] 林绍福,李昀辉.一种基于区块链与零知识证明的个人轨迹证明方法:中国, CN202110716097.6 [P].2021-10-19.

[18] BHANDARI S, HARSHA P, KUMAR M, et al. Algorithmizing the multiplicity schwartz-zippel lemma[C]//Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms. Philadelphia:Society for Industrial and Applied Mathematics, 2023: 2816-2835.

[19] MENEZES A, SARKAR P, SINGHG S. Challenges with assessing the impact of nfs advances on the security of pairing-based cryptography[C]// Proceedings of the International Conference on Cryptology in Malaysia. Cham:Springer, 2016: 83-108.

[20] HAQUE M A, IQBAL M S, KABIR M M. An automated toll plaza system using RFID and GSM module: perspective of bangladesh[C]// Proceedings of the 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI). Piscataway:IEEE, 2020: 1-6.

This work is partially supported by National Key Research and Development Plan Project (2020YFF0305400).

WANG Yifan, born in 2000, M. S. candidate. His research interests include blockchain and data governance,privacy protection for spatiotemporal data.

LIN Shaofu, born in 1967, Ph. D. professor. His research interests include smart city spatiotemporal big data,big data computing and intelligence,blockchain and data governance,Internet of Things and perceptual intelligence.

LI Yunjiang, born in 2001, M. S. candidate. His research interests include blockchain and data governance,privacy protection for spatiotemporal data.