清华大学

本科生毕业设计（论文）开题报告

学院：新雅书院

专业：计算机科学与技术

班级：新雅 91/计 92

姓名：狄永正

指导教师：向勇

二○二三年 一月 四日

一、 毕业设计（论文）选题的内容

本课题主要研究的内容是树状区块链的跨链操作的研究与设计。项目背景是使用树状的地理区块链构建基于以太坊的区块链网络，基于此网络在其中部署并运行出租车调度智能合约，构建基于树状区块链的出租车调度系统。本课题旨在从底层上优化现有的基于树状区块链的调度系统，实现跨链操作，提高区块链性能，同时增强其适用性。

二、 研究方案

2.1 本选题的研究背景

区块链技术（Blockchain technology，简称 BT）是利用块链式数据结构来验证与存储数据，利用分布式节点共识算法来生成和更新数据，利用密码学的方式保证数据传输和访问的安全，利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。用区块链技术所串接的分布式账本能让两方有效纪录交易，且可永久查验此交易。区块链技术具有去中心化、去信任化、匿名化、可扩展、独立性、安全性等特点，可应用到各种安全交易之中。

现阶段，城市中越来越多的流动车辆的增加极大的增大了城市的交通压力，在当下社会中，人们都过着快节奏的生活，对交通的便捷性需求自然日益增长。越来越多的人会选择计程车或网约车出

行；计程车，网约车有着针对性强，更为便捷，流动基数更多等特点，也切实的便捷了人们的出行。

随着智能车的发展与普及，车辆之间的交互将变得必不可少，为营造更安全高效的交通环境。决定使用区块链技术来构建车辆与路测节点间的特殊自组网，来进行车辆间或车辆与路侧节点间的数据交互。区块链的去中心化、独立性、匿名性等特点保证了该技术的透明安全性。

使用区块链技术可以去除中心管制，并基于此建立可信任、去中心化的数据库，创造共享式经济[1]。同时，在出租车调度系统中应用该技术可以消除中介，允许乘客与司机的直接交流与交易，能够为双方提供更为可信的验证，降低信任成本。在网络出租车服务中使用区块链技术有助于参与的所有利益相关方关系更加紧密[2]。

2.2 本选题的主要任务

1. 在导师的指导下阅读论文，查询文献，参考现有仓库，学习项目内设计的相关知识，了解出租车调度系统的系统模型（车辆乘客终端与树状区块链），地图的存储编码方式，地理树状区块链的数据结构，区域搜索算法，区域调度算法，区域快速查询算法等技术[3]，同时通过阅读论文，阅读前辈的复现手册等行为实现出租车调度系统的复现，能够在本地建立树状区块链，部署现有的调度系统合约，能够实现事件的正常交互与监听。能显示目前系统的用户界面，且复现完整的调度逻辑。

2. 研究树状区块链的数据结构，了解树状区块链的工作原理及底层架构，研究传统方法的跨链连接以及周畅前辈目前正在实现的跨链技术，给出文档说明，关注区块链技术的发展情况。

3. 做到在出租车调度系统的树状区块链上实现跨链技术，并投入到区域间的交流应用当中。

4. 针对树状区块链的跨链技术进行性能测试实验，测试跨链技术对速度的性能提高效果，研究哪项指标会影响到其性能同时测试指标参数对性能的影响情况，希望做到尽可能的改善区块链。

5. 研究新的合约协议（基于前面任务的完成情况）探索操作系统编程和区块链技术融合的可行性。

6. 完成毕业论文的中英文编写。

2.3 技术方案的分析、选择

2.3.1 已有工作

目前项目已经实现了基于以太坊智能合约平台实现 Geohash 矢量地图的存储与调用，实现了基于 Geohash 的导航算法以及基于 Geohash 的车乘调度系统。Geohash 是一种新型的地址编码方式，它可以使用 Base32 将传统的矢量地图编码成一维的字符串代替二维的经纬度数据，这么做可以将原本的二维空间查询转换为一维字符串匹配。利用此优势，GeoHash 编码可以实现时间复杂度为 O(1)的快速查询[4]。实现基于 Geohash 的导航算法的意义在于，不仅可以摆

脱对外部地图数据的依赖，极大的保障了地图数据的安全性，还可以提高地图搜索的速度，提高调度系统的整体性能。

在导航算法中，使用 A*算法[5]，以道路长度作为计算因子。此外，实现了在区块链上运行信誉评估系统，通过用户交互以及用户活跃度，作为主要因素衡量车辆的信誉度，同时允许司机和乘客进行相互评分，作为信誉度计算的一定参考。此方法基于用户间的交互，一定程度上可以提高数据可信度，确保信誉度机制的正向发展。出租车调度系统基于这些技术得以运行。

2.3.2 调研情况

2.3.2.1 树状区块链结构设计

将传统的区块链应用到出租车调度系统中的一个很大的弊端是，传统区块链在面对数量庞大的节点时，因为节点全在一条链上，其查询效率必然会降低；此外，传统区块链结构不能很好地支持对发生在特定区域的事务的查询：用户需要回溯链结构上的所有事务，然后匹配交易发生的位置[6][7]。为满足车联网所需的性能要求，大幅度提高地理区块链的区域搜索速度，项目决定用“树状区块链”来代替传统区块链。

如图 1 所示，树状区块链按照 Geohash 编码方式划分树状结构，根据不同长度的 Geohash 编码表示父链与子链关系。不同于传统区块链的结构单一，树状区块链结构中的区块根据其作用不同可以划分为创世块（Genesis Block），分支区块（Branch Block）和普通区

块（Common Block）三类。其中创世块是所有区块的根节点，所有的区块链都有相同的创世块 Gensis，然后根据 Geohash 范围划分不同的区域子链。分支区块以 Geohash 作为索引，是指定分支的第一个区块，只维护直接下层区域的索引信息，不记录交易信息。分支区块由于具备指向同层级前一个分支区块的平行链指针使得原有单链结构成为树状多链构。普通区块则基本与传统区块相同。

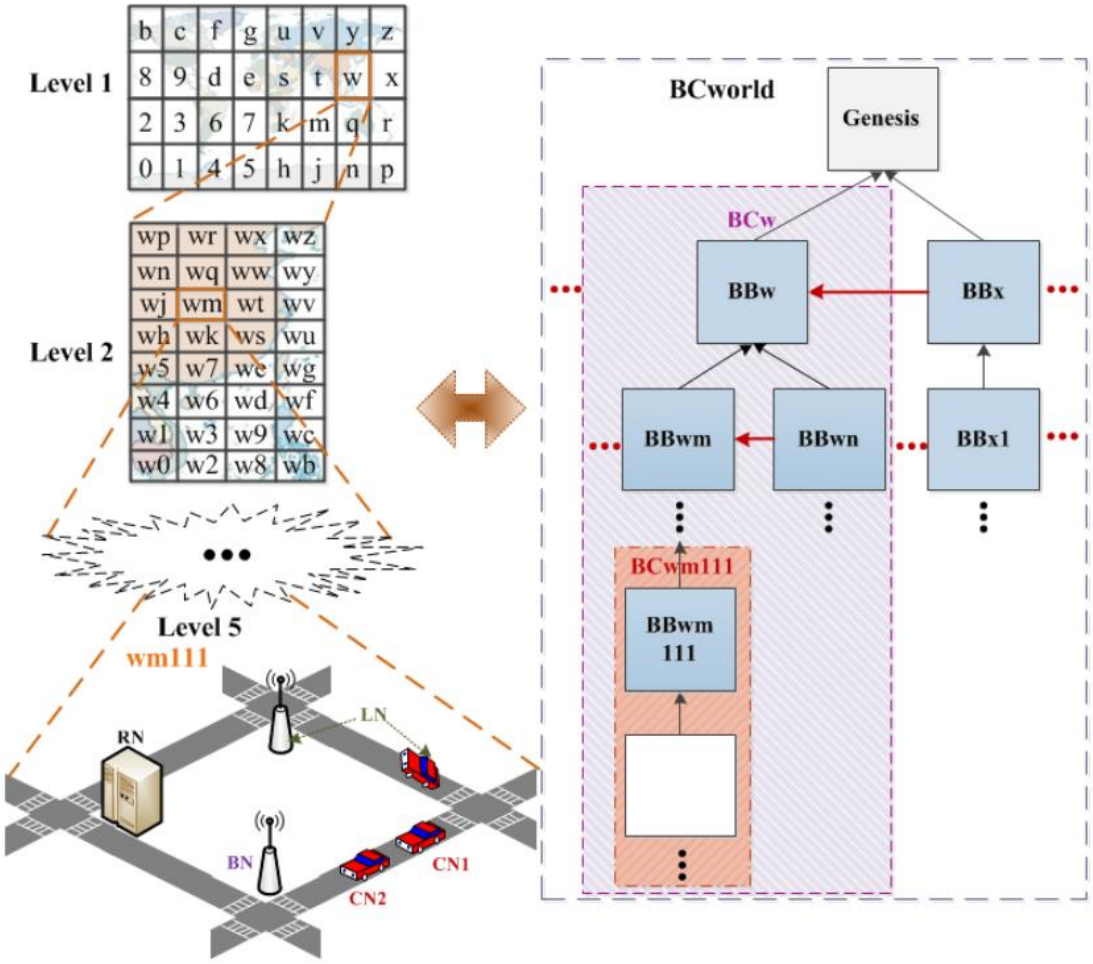

图 1 树状区块链示意图

图二中是树状区块链的内部结构属性示意图，展示了区块链的存储的各种属性，以太坊的结构包括三种查找树：收据查找树、地理

状态查找树和交易查找树。除此之外，还添加了一个区域状态查找树来快速查询与分层地理位置相关的数据，以及一个帐户位置查找树来支持查询每辆车的历史交易位置。

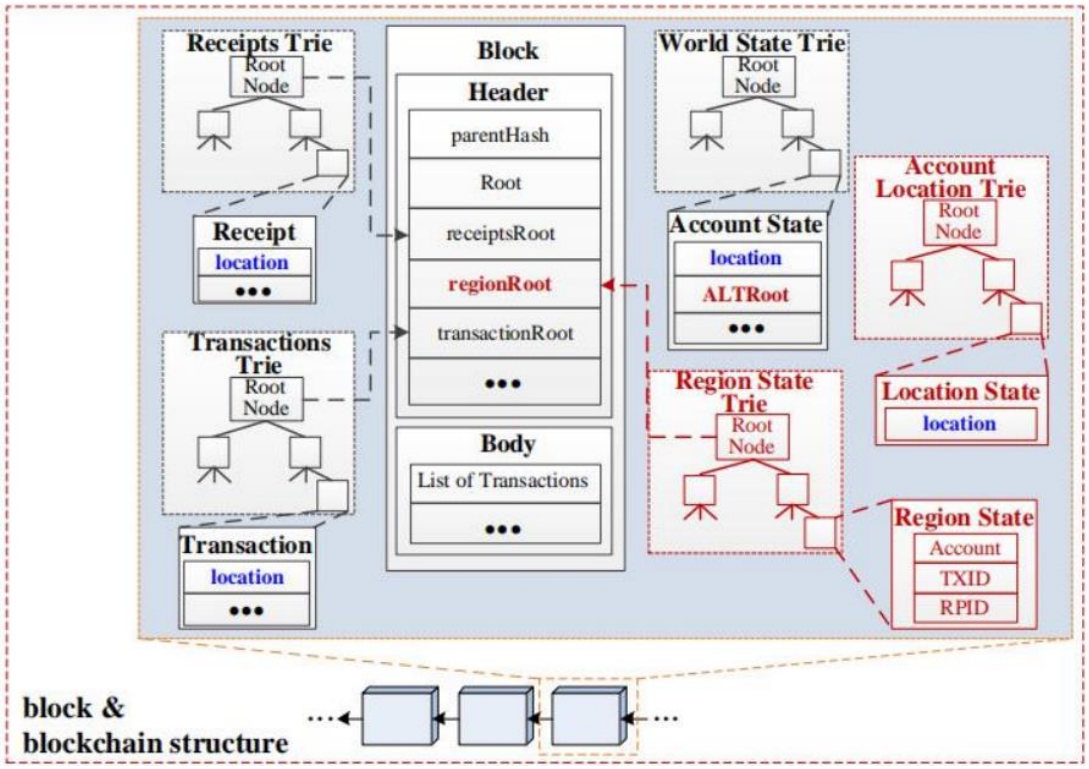

图 2 树状区块链内部结构属性示意图

在现有的工作中，树状区块链在区域查询时可以对各种节点的各种属性进行高速索引，做到既有传统区块链所具有的安全性优势，同时也可以提高区块链的工作效率。但是，目前的工作仍有改善的空间，当前工作针对区域中的搜索可以高效完成，但当节点的地理位置发生较大移动时，此时必须要考虑将节点进行跨链移动，维持多链间的信息同步。简而言之，为使得树状区块链适配更广的适用范围，同时保持工作效率，需要基于现有的出租车调度系统，在其上实现树状区块链的跨链操作，针对树状区块链的跨链技术进行性

能测试实验，测试跨链技术对速度的性能提高效果，研究哪项指标会影响到其性能同时测试指标参数对性能的影响情况，希望做到尽可能的改善区块链。

2.3.2.2 传统跨链技术的简单介绍

2.3.2.2.1 中继技术：Polkadot 和 COSMOS

Polkadot 是由原以太坊主要核心开发者推出的公有链[8]。Polkadot 计划将私有链融入到公有链的共识网络中，同时又能保有私有链的原有的数据隐私和许可使用的特性。它可以将多个区块链互相连接。Polkadot 还是以以太坊为主，实现其与私链的互连，并以其他公有链网络为升级目标，最终让以太坊直接与任何链进行通讯。

Cosmos 是 tendermint 团队推出的一个支持跨链交互的异构网络。Cosmos 采用的 Tendermint 共识算法，是一个类似实用拜占庭容错共识引擎，具有高性能、一致性等特点，而且在其严格的分叉责任制保证下，能够防止怀有恶意的参与者做出不当操作的技术。

2.3.2.2.2 哈希锁定技术

全称为哈希时间锁定合约，英文为 HTLC（Hash TimeLock Contract）[9]，是闪电网络中提出的一种新的技术实现形式，指在智能合约的基础上，让双方先锁定资产，如果都在规定的时间内输入正确哈希值的原值，即可完成交易。

2.3.3 计划进行的测试工作

目前所计划的测试工作主要是基于树状区块链的跨链操作的实现之上，将其应用到车辆调度系统当中。

设定车辆每隔一段时间发送一次位置交易，制定车速。车辆节点将车辆位置写入事务中，以记录车辆的移动。统一车辆的移动路径长度，分别实现地理区块链同一区域内的数据传递和跨不同区域的数据传递，每个车辆节点每隔固定时间发送一个事务。

为了评估跨链操作的性能，主要探索如下两个指标：(1)将相同内容和相同交易数量的时间作为构建时间，比较是否进行跨链操作所需要的时间成本。(2)取写入区块链的内容相同、交易量相同的链上数据和本地数据量，比较是否进行跨链操作所需的空间成本。跨链操作一般需要侧链，此对比主要探索跨链操作相较于单区域区块链到底需要额外支出多少空间消耗。

2.4 实施技术方案所需的条件

所有操作主要在操作系统为 Ubuntu 22.04.1 LTS 的虚拟机平台上测试，需要用到的技术平台框架大致有以太坊平台，leaflet 框架，Geohash

2.5 存在的主要问题和技术关键

2.5.1 主要问题

目前存在的主要问题是：本系统相较于传统区块链采用的是树状区跨链的方法，拓扑结构较为复杂，在复刻时需要维护更多，对确

保跨链交易的原子性有更高的要求。因此需要更加深入地理解树状区块链和普通传统区块链的不同，基于此实现传统跨链方法在树状区块链上的复刻。

此外，在探索树状区块链跨链操作的性能效果时需要设计针对性的测试用例，这需要对跨链技术的原理有着较为深刻的理解。

2.5.2 技术关键

树状区块链的数据结构，跨链技术的原理及应用，以及针对区块链的各种管理工具。

2.6 预期能够达到的研究目标

本项目预期达到的目标为，成功实现树状区块链的跨链操作，并可以投入到出租车调度系统当中进行使用，同时，本项目还需要测试跨链操作对区块链的性能会具有怎样影响，通过优化指标的方式尽可能地提高树状区块链的速度，减少树状区块链的资源开支。

完成毕业论文一份，开发软件成果一份，完成毕业论文的英文翻译工作。

三、 课题计划进度表

时间	工作	完成标志
2022.12.1—2023.1.9	参与选题，查阅文献，了解课题研究内容，确定毕设方向并完成开题报告	完成开题报告，完成系统复现

2023.1.9—2023.1.31	继续框架的学习与研究，学习前辈的跨链实现，编写文档；同时研究传统区块链的跨链技术的实现	编写一份跨链技术的说明文档，明确跨链技术的工作原理
2023.2.1—2023.3.1	剖析基于地理位置的树状区块链的数据结构，用传统方法尝试实现跨链连接，同时研究新的合约	能够实现树状区块链的跨链操作，并且可以进行后续实验
2023.3.1—2023.4.1	进行对比实验测试，研究哪项指标会影响到其性能，同时测试指标参数对性能的影响情况，尝试基于该项目设定相应协议以提高交流速率	给出实验结果，并写出实验报告，描绘出影响区块链性能的因素
2023.4.1—2023.5.1	针对性能测试进行优化，有可能的话对安全性进行维护的探索；进行总结并开始准备论文的编写	同样给出实验报告，描述优化测试的结果
2023.5.1—2023.6	完成最终的毕业论文，参加答辩	成功完成毕业设计

四、 参考文献

[1] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," in IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218.

[2] Dorri A, Steger M, Kanhere S S, et al. Blockchain: A distributed solution to automotive security and privacy[J/OL]. IEEE Communications Magazine, 2017, 55(12): 119-125. DOI: 10.1109/MCOM.2017.1700879.

[3] ZHOU C, LU H, XIANG Y, et al. Geohash-Based Rapid Query Method of Regional Transactions in Blockchain for Internet of Vehicles[J]. Sensors [Online]. Available: https://doi. org/10. 3390/s22228885, 2022.

[4] Liu J, Li H, Gao Y, et al. A geohash-based index for spatial data management in distributed memory[C]//2014 22Nd international conference on geoinformatics. 2014: 1-4.

[5] 张海亮,张征.基于 GeoHash 索引的 A~*算法优化[J].火力与指挥制,2021,46(06):78-83.

[6] Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, A.; Guizani, M. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1212–1239.

[7] Ibrahim, M.; Lee, Y.; Kahng, H.K.; Kim, S.; Kim, D.H. Blockchain-based parking sharing service for smart city development. *Comput. Electr. Eng.* **2022**, *103*, 108267.

[8] Hanaa Abbas; Maurantonio Caprolu; Roberto Di Pietro. Analysis of Polkadot: Architecture, Internals, and Contradictions. DOI: https://doi.org/10.48550/arXiv.2207.14128

[9] 张诗童,秦波,郑海彬.基于哈希锁定的多方跨链协议研究[J].网络空间安全,2018,9(11):57-62+67.