北京理工大學

本科生毕业设计（论文）

树状区块链测试与改进

The Testing and Enhancements of Tree-Like Blockchain

学　　院：计算机学院

专　　业：计算机科学与技术

班　　级：07111905

学生姓名：傅泽

学　　号：1120192062

指导教师：陆慧梅

2023 年 5 月 9 日

原创性声明

本人郑重声明：所呈交的毕业设计（论文），是本人在指导老师的指导下独立进行研究所取得的成果。除文中已经注明引用的内容外，本文不包含任何其他个人或集体已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。

特此申明。

本人签名：　　日 期：　　年　月　日

关于使用授权的声明

本人完全了解北京理工大学有关保管、使用毕业设计（论文）的规定，其中包括：①学校有权保管、并向有关部门送交本毕业设计（论文）的原件与复印件；②学校可以采用影印、缩印或其它复制手段复制并保存本毕业设计（论文）；③学校可允许本毕业设计（论文）被查阅或借阅；④学校可以学术交流为目的，复制赠送和交换本毕业设计（论文）；⑤学校可以公布本毕业设计（论文）的全部或部分内容。

本人签名：　　日 期：　　年　月　日

指导老师签名：　　日 期：　　年　月　日

树状区块链测试与改进

摘　要

2008 年，随着中本聪发布《Bitcoin: A Peer-to-Peer Electronic Cash System》论文，区块链技术横空出世，并迅速以其去中心化、不可篡改等特点，迅速博得了大量行业的青睐。目前，区块链技术已经在数字货币、车联网等领域取得了亮眼的成绩。然而，传统区块链采用单链结构，每个区块仅存储上一个区块的哈希信息，在需要应对大吞吐量的工况下，容易因链条过长导致性能下降；此外，在应用于车联网这一场景下时，由于区块并未按照地理位置存储，而车辆节点需要关心的信息大多来自临近区域的区块数据，故可能需要耗费诸多不必要的查询开销。

为解决上述两个问题，“树状区块链”应运而生。在树状区块链中，区块被分为创世块、分支区块和叶子区块三种。叶子区块和传统的区块链并无太大差异；分支区块则负责将数个叶子区块组织起来，按照叶子区块所代表的地理位置，结合 GeoHash 编码技术形成类似于字典树的树状结构；创世块和分支区块类似，但它没有父链指针。由于树状结构相比单链结构的深度更小，且采用了与地理位置相关的 GeoHash 进行分支构造，故树状区块链有望为上述两个问题提供合理的解决方案。

本课题首先研究树状区块链相较传统链式区块链的优势与局限性；其次，以出租车调度系统为背景，测试树状区块链和传统链式区块链在运行该调度系统时的性能表现差异；最后，讨论将现有树状区块链的运行平台由以太坊支持的以太坊虚拟机（EVM）迁移至兼容性更广、性能更佳的 Web Assembly 平台上的优势及可行性，并进行部分迁移工作加以佐证。

关键词：北京理工大学；本科生；毕业设计（论文）

The Testing and Enhancements of Tree-Like Blockchain

Abstract

In 2008, with the release of Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" paper, blockchain technology came into the world, and quickly with its decentralized, tamper-free characteristics, quickly won the favor of a large number of industries. At present, blockchain technology has made remarkable achievements in digital currency, Internet of vehicles and other fields. However, the traditional blockchain adopts the single-chain structure, and each block only stores the hash information of the previous block. Under the working condition of large throughput, the performance is likely to be degraded due to the long chain. In addition, when applied to the scenario of the Internet of vehicles, because the block is not stored according to the geographical location, and most of the information that the vehicle node needs to care about is from the block data in the adjacent area, it may consume a lot of unnecessary query costs.

To solve the above two problems, "tree-like blockchain" came into being. In a tree-like blockchain, blocks are divided into genesis blocks, branch blocks and leaf blocks. The leaf block is not very different from the traditional blockchain, while the branch block is responsible for organizing several leaf blocks, according to the geographical location of the leaf block, combined with GeoHash coding technology to form a tree structure similar to dictionary tree. The major difference between the branch block and the genesis block is that a genesis block does not have the so-called "parent block pointer". Due to the smaller depth of the tree structure compared to the single chain structure and the use of GeoHash for branch construction, it is expected to provide a reasonable solution to the above two problems.

Based on the laboratory's existing work "tree-like blockchain", this topic studies the advantages and limitations of tree blockchain compared with traditional blockchain. Taking the taxi dispatching system as the background, we test the performance differences between the tree blockchain and the traditional blockchain when running the dispatching system. Finally, the advantages and feasibility of migrating the Ethereum Virtual Machine (EVM)

supported by Ethereum to the Web Assembly platform with wider compatibility and better performance are discussed, and some migration work is carried out to prove it.

Key Words: BIT; Undergraduate; Graduation Project (Thesis)

目 录

第 1 章 绪论

1.1 研究背景

区块链是一种分布式的共享账本，允许数个参与方一同共享数据。区块链技术所拥有的去中心化、透明性和安全性等优势，令这一新兴的概念迅速为各行各业接受：中国人民银行数字货币研究所正在积极探索区块链技术在低并发、低敏感的资产确权、交易转让、账本核对等场景下的应用[1]；区块链透明化的特点和极高的安全性也引起了地产行业的注意[2]。可以预见，区块链技术在未来将吸引更多行业加入，以其去中心化、不可篡改等特性造福人类社会。

树状区块链，是实验室正在开发并已趋于完善的改良型区块链。其基本思想大致为：将区块分为创世块、分支区块和叶子区块三种；结合 GeoHash 编码技术，不再采用传统区块链的单链结构，形成类似于字典树的树状结构；同时，为了满足快速查询的需要，在区块中增添了一些辅助数据结构。经过以上改良，树状区块链可以在对地理位置敏感、且网络结构变化较频繁的应用场景中，发挥相较传统区块链更好的理论性能。

车联网技术（Internet of Vehicle）属于物联网技术的范畴，其思想乃是在车辆上搭载接入网络的设备，旨在实现不同车辆之间的相互通信；不仅如此，车联网技术也容许车辆与行人、路边基站等交通参与方和交通基础设施通信，实现实时的车况检测、路况查询与收集等功能，对于提升车主用车体验、乘客出行体验有强大的潜力。2022 年 12 月 8 日，公安部发布的数据显示全国机动车保有量到达 4.15 亿辆，机动车驾驶员人数超过 5 亿位！随着如何安全有效地管理如此庞大的保有量带来的海量数据这一巨大挑战变得日益严峻，人们纷纷将目光转移到了区块链上[3]。然而，传统区块链在处理车联网场景下的具体事务时，往往存在诸如此类的一些弊端：

- 车辆作为区块链网络的参与者（节点）时，其地理位置可能发生很大变化，致使网络结构需要频繁更新；
- 传统区块链采用单链结构，在区块链上执行的查询时间复杂度较高；
- 在车联网系统中，车辆应该关心的信息大部分来自于其所在位置的临近街区，而传统区块链并不以地理位置索引区块及其交易，故一次查询可能会获得较多

无用信息等。

由于树状结构相比单链结构的深度更小，且采用了与地理位置相关的 GeoHash 进行分支构造，故有效降低了查询开销，令基于位置的信息查询能够更加“有的放矢”，有望为运用区块链技术处理车联网问题提供合理可行的解决方案。

目前，实验室已有的树状区块链采用以太坊（Ethereum）实现。以太坊是一个开源的区块链计算平台，允许开发者进行去中心化应用程序（DApp）的开发和部署。其支持以 Solidity 编程语言编写运行在在以太坊虚拟机上的脚本程序（智能合约 Smart Contract），极大拓宽了区块链的功能适用性。

Substrate 是一组开源、模块化的区块链开发框架，允许开发者自由地使用官方预定义的各种组件构建个性化的区块链，并于其上使用基于 Rust 的 ink! 编程语言进行智能合约开发。与以太坊比较，Substrate 具有包括而不仅限于如下优势：

- 支持模块化设计，程序员可以轻松增删模块，构建更加贴近实际需求的区块链
- 采用 Rust 编程语言作为其底层实现，速度更快，效率更高
- 支持编译为大多数现代浏览器支持的 WebAssembly 二进制，提供了更好的跨平台兼容性

本文将在车联网的应用场景下，以实验室已有工作——出租车调度系统为例，探究树状区块链在不同工况下的性能表现，验证其拥有相较传统单链区块链更好的性能表现。本文还将积极尝试为将树状区块链从以太坊平台转向更优秀的 Substrate 平台。鉴于时间和笔者能力之限，本文仅讨论区域索引区块链的部分特性的迁移工作，此举旨在验证两平台在功能上的相似性，进而确保未来树状区块链的底层功能迁移工作的可行性。

1.2 相关技术调研

1.2.1 区块链技术概述

2008 年，一位自称为中本聪的人发布了名为《Bitcoin: A Peer-to-Peer Electronic Cash System》的论文，宣告了区块链技术的诞生。区块链，乃是一个分布式的账本；区块链网络不存在所谓的“中心服务器”，每台参与构成区块链网络的计算机（又被称为“节点”）均持有一份该账本的副本。每一笔交易，都将记录在名为“区块”的

数据结构中；随着区块的不断产生，它们将形成一条单向链状结构，且区块上存储的数据将不可再被修改。通过称为共识算法的机制，各节点能够就区块链的当前状态达成一致，并在链上数据发生变化时及时追踪并更新到自身存储的账本中。不仅如此，若某个节点尝试擅自修改自身所持有的账本，其行为会被共识算法拒绝，从而规避了恶意篡改链上数据的风险。上述区块链的优势，令区块链这一新兴的概念迅速吸引了各行各业的眼球。可以预见，区块链技术在未来将吸引更多行业加入，以其去中心化、不可篡改等特性造福人类社会。

1.2.2 智能合约概述

智能合约（Smart Contract）这一概念由 Nick Szabo 于 1994 年提出。在比特币的支付模型中，仅存在一个简单的堆栈计算机。由于其可用的操作方法并非图灵完备，只能执行比较简单的操作，从而限制了区块链的应用场景。智能合约的出现打破了这一局面。在 Szabo 于 1996 年撰写的《Smart Contracts: Building Blocks for Digital Markets》一文[4]中，Nick 设想智能合约就是运行在区块链上的一段程序，当满足某种条件时，相应代码将自动被执行，而该过程人类无需也无法介入。智能合约一定程度上避免了交易双方抵赖的问题，并且其图灵完备的特性也令区块链技术在不同应用场景下的适应性大大增加了。

1.2.3 区域索引区块链和树状区块链概述

周畅设计的区域索引区块链，实现了区块链地理信息索引方法，能够依据地理位置信息快速查询特定位置的交易[5]。如图 1-1 所示，相较以太坊官方实现的传统区块链而言，区域索引区块链在区块头中加入了区域状态树的树根哈希，以支持基于位置的快速信息查询；同时，为追踪每个账户的包括位置信息的完整状态，在账户状态数据结构中还加入了当前的地理位置字段、和账户位置树这一数据结构。不仅如此，在记录交易、收据时，均会记录发起动作的地理位置信息，并以此更新发起人的账户的当前位置及账户位置树。文献[5]中指出，采用 3 到 6 位 GeoHash 编码时，区域索引区块链相较传统的无索引区块链，执行相同查询的耗时仅为后者的 5.3%。

区域索引区块链仍然保留了传统区块链的单链结构，当区块数量很大时，其查询效率仍然会随之降低。因此，周畅提出并设计了基于区域索引区块链改良的树状区域索引区块链（下简称树状区块链）。其按照 Geohash 编码长度，表示父链和子链的关系，并划分区域子链。树状区块链的区块也分为三种：叶子区块、分支区块和创

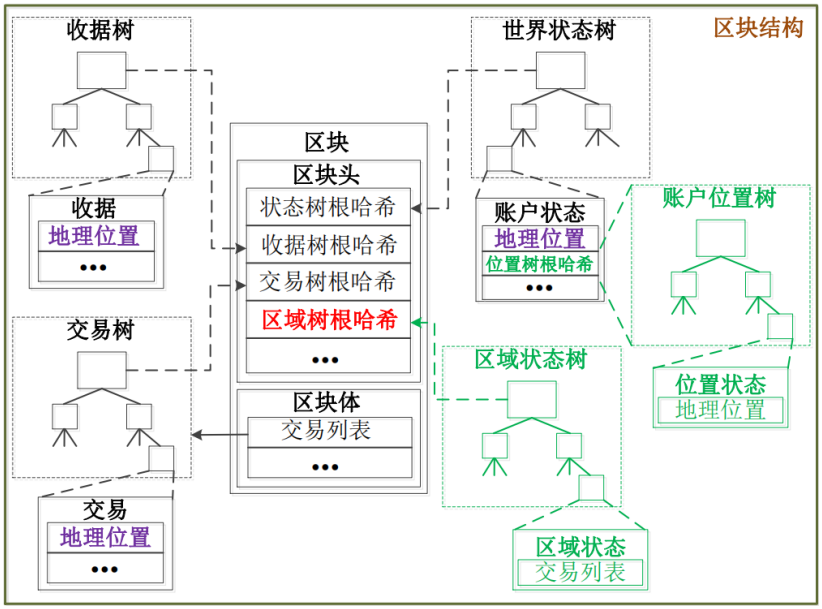

图 1-1 区域链区块示意图

世块。叶子区块和传统的区块链并无太大差异，叶子区块及其后续区块均采用传统的单链结构加以组织；分支区块则负责将数个叶子区块组织起来，按照叶子区块所代表的地理位置，创世块和分支区块十分相似，但它没有父链指针。上述树状区块链的设计，进一步缩短了区块链网络中的单链长度，进而提升了查询效率。

1.2.4 以太坊和 Substrate

中本聪提出的比特币区块链系统支持简单的基于栈的编程语言，由于其并非图灵完备（例如不支持循环等结构），程序员仅能在其上进行受限的操作，这很大程度上限制了区块链技术的应用场景。以太坊[6]技术的诞生，旨在提出一种建立分布式应用程序（又名去中心化应用程序，DApps）的新方法，其提供名为以太坊虚拟机（EVM），采用图灵完备的编程语言，令程序员得以编写更复杂更强大的智能合约，进而根据实际需求灵活定制状态转换函数等功属性。

以太坊技术的成熟引领人们走进了 Web 2.0 时代。然而，随着以太坊在各行各业使用愈加广泛，其局限性亦逐渐显露。简而言之，以太坊为保证其功能全面性，其官方实现非常复杂且可扩展性不足，导致程序体积巨大、运行效率低下、且核心定制变得尤为繁琐。Substrate 提出了一种模块化的区块链构建框架，允许程序员自行选用充分必要的模块构建更贴近实际需求，拥有更少多余功能的区块链。此外，Substrate 选用 Rust 编程语言作为其底层实现，令区块链在 WebAssembly 上运行成为可能。由

于现代浏览器普遍支持 WebAssembly，这意味着区块链的运行环境终于从以太坊虚拟机（EVM）中解放出来，可以在浏览器中直接运行，不仅程序运行速度更快，且跨平台兼容性大大提升。

1.3 本文研究内容及贡献

本文将在车联网这一应用场景下，首先基于区域索引区块链，复现实验室已有工作——出租车调度系统的有关工作，证明该系统的可用性。此后，设计并进行树状区域索引区块链在单父链双子链的网络结构下的跨链转账实验，探究树状区块链在不同转账请求压力下的性能表现，验证其功能可用性，并测试跨链操作带来的额外时间开销。作为测试实验的收尾，本文将设计实验，令出租车调度系统分别在网络结构不同的树状区块链上运行，收集并可视化实验数据，评估树状区块链在不同工况的实际应用场景下的性能表现。本文还将为树状区块链从以太坊平台转向更优秀的 Substrate 平台做出积极探索。鉴于时间和笔者能力之限，本文仅讨论区域索引区块链的部分功能特性的迁移工作，此举旨在验证两平台在功能上相似，进而证明未来树状区块链的底层功能迁移工作的可行性。

1. 基于区域索引区块链，复现实验室已有工作——出租车调度系统，证明该系统的可用性；编写帮助文档和实验日志，以便后人推进研究

2. 设计并进行树状区域索引区块链在单父链双子链的网络结构下的跨链转账实验，记录其对 10 个、20 个、40 个、80 个、120 个、160 个、200 个账号执行子链之间的跨链转账的耗时、吞吐量等数据，并进行可视化；编写帮助文档和实验日志，以便后人推进研究

3. 在单子链、单父链四子链的网络结构下分别运行出租车调度系统，探究树状区块链在不同工况实际场景中的性能表现，并进行数据可视化；编写帮助文档和实验日志，以便后人推进研究

4. 探索区域索引区块链的部分功能特性从以太坊向 Substrate 的迁移的可行性，为 Substrate 的官方实现引入账户地理位置这一字段，令其可以在创世块配置文件中修改、在账户查询时显示；编写实验日志，以便纠错和改进

公式标注应于该公式所在行的最右侧。对于较长的公式只可在符号处（+、-、*、/、≤≥等）转行。在文中引用公式时，在标号前加“式”，如式（1-2）。阅后删除此段。

公式-示例：（阅后删除此段）

$$LRI = 1 \diagup \sqrt{1 + \left(\frac{\mu_R}{\mu_s}\right)^2 \left(\frac{\delta_R}{\delta_s}\right)^2} \tag{1-1}$$

第 2 章 基于区域索引区块链的出租车调度系统复现

本章讨论基于区域索引区块链的出租车调度系统的复现工作。

基于区域索引区块链的出租车调度系统，以董斌的区块链地图存储作为基础，由成佳壮首先提出并实现路径规划和司乘匹配等算法，并随后经过万琦玲完善，并初步形成了复现手册；它是一套采用实验室已有成果——区域索引区块链作为服务器后端、Vue 2.JS 作为前端的出租车调度系统。在万琦玲设计的前端页面上，用户可以通过实时地图信息，直观地获得自己的位置，以及附近在线的乘客、司机等信息。用户角色分为乘客和司机两大类，前者可以进行提交乘车请求、确认上车和付款等操作，而后者可以选择是否接受派来的订单，确认到达乘客上车地点和确认到达乘客下车地点等操作。

本文将基于上述实验室已有工作，进行该基于区域索引区块链的出租车调度系统的复现工作，并详细讲解在复现过程中遇到的问题，及其解决方案。此外，该部分工作还补充了初版复现手册的缺漏，修正了其中的错误，重构了已有的脚本代码，提升了可扩展性和鲁棒性，形成了新版的复现手册，方便后人参考[1]。

2.1 环境配置

本文复现工作将在如下环境中进行：

表 2-1 复现环境

中央处理器	Intel Core i5-12500H
图形处理器	Intel Iris Xe 80EU
内存	24GB
操作系统	Ubuntu 22.04.1 LTS
虚拟机	VMWare Workstation Pro 17

将 Ubuntu 虚拟机环境配置妥当之后，还需安装 node.js、npm、web3.js 等 JavaScript 库。同时，将区域索引区块链的二进制可执行文件（代码仓库中的 geth1 二进制可执

[1] https://github.com/Endericedragon/ReproducingBlockchain

行文件）存放到/usr/local/bin 文件夹下备用。

2.2 复现步骤

详细的复现过程已记录于代码仓库的《8 重做调度系统复现实验.md》文档中，本文将只进行简单介绍。需要指明的是，原复现手册中存在许多前置实验，本文略过了这些前置实验，仅详细介绍最后有关调度系统复现的实验。

2.2.1 建立区域索引区块链

启动终端，切换至创世配置文件 genesis.json 所在的目录，随后键入如下指令并执行：

代码 2.1: 初始化区块链

```
geth1 --identity "MyEth" --rpc --rpcaddr 127.0.0.1 --rpcport "8545" --rpccorsdomain "*" --datadir gethdata --port "30303" --nodiscover --rpcapi "eth,net,personal,web3,admin" --networkid 91036 init genesis.json
```

对于其中的关键参数选项解释如下：

- rpcaddr、rpcport：RPC 端口的地址及端口号。外部程序可以使用该端口接入区块链，进而借助 JSON-RPC API 或者 web3.js 库和区块链进行交互。
- datadir：该选项指定链上数据在本地永久存储的位置。
- rpcapi：使用 RPC 端口与链交互时，仅能使用该选项指定的数个功能。本文将使用 eth，net，personal，web3，admin 这 5 个功能模块，它们涵盖了挖矿、发现节点、账号管理等功能，足以满足复现实验要求。
- init genesis.json：指定使用名为 genesis.json 的创世配置文件进行初始化。

执行结束后，再执行以下命令，即可启动该区块链：

代码 2.2: 启动区块链

```
geth1 --datadir ./gethdata --networkid 91036 --port 30303 --rpc --rpcaddr 127.0.0.1 --rpcport 8545 --rpcapi 'personal,net,eth,web3,admin' --rpccorsdomain='*' --ws --wsaddr='localhost' --wsport 8546 --wsorigins='*'
```

```
--wsapi 'personal,net,eth,web3,admin' --nodiscover --allow-insecure-unlock
--dev.period 1 --syncmode='full' console
```

注意其中的 syncmode 参数选项，其值为'full'。此时，该区块链将仅使用区域索引方法进行加速，而不会使用任何树状区块链的功能特性。

启动区块链后，终端中将出现 JavaScript 控制台，可以使用 JavaScript 编程语言的一个子集和链进行交互[7]。此时可以创建测试账户，充当司机和乘客；并且，每次启动区块链，都需要解锁这些账户，否则将无法进行智能合约部署等工作。本文创建了 8 个测试账户，分别扮演司乘角色，进行后续的实验。

创建账号后，还需前往创世配置文件中，为创建的账号赋予初始余额。赋予余额后，为强制 geth1 重新加载创世配置文件，需要手动删除存储链上数据的 gethdata 目录中的 geth 目录，并随后重新初始化并启动区块链。此时，geth1 将从创世块配置信息中加载账户余额，确保后续实验步骤可以正常开展。至此，区域索引区块链已经建立完成。

2.2.2 部署合约

实验室已有成果——出租车调度系统由两份智能合约构成，其文件名和其功能如下表所示：

表 2-2 智能合约功能概述

文件名	功能
StoreMap.sol	存储详细的地图数据，提供数据查询的结构及 A-Star 寻路等算法的实现
StoreTraffic.sol	司机和乘客的信息管理，提供司乘位置的改查、基于 Geohash 的距离计算等服务

将两份合约部署到区块链上，即完成树状区块链的部署工作。首先，使用

Remix Desktop 编译合约，记录编译结果中的 ABI 字段并进行进行压缩转义，同时记录 bytecode（下称字节码）字段。然后，将二者复制入附录 B 中的代码模板（其中的标识符 Contract 和 contractInstance 可以任意修改），将两份编辑好的模板先后复制入正在运行 geth1 的 JavaScript 命令行后并点按回车后，合约部署的请求就已经提交至交易池。开始挖矿并密切观察控制台输出，直至观察到形似以下格式的输出。此即为两份合约各自的合约地址，其顺序与提交合约部署申请的顺序一致：

代码 2.3: 合约地址

```
null [object Object]
Contract mined! Address: 0x23b98f92ceac005e570b6768da377b3abd11012e
[object Object]
null [object Object]
Contract mined! Address: 0xfa6b8f0b92b323c28557faf69da028e33856f6ca
[object Object]
```

笔者的部署顺序是：先部署 StoreMap，再部署 StoreTraffic。因此，地图存储合约的地址即为 0x23b98f92ceac005e570b6768da377b3abd11012e，而调度合约地址为 0xfa6b8f0b92b323c28557faf69da028e33856f6ca。

2.2.3 上传地图数据

成佳壮完成了上传地图所需的 JavaScript 脚本。使用时，首先需要前往该脚本源代码（对应代码仓库中的`uploadmap_cjz_3.js`），修改其中关于 StoreMap 合约地址的字符串变量的值、执行数据提交的账号的公钥地址，以及要上传的地图文件。令区块链开始挖矿后，运行该脚本，将看到终端不断输出信息，直至输出“地图数据上传完成”字样，结束挖矿。此时，所有地图数据就已全部上传到区块链上了。

2.2.4 配置前端并进行可用性测试

出租车调度系统的前端由 Vue 2 写成，在启动之前尚需一些配置方可正常运行。首先，需要修改`investigation-cjzhuang2020/cjz_underg_2021_09`目录下的一系列文件，各个文件的文件名及其内容如下表所示：

完成以上配置后，即可在区块链中开始挖矿，启动`vehicle_test.py`，程序将打开浏览器并自动操作，可观察到如下图的字样：

表 2-3 前端配置文件功能

文件名	功能
passengerAccounts.py	存储扮演乘客角色的账号的公钥
vehicleAccounts.py	存储扮演司机角色的账号的公钥
mapContract.js	关于地图智能合约的调用，需要修改合约地址，与 2.2.2 节记录的 StoreMap 合约地址一致
trafficContract.js	关于路径规划合约的调用，需要修改合约地址，与 2.2.2 节记录的 StoreMap 合约地址一致
passengers.js	存储每一位乘客的起始位置、上车位置和目的地位置
vehicles.js	存储每一位司机的初始位置

图 2-1 司机的初始化

此时启动passenger_test.py，程序将启动另一个浏览器窗口操作，此时需要在司机端浏览器窗口选择接客与否：

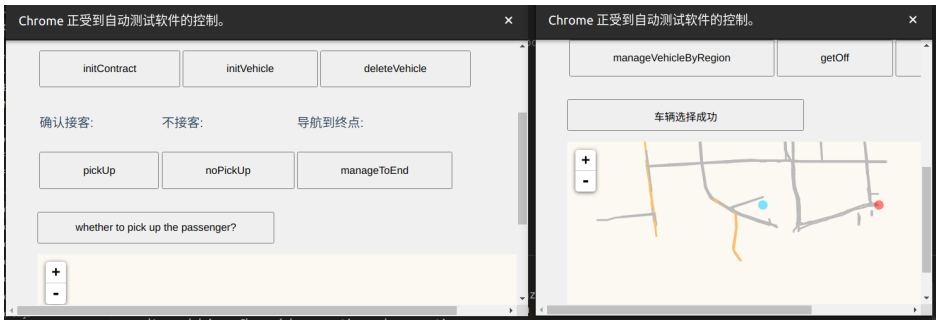

图 2-2 司机手动接客

按下 pickUp 按钮，程序将继续自动运行，直至看到如下输出，调度成功：

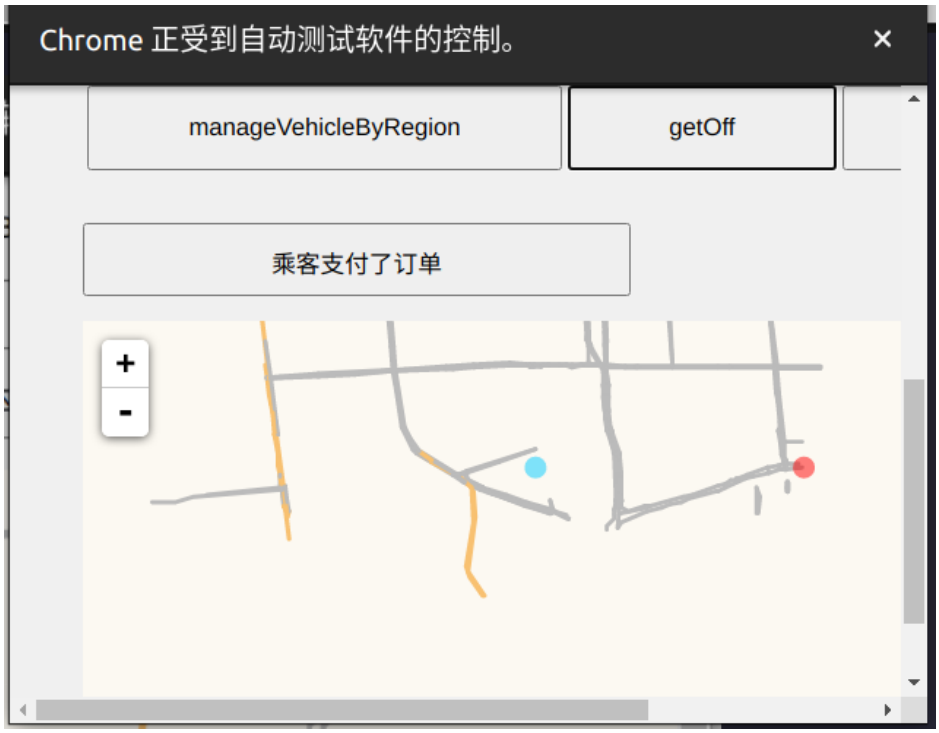

图 2-3 乘客抵达并支付

至此，原复现手册中的所有预期结果均已达到，调度系统复现实验全部完成。

2.3 问题及解决方案

笔者在进行出租车调度系统复现实验及其前置时，遇到许多原复现手册中未提及或未强调的注意事项；原版代码中，亦存在已废弃的语法和有待改进的设计。本节将陈述笔者遇到的问题及其解决方法。

2.3.1 创世配置文件指代不明

原复现手册中，并未指明在进行复现实验时使用的创世配置文件。经过笔者测试，附录 A 中的创世配置文件可用于所有出租车调度系统复现实验的全部环节。笔者已将其补充到代码仓库和新版复现手册中。

2.3.2 节点无法加入区块链网络

笔者在尝试建立双节点区块链网络时发现，无论如何使用`admin.addPeer()`函数，尝试将第二个节点连接到第一个节点，都无法成功，观察`net.peerCount`的值始终为 0，代表着第二个节点并未发现第一个节点。

实际上，节点与区块链网络中的其他节点使用的创世配置文件完全相同，是该节点加入此区块链网络的必要条件。因此，在配置第二个节点时，必须保证两个节点的创世配置文件完全相同。

需要注意的是，创世配置文件设定了各个账户的初始信息，例如余额和初始位置等等。因此，两个节点的创世配置文件完全相同，意味着两个节点中需要存在完全一致的账号。这要求程序员将第一个节点的 keystore 文件夹复制到第二个节点的相同的相对路径下。

综合以上两点，可以得出结论：当节点无法加入区块链网络时，需要检查节点的创世配置文件是否相同，以及节点的 keystore 文件夹内的内容是否一致。同时满足以上两点条件，节点才能成功加入区块链网络。

2.3.3 合约相关错误

在浏览器的前端系统中进行操作时，按下 F12 打开开发者选项窗口，可能会见到有关汽油费的错误提示（Out of Gas）。经过排查，这是合约的编写、上传、调用的过程出现了错误。由于问题隐蔽、报错信息不能直接反应实际问题点，笔者花费了较多时间调试合约相关之错误。现将部署合约以及与合约交互的正确操作流程陈述如下。

2.3.3.1 编译合约

笔者使用 Remix Desktop 进行合约编译。编译完成后，切换到编译选项界面，点击“Compilation Details”按钮，即可观察编译结果的详细信息，如下图所示：

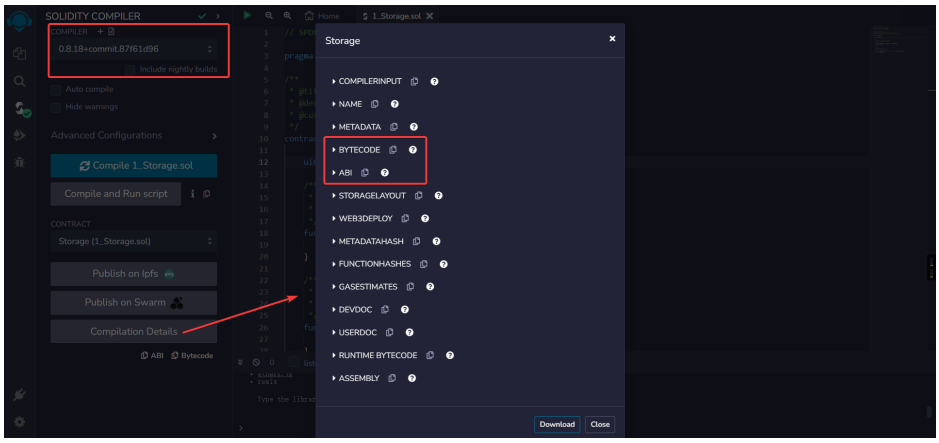

图 2-4 Remix IDE 编译选项界面

图中，更靠近中央部分的红框即为部署合约时需要使用的应用程序二进制接口（ABI）和以太坊虚拟机字节码（bytecode）信息，需要妥善记录保存。另外，在合约源代码所在的目录下的 artifacts 目录中，有一份与合约同名的 json 文件，该文件亦需要妥善保存备用。

2.3.3.2 部署合约

本文使用附录 B 中的合约部署模板进行合约部署工作，具体步骤如下：

1. 将代码模板中的“经过压缩转义后的 ABI”替换为经过压缩转义处理（即：去除多余空格，且为双引号等特殊字符进行转义处理）的上一步骤中获得之应用程序二进制接口
2. 将“获得的字节码字符串”替换为上一步骤中获得之以太坊虚拟机字节码
3. 修改变量名 Contract、contractInstance 为合适的名字，避免多份合约重名
4. 将经过以上修改的模板代码复制到正在运行 geth1 的控制台中，单击回车提交部署请求

5. 使用`miner.start()`开始挖矿，合约地址将随后在终端中显示

需要注意的是，在模板中，可见一名为 position 的字段。若该字段指代的 Geohash 在区块链的管辖范围之外（即：区块链管辖的 Geohash 并非 position 字段的前缀），将获得 out of the blockchain 错误，无法继续部署。因此，每次部署前，均需检查 position 字段指示的范围是否在区块链管辖范围以内。

2.3.3.3 合约交互

部署完成后的合约可以使用合约地址与其建立交互渠道，并调用合约内定义的方法。在 web3.js 库的辅助下，与合约进行交互仅需短短数行代码。最小示例如下：

代码 2.4: 合约交互

```
// 使用web3.js库
const Web3 = require('web3');
// 使用WebSocket协议连接到区块链，本例中端口号为8546
let web3 = new Web3(new Web3.providers.WebsocketProvider("ws://127.0.0.1:8546"));
// 部署合约时获得的合约地址
let contractAddress = '0x23b98f92ceac005e570b6768da377b3abd11012e';
// 编译合约时保存的应用程序二进制接口信息
let contractAbi = JSON.parse(fs.readFileSync('./contractAbi.json', 'utf-8'));
// 合约实例
let contractInstance = new web3.eth.Contract(mapContractAbi, mapContractAddress);
// 调用合约中定义的example方法
contractInstance.methods.example().then((res) => {/* 处理返回值res */});
```

在进行实验时，若出现难以排查的错误，应首先考虑合约相关错误。综合上述部署步骤，合约相关错误可以从以下几点进行排查：

- 从编译详情处获得的各项数据是否正确？例如，以太坊虚拟机字节码是否与应用程序二进制接口出自同一次编译过程？

- 部署合约时，是否正确配置各选项，例如 position 字段？
- 部署完成之后，是否正确记录合约地址？
- 进行合约交互前，是否确认区块链允许 WebSocket 协议连接？部分功能，例如订阅事件，仅能在 WebSocket 连接下进行。若无，则这些功能可能失效，与合约的交互可能失败。

2.4 本章小结

本章介绍了使用区域索引区块链进行基于区块链的出租车调度系统的复现实验之相关工作。首先，简要介绍该调度系统的功能及其组成部分；其次，介绍实验进行的环境配置和包括建立区块链、部署合约、上传地图、前端调试和使用等复现步骤，并展示了复现工作的运行结果，证明了复现工作的正确性；最后，介绍了在进行复现实验时遇到的典型疑难问题，对这些问题进行了产生原因的剖析，给出了解决方法和排查思路。

第 3 章 基于树状区块链的跨链转账测试

3.1 树状区块链的跨链转账

树状区块链，乃是以区域索引区块链为基础，旨在解决传统区块链单链结构面对大量区块时产生高昂性能代价的痛点。其借助 Geohash 技术，编码地理位置，并借此对区块链进行划分，形成类似于字典树的树状结构。

然而，这样的结构带来了一个问题：若某个账户的位置发生了较大改变，以至于它离开了目前所在的子链的管辖范围（即账户所在子链表示的 Geohash 范围不再是账户实际位置的 Geohash 编码表示的前缀），那么账户在新地理位置上发送的所有交易将失败，因为在逻辑上账户并不由管辖新地理位置所在片区的区块链直接管辖，后者可能根本没有关于该账号的任何记录，或者其上与该账户关联的信息并非切实。

对此，树状区块链的解决方案是：账户需要向一个特殊的管理账号发送一种特殊的交易，该交易及其携带的信息足以令管理账号从账户原先所在的区块链中，将账户的各项信息转移到新区块链上。此后，该账户可以认为由新区块链接手管辖，可以正常进行诸如发送交易等的区块链交互操作。由于上述转账过程与同一区块链内两不同账户间的转账不同，乃是横跨两个区块链的、同一账户之间的转账，故称该特殊转账过程为“跨链转账”。

显然，在尝试解决单链结构的效率问题的同时，树状区块链引入了跨链转账所需的额外时间开销。跨链转账操作的效率，将对用户的使用体验有较大的影响。因此，本章将围绕跨链转账这一主题进行探究。首先，设计并进行数组跨链转账测试实验；其中，以较小规模的 10 账号跨链转账实验测试跨链转账的正确性；验证正确性后，再开展更大规模的跨链转账测试，检验跨链转账操作在不同压力情况下的运行效率波动；最后，给出一个简单的数学模型，探究树状区块链跨链转账代价与其链上数据查询复杂度降低带来的性能优势基本持平时的临界条件，进而给出适用树状区块链代替传统单链结构区块链的应用场景建议。

3.2 设计测试

跨链转账测试实验将在如图 3-1 所示的区块链网络中进行。

该区块链网络共由三个链组成，分别以链 w1，链 w11 和链 w12 指代。链 w1 为

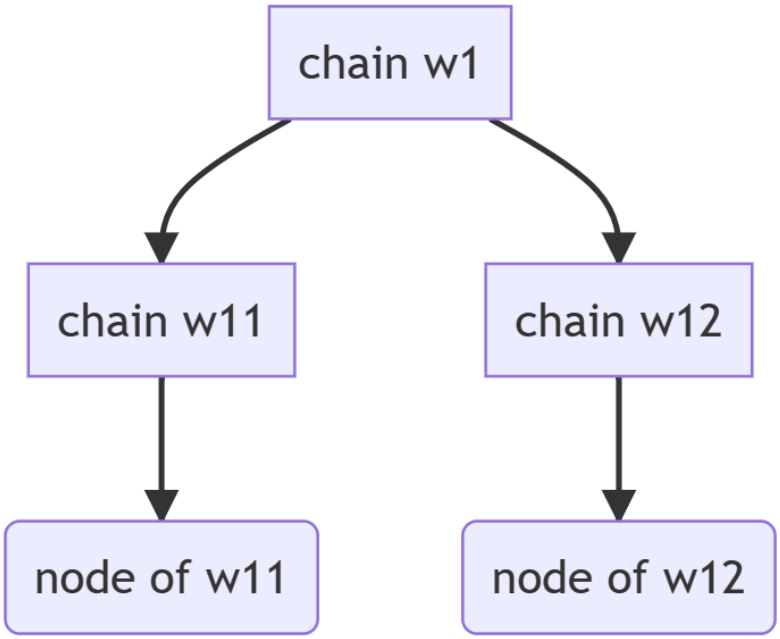

图 3-1 2leaf 结构

树状区块链中的分支区块链，其管辖的地理位置范围为 Geohash 编码为 w1 的所有区域；由链 w1 负责串联的子链 w11、子链 w12 均为叶子区块链，分别管辖 Geohash 编码前缀为 w11、w12 的所有区域，其下分别运行有一个节点，可以同传统区块链节点一样进行挖矿、交易等操作。初始时，两子链中存在相同的数个账号，但 w11 中的账号均有 5×10^{40} 单位的余额，w12 中的账号的余额均为 0，模拟账号进行了大范围物理位置变动后。管辖权仍未移交给管辖新地点的子链的情况。跨链转账开始后，待所有链 w11 中的账号同时发起转账申请后，树状区块链将开始串行地遍历所有子链 w11 中的账号，并将它们在链 w11 的余额全部转移至链 w12 的对应账号之下。待转账完成之后，检查链 w12 中各账户的余额，即可证明跨链转账的功能正确性。

在此过程中，监控程序将记录所有账号发起转账申请的时间戳、以及转账完成时的时间戳。通过分析以上数据，即能得到每个账号从串行处理开始至转账完成所花费的总时间，进而在初始待转账账号数量不同时，得出树状区块链在不同工况下的跨链转账效率。

本测试将从 10 个账号的小规模跨链转账测试开始，测试在小压力工况下跨链转账功能是否运转正常；在此基础上，继续开展 20 账号，40 账号，80 账号，120 账号，

160 账号及 200 账号跨链转账实验，探究面对不同压力工况时树状区块链的性能表现变化。

3.3 环境配置

跨链转账测试的测试环境如下：

表 3-1 跨链转账测试环境

中央处理器	Intel Core i5-12500H
图形处理器	Intel Iris Xe 80EU
内存	24GB
操作系统	Ubuntu 22.04.2 LTS
虚拟机	VMWare Workstation Pro 17

另外，还需安装`make`程序包，并下载树状区块链的源代码[1]。

3.4 测试步骤

3.4.1 编译并配置树状区块链

下载源代码后，在源代码目录启动终端，输入`make geth`，等待编译完成，即能在`build/bin`目录中发现 geth 二进制可执行文件。将其重命名为 geth-tree，并复制到`/usr/local/bin`目录中。

3.4.2 进行测试

代码仓库[2]给出了构建图 3-1 所示的区块链网络的数据文件和脚本，并附有一份实验手册。本节将简要介绍测试步骤。

1. 确认 w1、w11 和 w12 的数据目录中不存在`gethdata/geth`子目录。若存在，则需要将其删除；

2. 在代码仓库根目录中启动终端，运行`sh w1_init.sh`指令，启动分支区块链 w1，并留意形如`INFO [04-1020:36:48.833]` Started P2P networking self=”enode://.....”|

[1]https://github.com/xyongcn/BlockChain2017/tree/master/src/go-ethereum1.9.12-modify/go-ethereum

[2]https://gitee.com/endericedragon/transfer-2leaf

的输出，记录该双引号包裹的字符串；

3. 在链 w11 和链 w12 的预加载脚本中，替换admin.addPeer()方法的参数为上一步中记录的字符串

4. 另启动两个终端，分别执行启动链 w11 和链 w12 的脚本，若观察到形如

```
INFO [04-10|20:54:02.335] Block synchronisation started
---k:aaaaaaaaaaaaw1,v.RegionId:w1,v.Number:1---
---parent.Number:0, branchb.RegionId:w1,ptd:131072---
!!commitBranchBlock[aaaaaaaaaaaaw1][1]--[td:262144]success!!
```

字样，即为子区块链和父区块链同步成功，可以进行下一步骤的实验；

5. 另启动一个终端，运行branchnode-remastered.js脚本。该脚本将监视父区块链 w1 的日志内容，并根据之运行相应代码，完成转账等操作；

6. 在链 w11 和链 w12 中启动挖矿后，启动一个终端，执行node transfer_test_step1.js指令。该指令将从链 w11 的矿工账号，分别为链上的其他账号转账 10000 单位的资产作为初始资金，在接下来的步骤中，这些资产将被转移到链 w12 中的同名账号上；

7. 确认初始资金全部到位后，执行node transfer_test_step2.js，终端中将出现与挖矿提示line:--handler-TX_request--不同的输出，等待，直至终端仅输出挖矿提示；

8. 执行node query_transfer_time_w11_w12.js，脚本将访问链 w11 和链 w12 上的所有区块，统计其中包含的交易及其详细信息，生成测试结果报告。

3.5 测试结果分析

使用eth.getBalance(accountAddress)函数，可以在 Geth 的 JavaScript 控制台中年轻松地查看给定账号的余额，进而检查转账是否成功。本章所有测试均已确认在跨链转账结束后，原链 w11 中各账户的余额均为 0，而链 w12 中的对应账户余额为 10000 单位，从而证明了跨链转账功能的正确性。

由于测试设计为将账户余额从链 w11 转账到链 w12 中，故在生成的测试报告中，仅需关注tx_request_w12.txt和tx_result_w11.txt文件即可。前者记录了发起转账申请的时间戳，由于所有账号乃是同时发起转账申请，故所有条目的时间戳均相同；后者记录了各账户在链 w12 真正收到资产的时间戳。根据后者（即tx_result_w11.txt文件），可以轻松重建树状区块链串行处理所有账户的顺序，以及处理各个账户分别花费的时间。

3.5.1 小规模跨链转账实验结果分析

本文以 10 账号参与的跨链转账测试结果作为小规模跨链转账测试的测试结果。根据测试报告内容，所有 10 个账号均在时间戳 1683465655 发起转账申请，但在链 w12 上收到资产的时间戳不同，数据如下：

表 3-2 10 账号测试结果

账号公钥地址	收到资产的时间戳
0x4461e120a1bcbdc9e08730f59c7e169bac5de38f	1683465667
0x59cadf05182c56784b60960159c0fb4d16860d10	1683465680
0x8ed2d00a4ee496e51fab00ddc7561f85186e2a9c	1683465688
0x95fcbbba05858b53b829361a052450179d7a62ca	1683465694
0xcada164cb319316a133741dbaa1b40fcc8caec52	1683465703
0x1daf02e444bec7fc7fdbbac7704c57d001b19648	1683465711
0x023bc9309e89678b5de3ea084a5a91cc0679dd39	1683465720
0x4d326e5422c48ca1db8695bb59c9a58005a3fb44	1683465724
0x12d0e4381ef94a70a49252e35b9a65fadd3872b9	1683465735
0x0b424be2eb61a4fa045161198754613a93845857	1683465743
0xf41384cb20cd007daea6b0d7eefa3942ac44a3d1	1683465750

结合发起转账请求之时间戳，可以使用形如附录 C 的 Python 代码计算得到树状区块链为每个账户办理转账所花费的时间并可视化，如图 3-2 所示：

根据图 3-2 计算，得到如下测试数据：

观察图 3-2 不难发现，虽然 10 个账号的转账申请确实是同时发起的，但由于以太坊仅能串行处理的特性，导致从第一份转账请求发起，到最后一次转账交易完成

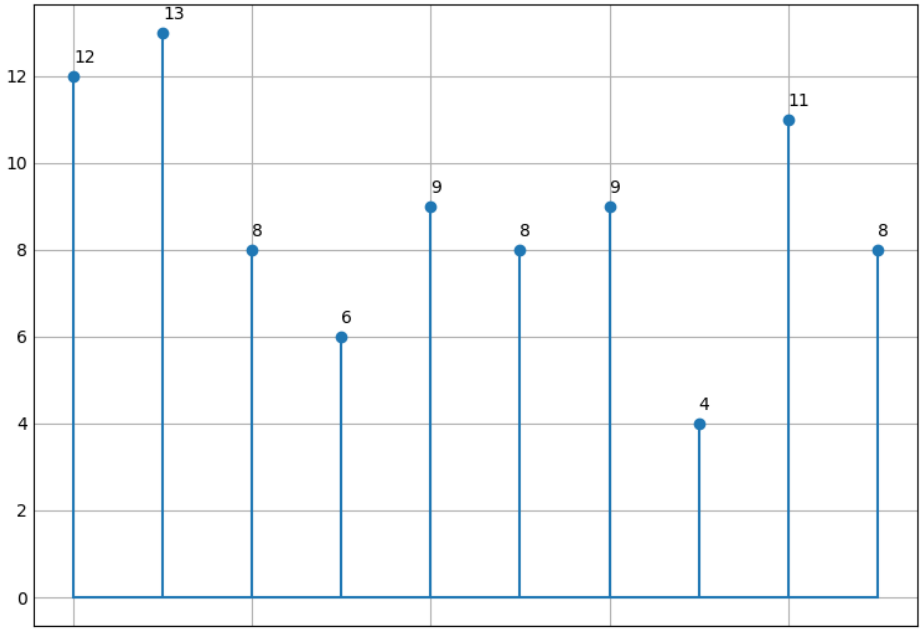

图 3-2 10 账号跨链转账测试的可视化

表 3-3 10 账号测试数据

总耗时（秒）	95
最快转账处理速度（秒）	4
最慢转账处理速度（秒）	13
平均转账处理速度（秒）	8.8000
转账处理速度方差（秒 ^{2}）	6.5600

并写入区块为止的总耗时较为夸张。同时，参与测试的 10 个账号之转账处理时间方差较大，最快转账处理速度较最慢处理速度的差距足有 7 秒。

3.5.2 大规模跨链转账实验结果分析

随着请求转账的账号数量增加，其转账处理效率是否会随之变化？本文继续以类似的方法，开展了 20 账号、40 账号、80 账号、120 账号、160 账号、200 账号的跨链转账测试。由于篇幅限制，本节将不展示可视化图示，仅展示经过计算得出的统计数据。

表 3-4 测试数据汇总

	20 账号	40 账号	80 账号	120 账号	160 账号	200 账号
总耗时（秒）	163	319	654	978	1363	1621
最快转账处理速度（秒）	4	2	1	2	1	1
最慢转账处理速度（秒）	16	17	21	17	27	21
平均转账处理速度（秒）	9.0556	8.6216	8.9589	8.5789	11.2645	8.7622
转账处理速度方差（秒 ^{2}）	8.0525	11.0460	19.0805	8.3666	25.9446	12.8407

观察表 3-4 的数据，可以提出以下猜想：

- 转账过程耗时和参与转账的账号存在线性关系；
- 虽然转账处理速度方差较大，但平均处理速度较为稳定，大约在 8.5 秒到 11.3 秒之间。

其中，第二个猜想可以从表 3-4 中较直观地得到，故本文将重点讨论第一个猜想的验证。

3.5.2.1 验证转账耗时和账号数量的线性关系

本文使用最小二乘法进行线性拟合计算。记账号数量为 x，假设 $time_\theta(x)$ 为 x 个账号跨链转账需要花费的时间，那么后者可以写作：

$$time_\theta(x) = \begin{bmatrix} 1 & x \end{bmatrix} \cdot \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix}$$

根据最小二乘法：

$$\vec{\theta} = (\vec{X}^T\vec{X})^{-1}\vec{X}^T \cdot \vec{Y}$$

其中，$\vec{X}$，$\vec{Y}$ 是分别为样本的输入向量和输出向量。根据以上算法，可得本例中的各个向量为：

$$\vec{X} = \begin{bmatrix} 1 & 20 \\ 1 & 40 \\ 1 & 80 \\ 1 & 120 \\ 1 & 160 \\ 1 & 200 \end{bmatrix} \quad \vec{Y} = \begin{bmatrix} 163 \\ 319 \\ 654 \\ 978 \\ 1363 \\ 1621 \end{bmatrix}$$

带入最小二乘法公式进行计算，可得：

$$\theta = \begin{bmatrix} -4.68767123 \\ 8.26794521 \end{bmatrix}$$

$$R^2 = 1 - \frac{\sum_i (y_i - \overline{y})^2}{\sum_i (y_i - times_{theta}(x_i))^2} = 0.9982362552443657$$

其中，x_i，y_i 代表 $\vec{Y}$ 的各个水平分量，$\overline{y}$ 代表 $\vec{Y}$ 的算术平均值。

拟合度 R^2 非常接近 1，这正证明了自变量——账号数量 x 和因变量——跨链转账耗时 $time_theta$ 确实可以在统计学上认为存在线性关系 $time_\theta(x) = -4.68767123 + 8.26794521 \cdot x$，进而验证了以太坊顺序串行处理收到的所有交易的特点。

3.6 基于测试结果进行数学建模

传统区块链单链结构的查询效率低，但胜在无需额外操作维护正确的账户状态；而树状结构的查询效率高，但引入了跨链转账的额外开销。根据使用场景的不同，用户需要在上述两种区块链实现中恰当进行选择，方能在特定的应用场合获得更好的使用体验。本节将基于已收集的测试数据，建立简单的数学模型，探讨在不同场景下使用树状区块链和传统区块链的理论性能差异，为用户在两种区块链实现之间的选择提供建议。

3.6.1 静态查询复杂度分析

静态查询复杂度分析，约束所有账号的地理位置不发生变化，因此不会考虑跨链查询的情况。本小节将基于以上约束，讨论单链结构区块链和树状区块链查询信息的复杂度情况。

在单链结构区块链下，所有链上信息均存储在同一条链中。若进行一次查询，最坏情况下需要遍历整条链才能获得结果。记总区块数为 n，则该过程的平均时间复杂度为 $O(n)$。

在树状区块链下，情况较为复杂，为简单起见，本节讨论一条父链，x 条子链组成的双层树状区块链，并假设所有区块均匀地分布在子链中。仍记总区块数为 n，那么每条子链中包含 $\frac{n}{x}$ 个区块。此时若进行一次查询，最坏情况下仅需遍历一条子链即可，平均时间复杂度为 $O(\frac{n}{x})$。

注意到当分母 x 越大，查询的时间复杂度越低。这是因为，在区块均匀分布的前提下，数状结构的深度随分支的增加而减少。结合树状区块链分支的实际意义，可以得到以下结论：

- 当链上交易发生的地理位置跨度较大，且在各地理位置范围分布较均匀时，适合使用树状区块链而非单链结构区块链；
- 当链上交易发生的地理位置非常集中时，树状区块链的表现和单链结构区块链接近，故无需使用树状区块链。

3.6.2 动态查询复杂度分析

动态查询复杂度分析，假设节点在树状区块链的各子链间周期性移动，从而将跨链这一开销纳入考量。本小节中，将针对节点中的一个账号进行分析。该账号行为描述如下：处于某一条子链中时，进行数笔笔交易，这些交易分别记录在不同的区块中。随后，账号立即转移前往下一个子链，此时若进行查询操作，必须先进行跨链转账，将该账户之余额转移到新子链上，然后再进行查询。

在单链结构区块链下，情况与静态查询情况类似，进行一次查询，最坏情况下仅需遍历一条子链即可，平均时间复杂度为 $O(n)$。

在树状区块链下，情况更为复杂。记 $lcm(c,q)$ 为账号跨链的间隔之间产生的区块数量 q 和查询间隔之间产生的区块数 c 的最小公倍数，那么在产生 $lcm(c,q)$ 个区

块的过程中，将发生 $\frac{lcm(c,q)}{c}$ 次查询，且账号将进行 $\frac{lcm(c,q)}{q}$ 次跨链移动。那么 $\frac{lcm(c,q)}{c}$ 次查询的总时间复杂度为 $O(q\times\frac{lcm(c,q)}{c})+\frac{lcm(c,q)}{q}\times T_{cross}$，其中 T_{cross} 为单个账户跨链转账的时间开销。那么，平均到每一次查询的时间开销即为 $(O(q\times\frac{lcm(c,q)}{c})+\frac{lcm(c,q)}{q}\times T_{cross})\times\frac{c}{lcm(c,q)}=O(q)+\frac{c}{q}\times T_{cross}$。

令 $lcm(c,q)=n$，比较两区块链实现在生成相同区块数量下的复杂度表现，列不等式：

$$O(lcm(c,q))\geq O(q)+\frac{c}{q}\times T_{cross}$$

由于在遍历长为 $length$ 的区块链链条时，可以认为找到目标区块的期望复杂度为 $\frac{length}{2}$；同时，经过实测，T_{cross} 的值可以取表 3-4 中跨链转账测试的平均处理速度的平均值（经过计算，为大约 9.2070 秒），故可以改写上述不等式为：

$$\frac{lcm(c,q)}{2}\geq\frac{q}{2}+\frac{c}{q}\times 9.2070$$

当满足上述不等式时，树状区块链将能提供相较传统区块链更优越的性能。

观察树状区块链的动态查询复杂度表达式可知，当查询非常频繁，即 c 的值变小时，复杂度将相应降低。

注意到，q 的增大在 $O(q)$ 中，对时间复杂度起到增加作用，却在 $\frac{c}{q}\times acc\times T_{cross}$ 中起到减少时间复杂度的作用。这是因为，增大 q 相当于容许子链拥有更长的长度，节点停留在同一子链中的时间延长，也就相应减少了跨链转账操作的次数。因此，即便是在树状区块链中，用户也需要合理设计子链的管辖范围，将节点跨链的频率控制在合理的区间内。

综上所述，在下列场景中，选择树状区块链将比选择单链结构区块链更优：

- 账号的物理位置变化范围不太大；
- 数据查询请求量较大。

3.7 本章小结

本章介绍了树状区块链为保证子链间数据一致性而生的新概念——跨链转账操作，介绍了该操作引入的额外时间复杂度。随后，设计并进行了一系列测试，按照压

力自小到大的顺序逐步验证了跨链转账操作的结果正确性、具体测量了该操作带来的额外时间开销，将其可视化并统计整理，进行统计学分析。在分析时，发现并合理利用一些最优化方法验证了参与转账的账户数量与转账耗时的线性关系，证明跨链转账这一操作为串行处理。最后，分别在静态和动态的场景下建立简单的数学模型，从理论与实际测量数据结合的角度比较了传统单链结构区块链和树状区块链的性能表现，并就在何场景下使用何者给出了一些建议。

第 4 章 基于树状区块链的出租车调度系统测试

第 5 章 改进树状区块链——从以太坊到 Substrate

树状区块链是在以太坊官方客户端 Go-Ethereum 的源代码上修改而来，因此，虽然在结构上做出了很大的调整，它也继承了许多 Go-Ethereum 的特点，例如共识算法和 EVM 虚拟机等特点，其性能表现也依然受制于 Go-Ethereum。从整体上评估，第三章的 3.5.2.1 节通过统计学方法，验证了以太坊顺序串行执行交易的特点，这样的执行策略使得以太坊在面对高并发请求时的处理效率不尽如人意；从局部评估，研究[8]表明，以太坊所使用的共识算法之一——基于工作量的证明（Proof of Work），其性能表现已落后其他更先进的算法。然而，以太坊并未在源代码层面留有太多的可扩展空间，这也意味着许多诸如更换共识算法，修改交易执行逻辑等的自定义修改在实践时困难重重，限制了在以太坊平台改良优化的空间。

Substrate[9]由 Parity Technologies 推出，是一套开源的区块链开发框架，允许开发者针对不同的用途对链进行不同程度的定制。在 Substrate 诞生前，人们花费了大量的精力，试图设计一个支持多链结构的新型区块链。然而，所有这些花费的时间、金钱和精力最终导向了一个结论：当下做出的深思熟虑的选择很可能成为未来的绊脚石。这是因为随着时间的推移，区块链依赖的某些特定的技术或假设，可能会阻碍并最终扼杀创新[10]。因此，以太坊创始人之一 Gavin Wood 成立了 Parity 技术公司，力图改写这一局面。他们的处女座——以太坊客户端 Parity，在相同的硬件配置环境下展现出了远胜 Go-Ethereum 的性能表现，提升幅度达到了可观的 89.8%[11]；在后续开发 Parity 自研的区块链 Polkadot 时，Gavin 意识到，仅需将 Polkadot 进行抽象，剥离部分细节，即能获得一个可扩展性极强，适用范围更广的区块链框架。在 2018 年，Polkadot 和用于开发它的区块链框架终于被分离开，成为两个独立的项目，而后者，即是本章讨论的主角——Substrate。

Substrate 在设计时，严格遵循三点原则：

- 将 Rust 编程语言作为代码库的核心编程语言。虽然 Rust 语言的学习曲线较为陡峭，但其极快的速度，极具辨识度的内存管理方式，灵活的抽象能力，以及可编译为 WebAssembly 的特点使它成为需要高性能表现，强内存安全性，及嵌入式设备友好性等特性之应用场景的不二之选；

- 将 WebAssembly 作为应用程序逻辑的执行环境。WebAssembly 是一种新型代

码，由万维网联盟创建，可从 Rust、C、C++ 等语言编译获得，且受到多种 JavaScript 引擎的广泛支持，具有良好的兼容性[12]。Substrate 的易升级性也建立于 WebAssembly 的基础之上：它将区块链的具体业务逻辑编译为 WebAssembly 字节码，并存储于区块链的数据存储区中，用户可以像发起普通交易一样发起一个申请修改链上存储的 WebAssembly 字节码的交易，从而便利地更新升级区块链系统；

- 广泛使用分层抽象、泛型实现和灵活的 API 作为主要的编码实践，并将库分离为不同的体系结构组件。在核心功能方面，Substrate 官方提供了许多不同的实现，例如数据库层的 RocksDB 和 ParityDB，共识层的 AURA 引擎和 Grandpa 引擎等，可以任由开发者选择；在应用功能方面，Substrate 允许开发者调用官方已开发妥当的模块 pallet 为他们的区块链添加自定义功能，例如保存并处理账号信息的 balances 模块，和管理智能合约的 contracts 模块；不仅如此，Substrate 也提供了这些模块的实现源代码，开发者可以自行下载并进行修改后引入区块链，实现功能的定制化。这一设计原则，赋予了 Substrate 极好的可扩展性，便于开发人员依据实际需要进行功能增删和优化改进等操作。

综上所述，将树状区块链自以太坊开发平台迁移至 Substrate 开发框架内，不仅能降低开发难度，获得更好的性能表现和安全性，还能获得更好的兼容性，令区块链能够在浏览器中乃至嵌入式设备上运行，为创造万物互联的世界贡献了一股坚实的力量。本章首先分析 Substrate 开发框架的逻辑结构，其次以官方提供的节点模板为例介绍其代码结构，最后在节点模板的基础上，引入树状区块链的部分特性——账号地理位置，以证明将树状区块链从以太坊开发平台迁移至 Substrate 开发框架的可行性。

结　论

本文结论……。[13]

结论作为毕业设计（论文）正文的最后部分单独排写，但不加章号。结论是对整个论文主要结果的总结。在结论中应明确指出本研究的创新点，对其应用前景和社会、经济价值等加以预测和评价，并指出今后进一步在本研究方向进行研究工作的展望与设想。结论部分的撰写应简明扼要，突出创新性。阅后删除此段。

结论正文样式与文章正文相同：宋体、小四；行距：22 磅；间距段前段后均为 0 行。阅后删除此段。

参考文献

参考文献书写规范

参考国家标准《信息与文献参考文献著录规则》【GB/T 7714—2015】，参考文献书写规范如下：

1. 文献类型和标识代码

普通图书：M　　会议录：C　　汇编：G　　报纸：N

期刊：J　　学位论文：D　　报告：R　　标准：S

专利：P　　数据库：DB　　计算机程序：CP　　电子公告：EB

档案：A　　舆图：CM　　数据集：DS　　其他：Z

2. 不同类别文献书写规范要求

期刊

[序号] 主要责任者. 文献题名 [J]. 刊名, 出版年份, 卷号 (期号): 起止页码.

[5] 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.

[8] 庄海燕. 基于私有区块链的共识算法性能分析[J]. 滨州学院学报, 2020(02): 63-68.

[12] Haas A, Rossberg A, Schuff D L, et al. Bringing the Web up to Speed with WebAssembly[J]. SIGPLAN Not., 2017, 52(6): 185-200.

普通图书

[序号] 主要责任者. 文献题名 [M]. 出版地: 出版者, 出版年. 起止页码. [14]

[13] 李成智, 李小宁, 田大山. 飞行之梦: 航空航天发展史概论[M]. 北京: 北京航空航天大学, 2004.

[14] Raymer, DanielP. Aircraft design: A Conceptual Approach[M]. Reston, Virginia: American Institute of Aeronautics, 1992.

会议论文集

[序号] 析出责任者. 析出题名 [A]. 见 (英文用 In): 主编. 论文集名 [C]. (供选择项: 会议名, 会址, 开会年) 出版地: 出版者, 出版年. 起止页码. [15]

[2] Madhura K, Mahalakshmi R. Usage of block chain in real estate business for transparency and improved security[C]//. 2022: 1-10.

[3] Aung N, Kechadi T, Zhu T, et al. Blockchain Application on the Internet of Vehicles (IoV)[C]//2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE). IEEE, 2022.

[11] Rouhani S, Deters R. Performance analysis of ethereum transactions in private blockchain[C]//2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2017: 70-74.

[15] 孙品一. 高校学报编辑工作现代化特征[C]//张为民. 中国高等学校自然科学学报研究会. 科技编辑学论文集 (2). 北京: 北京师范大学出版社, 1998: 10-22.

专著中析出的文献

[序号] 析出责任者. 析出题名 [A]. 见 (英文用 In): 专著责任者. 书名 [M]. 出版地: 出版者, 出版年. 起止页码. [16]

[16] 罗云. 安全科学理论体系的发展及趋势探讨[M]//白春华, 何学秋, 吴宗之. 21 世纪安全科学与技术的发展趋势. 北京: 科学出版社, 2000: 1-5.

学位论文

[序号] 主要责任者. 文献题名 [D]. 保存地: 保存单位, 年份. [17][18]

[17] 张和生. 嵌入式单片机系统设计[D]. 北京: 北京理工大学, 1998.

[18] Sobieski I P. Multidisciplinary Design Using Collaborative Optimization[D]. United States – California: Stanford University, 1998.

报告

[序号] 主要责任者. 文献题名 [R]. 报告地: 报告会主办单位, 年份. [19][20]

[19] 冯西桥. 核反应堆压力容器的 LBB 分析[R]. 北京: 清华大学核能技术设计研究院, 1997.

[20] Sobieszczanski-Sobieski J. Optimization by Decomposition: A Step from Hierarchic to Non-Hierarchic Systems[R]. NASA CP-3031, 1989.

专利文献

[序号] 专利所有者. 专利题名 [P]. 专利国别: 专利号, 发布日期. [21]

[21] 姜锡洲. 一种温热外敷药制备方案: 88105607[P]. 中国. 1989-07-26.

国际、国家标准

[序号] 标准代号. 标准名称 [S]. 出版地: 出版者, 出版年. [22]

[22] GB/T 16159—1996. 汉语拼音正词法基本规则[S]. 北京: 中国标准出版社, 1996.

报纸文章

[序号] 主要责任者. 文献题名 [N]. 报纸名, 出版年, 月 (日): 版次. [23]

[23] 谢希德. 创造学习的思路[N]. 人民日报, 1998-12-25(10).

电子文献

[序号] 主要责任者. 电子文献题名 [文献类型/载体类型]. 电子文献的出版或可获得地址 (电子文献地址用文字表述), 发表或更新日期/引用日期 (任选). [24]

[1] 马梅若. 数研所推出贸易金融区块链平台提升贸易融资效率助力经济快速发展[EB/OL]. 中国金融新闻网. (2020-09-10) [2023-04-24]. https://www.financialnews.com.cn/if/if/202009/t20200910_200546.html.

[4] Szabo N. Smart Contracts: Building Blocks for Digital Markets[EB/OL]. 1996 [2023-04-24]. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[6] Buterin V. 以太坊白皮书[EB/OL]. 2014 [2023-05-02]. https://ethereum.org/zh/whitepaper/.

[7] Go-ethereum Authors T. JavaScript Console[EB/OL]. 2023 [2023-05-02]. https://geth.ethereum.org/docs/interacting-with-geth/javascript-console.
[9] Technologies P. Home | Substrate[EB/OL]. 2023 [2023-05-02]. https://substrate.io/.
[10] Technologies P. Substrate Documentation[EB/OL]. 2023 [2023-05-02]. https://docs.substrate.io/.
[24] 姚伯元. 毕业设计 (论文) 规范化管理与培养学生综合素质[EB/OL]. 中国高等教育网教学研究. (2005-02-02) [2013-03-26]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/201201/P020120709345264469680.

关于参考文献的未尽事项可参考国家标准《信息与文献参考文献著录规则》（GB/T 7714—2015）

附　录

附录 A 创世配置文件

代码 A.1: 创世配置文件

```
{
    "config": {
        "chainId": 666,
        "homesteadBlock": 0,
        "eip150Block": 0,
        "eip150Hash": "0
x0000000000000000000000000000000000000000000000000000000000000000",
        "eip155Block": 0,
        "eip158Block": 0,
        "byzantiumBlock": 0,
        "constantinopleBlock": 0,
        "petersburgBlock": 0,
        "istanbulBlock": 0,
        "ethash": {}
    },
    "nonce": "0x0",
    "timestamp": "0x5ddf8f3e",
    "extraData": "0
x0000000000000000000000000000000000000000000000000000000000000000",
    "gasLimit": "0 xffffffff ",
    " difficulty ": "0x20000",
    "mixHash": "0
x0000000000000000000000000000000000000000000000000000000000000000",
    "coinbase": "0x0000000000000000000000000000000000000000",
```

```
22          " alloc ": {},
23          "number": "0x0",
24          "gasUsed": "0x0",
25          "parentHash": "0
    x0000000000000000000000000000000000000000000000000000000000000000"
26      }
27
```

一些关键字段的解释如下：

- gasLimit：区块链为防止恶意参与者不停发送交易耗尽服务器资源，往往都对交易进行“收费”。gasLimit 字段限制一次交易的最大花费。为保证实验成功，故此处设置得较大。
- difficulty：挖矿难度。难度越低，越容易挖到符合要求的新区块，出块速度也越高。
- alloc：记录链上部分账户的余额等信息。由于该创世配置文件乃是为尚未准备账户的全新区块链所准备，故此项为一个空白的 JavaScript 对象。

附录 B 合约部署的代码模板

代码 B.2: 合约部署代码模板

```
1   abi = JSON.parse("经过压缩转义后的ABI")
2   bytecode = "获得的字节码字符串"
3
4   Contract = web3.eth.contract(abi);
5   web3.eth.estimateGas({data: bytecode})
6   contractInstance = Contract.new({
7       from: web3.eth.accounts[0],
8       data: bytecode,
9       gas: '3000000',
10      position :"w2511111111111",
```

```
        txtime:277001
    }, function (e, contract){
        console.log(e, contract);
        if (!e){
            if (!contract.address) {
                console.log("Contract transaction send: TransactionHash: " +
contract.transactionHash + " waiting to be mined ...");
            } else {
                console.log("Contract mined! Address: " + contract.address);
                console.log(contract);
            }
        }
    });
```

附录 C 跨链转账测试的数据可视化代码

代码 C.3: 跨链转账测试的数据可视化

```
import matplotlib.pyplot as plt
from matplotlib.axes._axes import Axes
from matplotlib.figure import Figure
import numpy as np

plt.style.use('_mpl-gallery')

# make data
times: list[int] = [1683465655]
with open("tx_result_w11.txt", "r", encoding="utf-8") as f:
    times += [int(each.split('\t')[1]) for each in f.readlines()]

times.sort()
```

```
14
15      x = range(len(times) - 1)
16      y = [times[i] - times[i - 1] for i in range(1, len(times))]
17
18      # plot
19      fig, ax = plt.subplots()
20      fig: Figure
21      ax: Axes
22
23      stem = ax.stem(x, y)
24
25      # ax.set(
26      #     xlim=(0, 8), xticks=np.arange(1, 8),
27      #     ylim=(0, 8), yticks=np.arange(1, 8)
28      # )
29
30      for (i, j) in zip(x, y):
31          plt.text(i, j + 0.3, j)
32
33      # ax.bar_label(stem)
34
35      plt.show()
36
```

致　谢

值此论文完成之际，首先向我的导师……

致谢正文样式与文章正文相同：宋体、小四；行距：22 磅；间距段前段后均为 0 行。阅后删除此段。