

北京理工大学

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 4 月 24 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，区块被分为分支区块和叶子区块两种。叶子区块和传统的区块链并无太大差异，而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。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 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. 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

摘 要	I
Abstract	II
第 1 章 绪论	1
1.1 研究背景	1
1.2 二级题目	2
1.2.1 三级题目	2
第 2 章 另一个章节	4
2.1 代码片段	4
结 论	5
参考文献	6
附 录	8
附录 A L ^A T _E X 环境的安装	8
附录 B B _I Thesis 使用说明	8
致 谢	9

第1章 绪论

1.1 研究背景

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。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。

车联网技术（Internet on Vehicle）是物联网技术的子集

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，区块被分为分支区块和叶子区块两种。叶子区块和传统的区块链并无太大差异，而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。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，故有望为上述两个问题提供合理的解决方案。

1.2 二级题目

1.2.1 三级题目

正文.....[3].....[4]

正文部分：宋体、小四；正文行距：22 磅；间距段前段后均为 0 行。阅后删除此段。

图、表居中，图注标在图下方，表头标在表上方，宋体、五号、居中，1.25 倍行距，间距段前段后均为 0 行，图表与上下文之间各空一行。阅后删除此段。

图-示例：（阅后删除此段）



图 1-1 标题序号

表-示例：（阅后删除此段）

表 1-1 统计表

项目	产量	销量	产值	比重
手机	1000	10000	500	50%
计算机	5500	5000	220	22%
笔记本电脑	1100	1000	280	28%
合计	17600	16000	1000	100%

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（+、-、*、

、 \leq 、 \geq 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）

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

1.2.1.1 生僻字

第 2 章 另一个章节

2.1 代码片段

```
1 import numpy as np
2
3 def incmatrix(genl1,genl2):
4     m = len(genl1)
5     n = len(genl2)
6     M = None #to become the incidence matrix
7     VT = np.zeros((n*m,1), int) #dummy variable
8
9     #compute the bitwise xor matrix
10    M1 = bitxormatrix(genl1)
11    M2 = np.triu(bitxormatrix(genl2),1)
12
13    for i in range(m-1):
14        for j in range(i+1, m):
15            [r,c] = np.where(M2 == M1[i,j])
16            for k in range(len(r)):
17                VT[(i)*n + r[k]] = 1;
18                VT[(i)*n + c[k]] = 1;
19                VT[(j)*n + r[k]] = 1;
20                VT[(j)*n + c[k]] = 1;
21
22            if M is None:
23                M = np.copy(VT)
24            else:
25                M = np.concatenate((M, VT), 1)
26
27            VT = np.zeros((n*m,1), int)
28
29    return M
```

代码 2.1: Python Code

结 论

本文结论……。^[5]

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.

[3] 余雄庆. 飞机总体多学科设计优化的现状与发展方向[J]. 南京航空航天大学学报, 2008(04): 417-426.

[4] Hajela P, Bloebaum C L, Sobieszczanski-Sobieski J. Application of global sensitivity equations in multidisciplinary aircraft synthesis[J]. Journal of Aircraft, 1990, 27(12): 1002-110.

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. [6]

[5] 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.

[6] Raymer, Daniel P. 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. [7]

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

[7] 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. [8]

[8] 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. [9][10]

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

[10] 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. [11][12]

[11] 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.

[12] Sobieszcanski-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. [13]

[13] 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. [14]

[14] 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. [15]

[15] 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). [16]

[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) [2020-09-10]. https://www.financialnews.com.cn/if/if/202009/t20200910_200546.html.

[16] 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/hlwzbg/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

附录相关内容...

附录 A L^AT_EX 环境的安装

L^AT_EX 环境的安装。

附录 B B^IThesis 使用说明

B^IThesis 使用说明。

附录是毕业设计（论文）主体的补充项目，为了体现整篇文章的完整性，写入正文又可能有损于论文的条理性、逻辑性和精炼性，这些材料可以写入附录段，但对于每一篇文章并不是必须的。附录依次用大写正体英文字母 A、B、C……编序号，如附录 A、附录 B。阅后删除此段。

附录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。

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。