**分类号：××× U D C：D10621-xxx-(2023)xxxx-0**

**密 级：公 开 编 号：xxxxxxxxxx**

**成都信息工程大学**

**学位论文**

|  |  |
| --- | --- |
| **论文作者姓名：** | **唐建国** |
| **申请学位专业：** | **区块链工程** |
| **申请学位类别：** | **×××学士** |
| **指导教师姓名（职称）：** | **高琳（讲师）** |
| **论文提交日期：** | **2024年4月28日** |

**面向高校学分认证的区块链应用系统设计与实现**

**摘要：**在当前的高等教育领域中，学分认证是一项至关重要的任务。学分认证涉及到学生的课程成绩、教学计划等数据的管理和验证，以确保学生所完成的课程和学习成果的真实性和可信度。然而，目前的学分认证过存在一些问题，如手工审核成本高、认证结果可信度低等。区块链是一种分布式、不可篡改的数据存储和交易记录技术，它可以提供高度透明、安全和可信的数据管理机制。通过将学生的学分和学习成果以区块链的形式进行存证，可以确保数据的真实性和不可篡改性。

近年来，学术界和行业开始探索如何利用区块链技术改进学分认证系统。国外的研究者提出了一些解决方案，如利用区块链确保学习日志的准确映射，利用智能合约实现学分认证的自动化等。然而，国内在这方面的研究还相对较少，有待进一步深入探索和实践。

区块链技术可以自动化和诚信化学分认证过程，降低人工审核的成本，并提高认证的效率。通过智能合约等技术手段，可以实现自动化的认证流程，减少繁琐的人工操作，并为学生和学校提供便捷的认证服务。这样的系统设计和实现有助于提高学分认证的可信度和公信力。

本课题设计并实现一个面向高校学分认证的区块链应用系统。该系统的设计目标是解决目前学分认证过程中存在的问题，提高认证的效率和可信度，促进学生学习成果的真实性和公信力。通过引入区块链技术，希望能够确保学分数据的安全存储和不可篡改性，减少学校和学生在认证过程中的人工成本，并提供便捷的认证服务。

通过设计和实现面向高校学分认证的区块链应用系统，期望能够推动区块链技术在教育领域的应用与发展，为学生和教育机构提供更加高效和可靠的学分认证服务。

**关键词：**区块链技术；学分认证；智能合约；不可篡改；安全存储

**Design and implementation of blockchain application system for college credit certification**

**Abstract:** In the current field of higher education, credit accreditation is a crucial task. It involves the management and verification of student course grades and teaching plans to ensure the authenticity and credibility of the courses completed and the learning outcomes achieved. However, there are some issues with the current credit accreditation process, such as high manual auditing costs and low credibility of accreditation results. Blockchain is a distributed and immutable technology for data storage and transaction records, providing a highly transparent, secure, and trustworthy data management mechanism. By recording student credits and learning outcomes on the blockchain, the authenticity and immutability of the data can be ensured.

In recent years, the academic community and industry have begun to explore how to use blockchain technology to improve credit accreditation systems. Researchers abroad have proposed solutions such as using blockchain to ensure accurate mapping of learning logs and using smart contracts to automate the credit accreditation process. However, domestic research in this area is still relatively limited and requires further exploration and practice.

Blockchain technology can automate and ensure the integrity of the credit accreditation process, reduce the cost of manual audits, and enhance the efficiency of accreditation. Through technologies like smart contracts, an automated accreditation process can be implemented, reducing cumbersome manual operations and providing convenient accreditation services for students and schools. Such system design and implementation can help improve the credibility and public trust in credit accreditation.

This topic designs and implements a blockchain application system for university credit accreditation. The system's design goal is to solve the existing problems in the credit accreditation process, improve the efficiency and credibility of accreditation, and promote the authenticity and public trust of student learning outcomes. By introducing blockchain technology, it aims to ensure the secure storage and immutability of credit data, reduce the manual costs for schools and students during the accreditation process, and provide convenient accreditation services.

By designing and implementing a blockchain application system for university credit accreditation, it is hoped to promote the application and development of blockchain technology in the education sector, providing more efficient and reliable credit accreditation services for students and educational institutions.

**Key words:** Blockchain Technology; Credit Accreditation; Smart Contracts; Immutable; Secure Storage

目 录

[成都信息工程大学 1](#_Toc11185)

[面向高校学分认证的区块链应用系统设计与实现 I](#_Toc31151)

[关键词：区块链技术；学分认证；智能合约；不可篡改；安全存储 I](#_Toc24596)

[1 引言 3](#_Toc5242)

[1.1 课题背景 3](#_Toc30330)

[1.2 国内外研究现状 3](#_Toc28947)

[1.3 面向高校学分认证的区块链应用系统项目研究的意义 4](#_Toc1258)

[2 面向高校学分认证的区块链应用系统需求分析 5](#_Toc20019)

[2.1 目标 5](#_Toc29914)

[2.2 范围 5](#_Toc1680)

[2.2.1 用户管理： 5](#_Toc22750)

[2.2.2 学分认证申请和审批： 5](#_Toc16986)

[2.2.3 学分认证记录和查询： 6](#_Toc16547)

[2.2.4第三方企业或机构请求查询学生学分详情： 6](#_Toc16832)

[2.2.5 区块链技术和智能合约： 6](#_Toc1520)

[2.2.6 安全性和隐私保护： 6](#_Toc28792)

[2.3 用户的特点 6](#_Toc8839)

[2.3.1 学生用户： 6](#_Toc12953)

[2.3.2 教师用户： 6](#_Toc24080)

[2.3.3 系统管理员： 7](#_Toc7508)

[2.3.4 顶级系统管理员： 7](#_Toc23680)

[2.4 假定条件和约束限制 7](#_Toc8771)

[2.5 软件环境 8](#_Toc6297)

[3 面向高校学分认证的区块链应用系统的分析与研究 9](#_Toc10858)

[3.1 引言问题及国外研究现状的不足 9](#_Toc29551)

[3.2 提出的方法与改进 9](#_Toc17959)

[3.3 信息获取途径 9](#_Toc2331)

[3.4 论文结构与实施策略 10](#_Toc409)

[4 面向高校学分认证的区块链应用系统的概要设计 10](#_Toc15363)

[4.1编写目的 10](#_Toc10569)

[4.2 背景 11](#_Toc13149)

[4.3术语 12](#_Toc26908)

[4.4总体设计 12](#_Toc11996)

[4.4.1系统体系结构 12](#_Toc16343)

[4.4.2功能模块列表 13](#_Toc24738)

[4.4.3功能模块功能描述 15](#_Toc21435)

[5 面向高校学分认证的区块链应用系统的详细设计 17](#_Toc18416)

[5.1系统简介与目标 17](#_Toc22786)

[5.2系统架构 18](#_Toc6700)

[5.3关键技术 18](#_Toc322)

[5.3.1区块链技术 18](#_Toc29998)

[5.3.2安全性设计 18](#_Toc25356)

[5.4功能模块设计 19](#_Toc11519)

[5.4.1用户管理 19](#_Toc819)

[5.4.2学分管理 19](#_Toc22626)

[5.5数据库设计 19](#_Toc13730)

[5.6测试和部署 19](#_Toc6887)

[6 面向高校学分认证的区块链应用系统的实现 20](#_Toc31160)

[6.1智能合约核心实现 20](#_Toc24665)

[6.2golang核心实现 21](#_Toc22125)

[6.3系统重要界面 23](#_Toc7356)

[7 面向高校学分认证的区块链应用系统的测试 23](#_Toc7387)

[7.1测试环境搭建 23](#_Toc32069)

[7.2功能测试 24](#_Toc27620)

[7.3性能测试 25](#_Toc6629)

[结 论 28](#_Toc26105)

[参考文献 30](#_Toc29794)

[致 谢 32](#_Toc21092)

[声 明 33](#_Toc14619)

# 1 引言

## 1.1 课题背景

区块链技术的引入到学分认证领域，特别是在高等教育中的应用，可以大幅度改进和优化现有的学分认证流程。在传统的学分认证过程中，学生的学习记录和成绩常常需要通过多个教育机构和行政部门手动处理和转移，这不仅增加了时间和财务成本，还可能因人为错误或资料遗失而影响数据的准确性和完整性。

此外，随着在线教育和远程学习的兴起，学生越来越可能在多个教育机构中修读课程，这进一步增加了学分转移和认证的复杂性。在这种背景下，一个可靠且易于验证的学分认证系统显得尤为重要。区块链的特性，如去中心化、透明性以及数据的不可篡改性，正好满足了这一需求。通过将学分信息存储在区块链上，可以实现各教育机构之间的无缝数据共享和验证，极大提高了学分认证的效率和安全性。

利用区块链技术，学分认证系统可以自动记录和验证学生的每一个学习活动，从课程注册、成绩录入到最终的学分授予，所有过程都在区块链上进行记录，这些记录对所有参与方均开放、透明而且难以篡改。这样的系统不仅可以减少对人工审核的依赖，降低操作成本，还可以增强学生和教育机构对学分认证结果的信任。

## 1.2 国内外研究现状

在全球范围内，区块链技术在高等教育的学分认证领域逐渐引起了广泛关注。国外在这一技术的应用研究相对成熟，多个国家的高等教育机构已经开始探索使用区块链来管理和验证学生的学习成绩和学历。例如，美国、欧洲和澳大利亚的一些大学已经实施了基于区块链的系统来存储学术证书和学分转移信息。这些系统的目的是为了提供一个更加透明、有效和安全的方式来处理学分认证，确保学术记录的真实性和永久性。

在学术研究方面，国外的研究者已经提出并实验了多种区块链应用方案，包括使用智能合约自动执行学分转移规则，以及通过区块链保障学生个人数据的隐私和安全。这些解决方案不仅显示了区块链在提高学分管理效率方面的潜力，还突出了其在防止学术欺诈和提升教育质量方面的重要作用。

相比之下，国内关于区块链在学分认证应用的研究还处于起步阶段。尽管中国的一些高等教育机构开始认识到区块链技术的价值，但实际应用的案例较少，且多集中在理论探讨和小规模试点。国内研究的重点更倾向于区块链技术的基础研究以及在其他行业（如金融、供应链等）的应用。

## 1.3 面向高校学分认证的区块链应用系统项目研究的意义

本项目的研究对于推动区块链技术在中国高等教育领域的应用具有重要意义。首先，通过实施区块链系统，可以有效地解决学分认证过程中存在的问题，如数据管理低效、认证周期长、认证成本高、以及认证结果的可信度不足。区块链的不可篡改性和透明性能够确保学生学习成果的真实性和公信力，从而增强社会对高等教育认证结果的信任。

此外，该项目还将探索如何通过智能合约等技术自动化学分认证和转移流程，这不仅可以减少人工操作的复杂性和出错率，还可以提高整个教育系统的运行效率。此种自动化程度的提高，有助于加快学生跨学科、跨机构的学习路径，促进教育资源的开放与共享。

最后，本项目还将为国内外在类似领域的研究提供宝贵的实践经验和数据支持，有助于全球教育技术的发展和创新。通过这一研究，可以为中国乃至全球的教育管理提供一种全新的、基于区块链的解决方案，推动教育公平和高质量教育的实现。

# 2 面向高校学分认证的区块链应用系统需求分析

## 2.1 目标

本项目旨在设计和实现一个面向高校学分认证的区块链应用系统，以提供可靠、透明和安全的学分认证服务。该系统将利用区块链技术和智能合约来改进和简化学分认证过程，以满足以下目标：

1. 提高学分认证的透明性：通过区块链的分布式账本和可追溯性特性，学分认证过程将变得透明可验证。学生、教师和学校管理人员可以轻松查看和验证学分认证记录，确保其真实性和准确性。
2. 简化学分认证流程：利用智能合约和自动化机制，该系统将简化学分认证流程，减少繁琐的人工操作和纸质文档的使用，实现高效的学分认证流程。
3. 提升学分认证的安全性：区块链的去中心化和加密特性将增强学分认证的安全性。学分认证记录将被加密和存储在区块链上，防止篡改和伪造。同时，系统将采取适当的身份验证和访问控制措施，确保只有授权人员可以访问和修改学分认证数据。

4. 支持跨学校的学分认证：该系统将支持不同高校之间的学分认证互认。学生可以在不同高校之间转移学分，并获取相应的学分认证记录。这将提供更大的灵活性和便利性，促进学生的学习和发展。

## 2.2 范围

本项目旨在设计和实现一个面向高校学分认证的区块链应用系统，涵盖以下需求范围和简单的功能描述：

### 2.2.1 用户管理：

- 学生用户：注册学生账户，登录系统，查看个人学分认证记录，提交学分转移申请等。

- 教师用户：注册账户，登录系统，审批学生的申请，提供审批意见和结果。

- 系统管理员：注册系统管理员账户，登录系统，管理学生和教师账户。

### 2.2.2 学分认证申请和审批：

- 学生可以通过系统提交学分转移申请。

- 教师可以审批学生的学分转移申请，提供审批意见和结果。

- 学分认证申请和审批过程应该是透明的，学生和教师可以查看申请和审批的状态和历史记录。

### 2.2.3 学分认证记录和查询：

- 系统应记录学生的学分认证记录，包括认证的状态、认证时间和学分数目等信息。

- 学生可以查询和查看学分认证记录，以验证认证的准确性和真实性。

### 2.2.4第三方企业或机构请求查询学生学分详情：

- 第三方机构申请查询某学生的学分详情次数

- 学生批准请求

### 2.2.5 区块链技术和智能合约：

- 设计和实现一个区块链网络，用于存储学分认证记录和智能合约的执行。

- 利用区块链的分布式账本和智能合约特性，确保学分认证数据的安全性、可验证性和不可篡改性。

### 2.2.6 安全性和隐私保护：

- 系统应采取适当的安全措施，保护学生和教师的个人信息和学分认证数据。

## 2.3 用户的特点

本项目涉及的用户具有以下特点：

### 2.3.1 学生用户：

- 学术背景：学生用户是正在高校就读的学生，具有不同学科领域的学术背景。

- 学分认证需求：学生希望通过学分认证系统获得学分认证，以便在毕业或转学时能够顺利转移学分或获得学分互认。

### 2.3.2 教师用户：

- 教育背景：教师用户是高校的教职工，具有丰富的教育经验和学科专业知识。

- 学分认证审批：教师需要审批学生的学分转移申请，并提供审批意见和结果。他们的审批将影响学生的学分认证结果。

### 2.3.3 系统管理员：

- 管理权限：管理员是具有管理权限的用户，负责管理学生和教师账户，设置系统参数。

### 2.3.4 顶级系统管理员：

- 顶级权限：顶级管理员具有管理普通管理员的权限。

## 2.4 假定条件和约束限制

在设计和实现面向高校学分认证的区块链应用系统时，需要考虑以下假定条件和约束限制：

1. 技术条件：

- 区块链技术：项目基于区块链技术实现，需要有相关的技术专家和开发人员具备区块链开发经验。

- 智能合约开发：需要具备智能合约开发能力，以实现学分认证申请和审批的自动化执行。

2. 平台和环境条件：

- 网络连接：系统需要可靠的网络连接，以确保学生、教师和管理员能够顺利访问和使用系统。

- 安全性要求：系统需要在防止未经授权访问和保护用户隐私方面具备必要的安全措施。

3. 高校合作：项目实施需要与高校合作，获取学生学分认证相关数据，并与高校的学分认证政策和流程相对接。

4. 法律和合规性要求：

- 数据保护法规：系统需要符合适用的数据保护法规，确保学生和教师个人信息的合法处理和保护。

- 隐私保护：系统需要保护学生和教师的隐私，确保认证数据只能被授权人员访问和使用。

5. 学校政策和流程：

- 学分认证政策：系统需要根据不同学校的学分认证政策和要求，进行相应的配置和适配。

- 审批流程：系统需要支持学校的学分认证审批流程，并能够适应不同学校的审批规则和流程。

## 2.5 软件环境

1) 操作系统：

- 服务器端：可以选择适用于服务器环境的操作系统，Windows Server。

- 客户端：可以支持各种常见的操作系统，Windows。

2) 数据库系统：

- 可以选择适用于区块链应用系统的数据库管理系统，如MySQL。

3) 开发平台及工具：

- 区块链应用系统的设计和实现可能涉及到多种开发平台和工具，如：

- 区块链平台：可以选择适合的区块链平台，如Ethereum。

- 开发语言：可以使用多种编程语言进行开发，如Solidity。

- 集成开发环境：Visual Studio Code。

- 版本控制系统：可以使用版本控制系统，Git。

4) 通信协议：

- 在区块链应用系统中，与其他系统或组件之间的通信可能涉及到不同的通信协议，如HTTP、WebSocket等。

# 3 面向高校学分认证的区块链应用系统的分析与研究

## 3.1 引言问题及国外研究现状的不足

如引言所述，尽管区块链技术已被识别为高等教育中学分认证的一个潜在革新工具，它能够提供不可篡改的数据记录、提高透明度和数据安全性，但目前应用仍面临若干挑战。这些挑战主要包括技术的成熟度、缺乏教育领域特定的区块链实施标准、以及对区块链技术法规和政策的需求。

## 3.2 提出的方法与改进

基于智能合约的学分认证系统提供了一个框架，能够在处理学分数据时提供以下改进和特点：

1. 数据不可篡改性和透明度：

- 学分一旦被记录在区块链上，通过智能合约保证数据的不可修改性。这对于维护学术诚信至关重要。

2. 自动化的学分处理：

- 智能合约允许自动化的学分录入、认证和转移，减少了人工干预的需要，从而减少错误和提高效率。

3.学分验证和第三方访问：

- 提供了一种机制，允许教育机构或雇主通过智能合约验证学分的真实性，同时保护学生数据的隐私。

4. 跨机构互操作性：

- 学分转移功能支持跨机构的学分互认，通过智能合约确保转移的安全性和有效性。

## 3.3 信息获取途径

为确保研究的及时性和相关性，以下途径将用于获取区块链技术在教育领域的最新研究和应用情况：

1. 国内外学术文献：

- 定期访问学术数据库如 IEEE Xplore, ScienceDirect, 和 Google Scholar，获取最新的研究论文。

2. 网站新闻与行业动态：

- 关注专门报道区块链技术的网站，如 CoinDesk 和 Blockonomi，以及教育技术新闻。

3. 协会或公司研究报告与白皮书：

- 分析由领先的区块链技术公司和教育机构发布的研究报告和白皮书，例如 IBM 的研究报告和 Hyperledger 的技术白皮书。

## 3.4 论文结构与实施策略

通过结合智能合约的详细功能分析和针对现有研究不足的具体改进措施，本研究将系统地构建一个面向未来的高校学分认证框架。研究将依据从文献、新闻以及行业报告中得到的最新知识，不断调整和优化系统设计，以确保其实用性和前瞻性。

这种方法不仅回应了引言中提出的问题，而且提供了一个具体的解决方案框架，能够显著提高高等教育学分认证的效率和可靠性。通过实施这一基于区块链的系统，预期能够推动教育技术的进步，同时为全球教育领域提供一个可行的、创新的解决方案。

# 4 面向高校学分认证的区块链应用系统的概要设计

# 4.1编写目的

本份概要设计说明书的编写目的是提供一个清晰的概要设计文档，用于指导面向高校学分认证的区块链应用系统的设计与实现工作。该文档旨在为开发团队、技术架构师、项目经理和其他相关利益相关者提供一个全面了解系统设计的参考。

预期读者包括但不限于以下人员：

- 开发团队成员：包括开发人员、测试人员等。

- 技术架构师：负责系统架构设计和技术方案选择的专业人员。

- 项目经理：负责项目管理和协调的人员。

- 利益相关者：包括业务部门代表、高校管理人员、学生等。

该文档旨在为以上人员提供一个整体了解系统设计的基础，以便更好地理解系统的功能和特性，并为后续的详细设计和开发工作提供指导。

## 4.2 背景

本节将描述面向高校学分认证的区块链应用系统的背景，包括以下内容：

1) 需开发的软件系统的名称、英文缩写和项目编号（可选）；

- 软件系统名称：高校学分认证区块链应用系统

- 英文缩写（可选）：UCAS（University Credit Authentication System）

2) 任务提出者和开发者：

- 任务提出者：本系统是由一位论文指导老师提出的项目，其论文指导老师对学生的研究方向和项目提出进行指导和支持。

- 开发者：该系统的开发者为该毕业设计学生自己。学生将负责系统的设计、开发和实施，并在论文指导老师的指导下完成系统的相关工作。

3) 软件系统应用范围和用户：

- 应用范围：该系统旨在解决高校学分认证的问题，使用区块链技术确保学分认证的透明性、安全性和可靠性。

- 用户：主要包括以下几类用户：

- 学生：申请学分转移、查看学分认证状态、管理个人学分记录、批准第三方企业或机构申请。

- 高校教务老师部门：审核学生的学分转移申请、管理学生学分记录。

- 企业或组织：查询学生的学分认证状态和学术成绩，用于招聘和选拔。

- 系统管理员：参与管理老师，添加课程等。

该系统的目标是提供一个去中心化、透明且不可篡改的学分认证平台，改善传统学分认证过程中的信任问题和操作繁琐性，为学生、高校和用人单位提供更高效、可靠的学分认证服务。同时，该系统也是毕业设计项目的一部分，旨在展示学生在区块链应用系统设计与实现方面的能力和研究成果。

## 4.3术语

1) 区块链（Blockchain）：一种去中心化的分布式账本技术，通过分布式节点之间的共识机制，实现对交易和数据的不可篡改记录和验证。

2) 学分认证（Credit Authentication）：指高校对学生所修读的课程和取得的成绩进行确认和认可的过程。

3) 高校教务部门（University Academic Affairs Office）：负责学校教务管理和学生学籍管理的部门，负责审核和管理学生的学分认证申请和学分记录。

4) 用户界面（User Interface，UI）：系统与用户之间进行交互和信息传递的界面，包括视觉设计和用户操作方式。

5) 智能合约（Smart Contract）：一种以计算机代码形式编写的自动化合约，基于区块链技术实现交易和合约条款的自动执行和验证。

6) 去中心化（Decentralized）：指系统中的数据和决策权分散在多个节点或参与方之间，而非集中在单一机构或服务器上。

7) 透明性（Transparency）：指系统操作和数据的可见性和可追溯性，用户可以查看和验证系统的运行状态和数据记录。

8) 安全性（Security）：指系统的抵御攻击、保护数据和用户隐私的能力，包括数据加密、身份验证和防止篡改等措施。

9) 可靠性（Reliability）：指系统的稳定性和可信度，能够持续提供准确和可用的服务，并对错误和故障有恢复和容错机制。

1. 操作繁琐性（Operational Complexity）：指传统学分认证过程中，需要学生和教务部门进行大量繁复的操作和文件交换，增加了流程的复杂性和工作量。

## 4.4总体设计

### 4.4.1系统体系结构

体系结构决定领域问题结构设计的走向，是系统设计的蓝图。编制并描述系统的体系结构图，并说明系统的运行原理。



图4-1-1 系统分层结构

系统的运行原理：

- 用户注册登录系统，通过jwt token权限身份验证。

- 老师上传学生课程成绩以及取得学分等信息

- 学生可查看自己学分详情，也可以提交学分转移请求，以及可以批准第三方机构或企业查看自己的学分详情。

- 系统管理员可以添加移除老师，以及创建课程信息。

- 第三方机构或企业可以申请查看学生学分详情。

### 4.4.2功能模块列表

Backend Service Modules

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **模块编号** | **模块**  **名称** | **功能编号** | **需求功能** | **优先级别** |
| 1 | 用户管理 | 1.1 | 用户登录 | 高 |
|  |  | 1.2 | 用户注册 | 高 |
|  |  | 1.3 | 用户详情查询 | 中 |
|  |  | 1.4 | 获取所有用户 | 低 |
| 2 | 权限管理 | 2.1 | 添加管理员 | 高 |
|  |  | 2.2 | 移除管理员 | 高 |
|  |  | 2.3 | 添加老师 | 中 |
|  |  | 2.4 | 移除老师 | 中 |
| 3 | 通信管理 | 3.1 | 发送验证码 | 中 |
| 4 | 验证和授权 | 4.1 | 验证用户是否存在 | 中 |

Smart Contract Modules

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **模块编号** | **模块**  **名称** | **功能编号** | **需求功能** | **优先级别** |
| 1 | 权限控制 | 1.1 | 用户登录 | 高 |
| 2 | 学分管理 | 2.1 | 添加课程信息 | 高 |
|  |  | 2.2 | 查询课程信息 | 高 |
|  |  | 2.3 | 记录学分认证信息 | 高 |
|  |  | 2.4 | 查询学分详情 | 高 |
|  |  | 2.5 | 学分转移请求 | 高 |
|  |  | 2.6 | 批准学分转移 | 高 |
|  |  | 2.7 | 执行学分转移 | 高 |
|  |  | 2.8 | 学分转移记录查询 | 高 |
|  |  | 2.9 | 学分修改 | 中 |
|  |  | 2.10 | 学分撤销 | 中 |
| 3 | 第三方交互 | 3.1 | 第三方查询权限管理 | 中 |
|  |  | 3.2 | 查询所有已批准的第三方查询请求 | 低 |

### 4.4.3功能模块功能描述

#### 4.4.3.1后端服务功能描述

1. 用户管理

1.1 用户登录

允许用户使用用户名和密码登录系统。验证凭据，并为认证的访问提供会话令牌。

1.2 用户注册

为新用户提供注册界面。收集用户详细信息如电邮、姓名和密码，并在数据库中安全存储。

1.3 用户详情查询

根据公钥检索并显示用户的详细信息，确保敏感信息如密码不被输出。

1.4 获取所有用户

列出所有注册用户，显示他们的公开资料，包括姓名和联系信息等非敏感数据。

#### 4.4.3.2. 权限管理

2.1 添加管理员

为用户添加管理权限，允许他们管理课程和执行系统的行政任务。

2.2 移除管理员

从用户中移除管理权限，限制他们访问行政功能。

2.3 添加老师

为用户分配教师身份，使他们能够访问管理课程或学生成绩等与教学相关的功能。

2.4 移除老师

从用户中撤销教师身份，阻止他们访问教学功能。

3. 通信管理

3.1 发送验证码

向用户的电邮发送验证码，以便进行密码恢复或电邮验证等操作。

4. 验证和授权

4.1 验证用户是否存在

基于公钥检查系统中是否存在用户，这对于执行操作如密码重置或用户资料更新前的验证非常有用。

智能合约功能描述

1. 权限控制

1.1 管理员权限验证

确保诸如添加或删除课程，或修改学生学分等操作只能由具有管理权限的用户执行。

2. 学分管理

2.1 添加课程信息

在系统中注册新课程，详细记录课程ID、名称、学分和创建时间。

2.2 查询课程信息

根据课程ID检索课程的详细信息。

2.3 记录学分认证信息

在课程完成后记录或更新学生的学分信息，包括成绩和颁发机构的详细信息。

2.4 查询学分详情

提供学生学分的详细视图，便于透明度和验证。

2.5 学分转移请求

允许学生发起将学分转移到其他机构的请求。

2.6 批准学分转移

允许管理员批准学分转移请求。

2.7 执行学分转移

执行已批准的学分转移，相应地更新系统和区块链。

2.8 学分转移记录查询

提供所有学分转移活动的日志，用于审核和验证。

2.9 学分修改

允许授权的教师修改学分详情，反映成绩变更或学分撤销。

2.10 学分撤销

使管理员能够在出现差异或错误时撤销学分。

3. 第三方交互

3.1 第三方查询权限管理

管理第三方访问特定学生学分信息的权限。

3.2 查询所有已批准的第三方查询请求

列出所有已批准的第三方请求，确保透明度和记录保存。

# 5 面向高校学分认证的区块链应用系统的详细设计

## 5.1系统简介与目标

面向高校学分认证的区块链应用系统旨在提升学分管理的透明度和安全性，解决现有系统中存在的数据可篡改性和管理效率低下的问题。通过利用区块链技术的固有属性，如数据不可篡改、去中心化存储和智能合约自动执行，该系统能够有效地提高学分认证过程的可信度和透明度。本系统特别适用于处理学分转移、记录和认证等教育管理活动，为学生、教育机构和认证机构提供一个共享、可信的数据环境。

## 5.2系统架构

该系统采用前后端分离的架构设计，前端使用React技术栈构建，后端采用Go语言与Gin框架实现，区块链部分则基于以太坊平台的Solidity智能合约进行开发。

前端（React）：负责用户界面的设计和实现，通过调用后端API获取数据，并与智能合约交互，实现如登录、注册、查看学分、申请转移学分等功能。

后端（Go + Gin）：处理身份验证、数据处理、权限控制等服务器端逻辑。它接收前端请求，与数据库和区块链后端进行交互，执行业务逻辑后返回结果。

区块链（Solidity + 以太坊）：核心数据（如课程信息、学分记录）存储在区块链上，确保数据的不可篡改性和透明度。智能合约负责执行如学分添加、修改、查询和转移等操作。

## 5.3关键技术

### 5.3.1区块链技术

智能合约：开发智能合约来管理课程、学分认证等关键数据，利用区块链的不可篡改特性来增强数据安全。

以太坊平台：选择以太坊因其成熟的生态系统和广泛的开发者支持，智能合约使用Solidity语言编写。

### 5.3.2安全性设计

数据加密：敏感信息（如用户密码）在存储和传输过程中使用加密技术保护。

访问控制：系统通过基于角色的访问控制（RBAC），确保用户只能访问授权的数据和操作。

交易验证：所有区块链交易必须经过网络验证，确保交易的有效性和数据的正确性。

## 5.4功能模块设计

### 5.4.1用户管理

用户认证：实现用户的注册和登录功能，包括密码管理和令牌生成，确保用户身份的安全验证。

权限分配：根据用户的角色（学生、教师、管理员等），分配不同的访问权限。

### 5.4.2学分管理

学分记录：通过智能合约自动记录学生的课程成绩和学分。

学分查询：提供一个界面供学生和教师查询学分详情。

学分转移与认证：允许学分在不同教育机构间转移，并由智能合约处理转移后的认证过程。

## 5.5数据库设计

模型定义：定义用户、课程、学分等数据模型，以支持系统功能。

数据关系：使用关系型数据库管理用户和课程之间的关系，例如哪些学生参加了哪些课程，以及他们的成绩如何。

## 5.6测试和部署

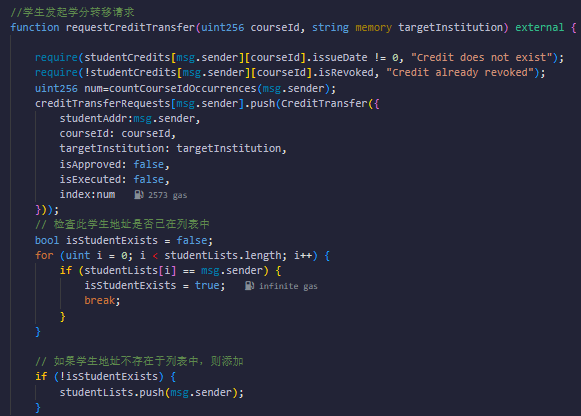
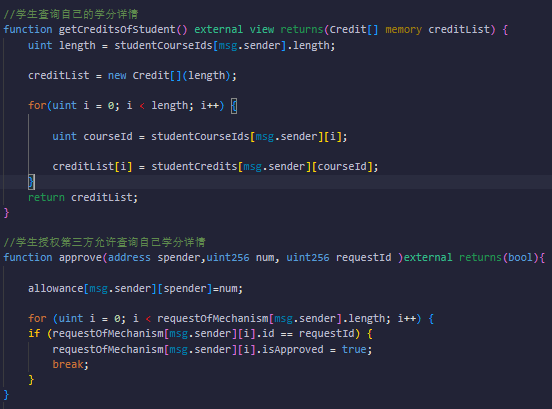
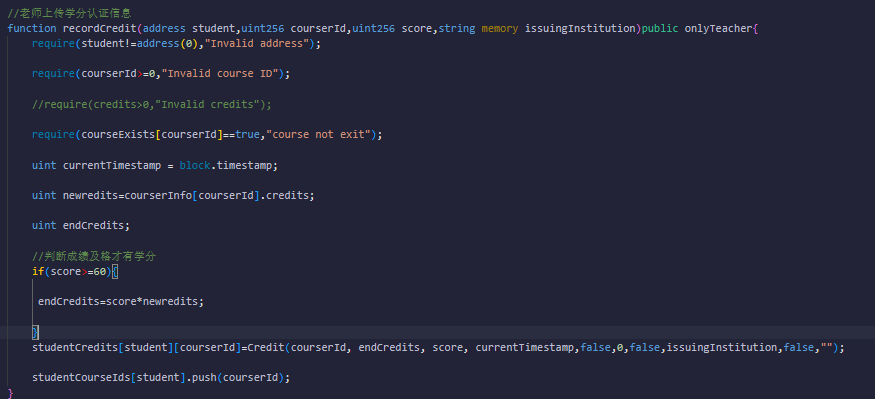
单元测试：对所有后端逻辑和智能合约代码进行单元测试。

集成测试：测试前端、后端和智能合约的集成，确保系统的整体功能按预期工作。

部署策略：详细说明如何将应用部署到生产环境，包括智能合约的部署和前后端服务的托管。

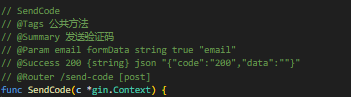
# 6 面向高校学分认证的区块链应用系统的实现

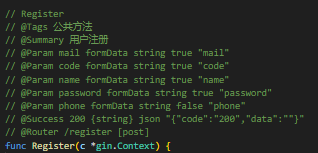
## 6.1智能合约核心实现

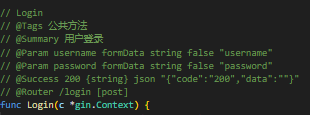


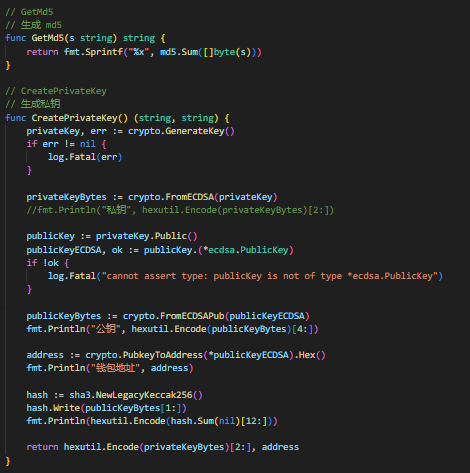
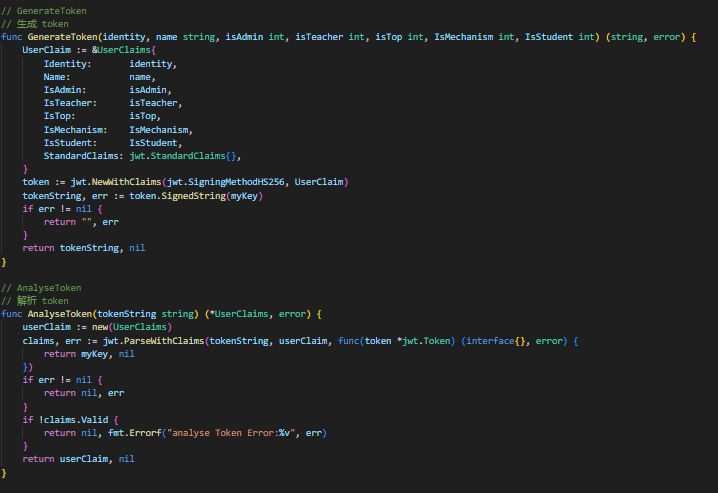
## 6.2golang核心实现

发送验证码：









## 6.3系统重要界面

# 7 面向高校学分认证的区块链应用系统的测试

## 7.1测试环境搭建

为确保面向高校学分认证的区块链应用系统的测试能够全面覆盖不同环境下的运行情况，下表列出了各种测试设备的硬件配置和软件配置，确保测试的有效性和全面性。

|  |  |  |
| --- | --- | --- |
| **设备名称** | **硬件配置** | **软件配置** |
| 服务器1 | Intel Xeon E5, 32GB RAM, 1TB SSD | Ubuntu 20.04 LTS, MySQL 8.0, Node.js 14, Ganache CLI |
| 服务器2 | Intel Xeon E5, 32GB RAM, 1TB SSD | Windows Server 2019, SQL Server 2019 |
| 开发工作站 | Intel i7-10700K, 16GB RAM, 512GB SSD | Windows 10 Pro, Visual Studio Code, Truffle Suite |
| 测试工作站 | Intel i5-9600K, 16GB RAM, 256GB SSD | Ubuntu 20.04 LTS, Docker, Jenkins, Postman |
| 移动测试设备1 | Apple iPhone 12, A14 Bionic, 4GB RAM | iOS 14, Mobile Safari |
| 移动测试设备2 | Samsung Galaxy S20, Exynos 990, 8GB RAM | Android 11, Mobile Chrome |
| 负载测试服务器 | AMD Ryzen 9, 64GB RAM, 2TB SSD | Ubuntu 20.04 LTS, Apache JMeter, LoadRunner |

表 1测试环境配置表

硬件配置解释：

服务器1 和 服务器2：高性能的服务器用于模拟生产环境，分别安装Linux和Windows操作系统，以测试应用在不同操作系统上的表现和稳定性。

开发工作站：配备高性能处理器和足够的内存，用于开发和初步测试智能合约以及应用程序代码。

测试工作站：配置适中的硬件，主要用于日常的功能测试和集成测试，安装有各种测试工具和环境。

移动测试设备：覆盖iOS和Android两大主流平台，确保移动端用户界面和功能的兼容性和性能。

负载测试服务器：专门用于执行性能测试，如模拟高并发访问，检测系统的承载能力和资源消耗情况。

软件配置解释：

操作系统：涵盖Linux和Windows，确保系统的跨平台兼容性。

数据库系统：包括MySQL和SQL Server，测试系统在不同数据库管理系统下的数据操作性能和一致性。

开发和测试工具：包括Visual Studio Code和Truffle Suite用于智能合约开发，Postman和JMeter用于API的功能和性能测试，Jenkins用于持续集成和部署。

移动操作系统和浏览器：确保应用在不同设备和浏览器上表现一致，特别是响应式设计和前端功能的兼容性测试。

## 7.2功能测试

在面向高校学分认证的区块链应用系统中，接口功能测试是确保各个系统组件正常交互的关键部分。以下是一个用表格形式给出的测试用例示例，它详细描述了各个接口的测试点。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **功能点** | **用例编号** | **测试标题** | **前置条件** | **输入及操作说明** | **预期结果** | **测试结果** |
| 登录接口 | TC\_001 | 测试正常登录 | 用户已注册 | 输入正确的用户名和密码 | 登录成功，返回用户信息 | 通过 |
| 登录接口 | TC\_002 | 测试密码错误登录 | 用户已注册 | 输入正确用户名和错误密码 | 登录失败，返回错误信息 | 通过 |
| 学分记录接口 | TC\_003 | 添加学分记录 | 用户登录，具有教师角色 | 输入学分详情，包括课程ID、学分、成绩等 | 学分记录成功 | 通过 |
| 学分记录接口 | TC\_004 | 添加无效学分记录 | 用户登录，具有教师角色 | 输入无效的课程ID或学分信息 | 学分记录失败，返回错误信息 | 通过 |
| 学分查询接口 | TC\_005 | 查询学生学分 | 学分记录已存在 | 查询指定学生的所有学分记录 | 返回学生的学分详情 | 通过 |
| 学分转移接口 | TC\_006 | 学分转移请求 | 学生登录，学分记录存在 | 请求转移学分到另一机构 | 学分转移成功 | 通过 |
| 学分转移接口 | TC\_007 | 学分转移请求失败 | 学生登录，学分记录存在 | 请求转移到不存在的学分 | 学分转移失败，返回错误信息 | 通过 |
| 学分审批接口 | TC\_008 | 审批学分转移请求 | 学分转移请求已提交 | 审批请求，同意转移 | 审批成功，更新学分状态 | 通过 |
| 用户注册接口 | TC\_009 | 用户成功注册 | 无前置条件 | 输入用户详细信息进行注册 | 注册成功，返回用户信息 | 通过 |
| 用户注册接口 | TC\_010 | 用户注册信息不完整 | 无前置条件 | 输入不完整的用户信息进行注册 | 注册失败，返回错误信息 | 通过 |

测试用例详解

登录接口测试（TC\_001, TC\_002）：验证用户可以通过正确的凭证登录系统，错误的密码应阻止用户登录，确保系统安全性。

学分记录接口测试（TC\_003, TC\_004）：确保只有授权的教师角色可以添加学分记录，且所有输入都必须验证其有效性。

学分查询接口（TC\_005）：测试系统能否正确返回请求的学分数据，包括对不同学生的查询处理。

学分转移接口（TC\_006, TC\_007）：验证学分可以被正确地从一个机构转移到另一个机构，或处理不合法的转移请求。

学分审批接口（TC\_008）：测试管理员对学分转移申请的审批过程。

用户注册接口（TC\_009, TC\_010）：确保用户可以注册新账户，同时测试系统如何处理不完整或无效的注册信息。

## 7.3性能测试

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **业务名称** | **性能测试需求** | **备注** |
| 1 | 用户登录 | 系统应能在2秒内响应登录请求 | 测试环境中模拟1000并发用户登录 |
| 2 | 学分记录添加 | 每个学分记录添加操作应在6秒内完成 | 同时测试智能合约执行时间 |
| 3 | 学分查询 | 学分查询响应时间不超过2秒 | 包括对单个学生和多个学生的查询 |
| 4 | 学分记录修改 | 修改操作应在6秒内完成，并确认数据正确性 | 修改测试涉及权限验证 |
| 5 | 学分转移 | 学分转移请求应在6秒内响应 | 测试在不同学院间的学分转移性能 |
| 6 | 学分转移审批 | 审批过程应在6秒内完成 | 测试审批流程的效率 |
| 7 | 大数据学分报告 | 生成报告的时间不应超过6秒 | 测试数据量在1000条以上 |
| 8 | 系统稳定性测试 | 系统应能连续运行24小时无故障 | 长时间运行检测内存泄漏等问题 |
| 9 | 前端页面加载 | 所有主要页面加载时间不应超过6秒 | 包括静态资源和动态内容的加载时间 |
| 10 | API吞吐量测试 | 系统API应至少支持每秒处理100个请求 | 特别测试学分添加和查询API |
| 11 | 数据库压力测试 | 数据库操作在高并发下的延迟应低于1秒 | 测试包括查询优化、索引效率和连接池配置 |
| 12 | 安全性能测试 | 系统对DDoS攻击和其他恶意攻击的响应时间应在1秒内 | 模拟各种网络攻击，测试系统的防护能力 |
| 13 | 移动端性能测试 | 移动端操作响应时间不超过3秒 | 包括登录、查询学分、提交学分转移请求等 |
| 14 | 高负载下的稳定性 | 在最大预期用户负载下，系统无明显性能下降 | 使用JMeter模拟高用户负载 |
| 15 | 并发用户支持 | 系统应支持至少5000名并发用户 | 测试系统在实际最高用户负荷下的表现 |

备注详解

用户登录：性能测试确保在高并发条件下，用户能快速登录系统。

学分记录添加和修改：关注智能合约的执行效率，以及系统如何处理并发的记录操作。

学分查询：由于频繁操作，优化数据库查询是此项测试的关键。

系统稳定性测试：通过持续运行测试，检查系统在长时间负载下的表现，关键是检测潜在的内存泄漏或资源溢出。

前端页面加载和移动端性能测试：确保用户在各类设备上的体验一致性和响应速度。

API吞吐量和数据库压力测试：确保后端服务可以处理大量请求，同时数据库能够有效地处理并发读写操作。

安全性能测试：评估系统抵御网络攻击的能力，确保在攻击情况下依然保持服务可用。

# 结 论

本研究成功设计并实现了面向高校学分认证的区块链应用系统，这一系统致力于解决当前高等教育领域在学分认证过程中存在的多个问题，包括高运营成本、流程复杂性、数据安全隐患以及认证效率低下。通过集成区块链技术，本系统在提高数据透明度和安全性的同时，实现了认证流程的自动化和智能化，极大地提升了学分认证的效率和可靠性。

理论贡献与技术创新：

理论与实践的结合：本研究不仅基于区块链技术的理论分析，还考虑了教育行业对数据可靠性和认证效率的具体需求，设计并实现了一个全新的应用模式。这一点展示了从理论到实践的转化，为区块链技术在教育行业的进一步应用探索了新路径。

系统设计的科学性和创新性：采用模块化的设计原则，系统高效地整合了用户界面、后端服务和区块链智能合约，每个模块承担明确的功能，保证了系统的高内聚性和低耦合性，便于未来的维护和扩展。

实际应用的显著效益：

操作效率的显著提升：自动化处理学分记录和认证过程显著降低了人工介入，减少了因手动处理引入的错误和延迟，从而提高了操作效率和数据准确性。

数据安全性和透明性的增强：利用区块链的不可篡改性，系统有效防止了数据被未授权修改的风险，增加了整个学分认证过程的透明度和信任度。

全面的系统测试与验证：

安全性和性能的全面验证：系统通过了包括安全性测试、性能测试、用户接受测试等多个层面的测试，验证了其在实际部署中的稳定性和可靠性。这些测试结果表明，系统能够在不同的操作条件和环境下稳定运行，满足高并发的用户需求。

用户体验的优化：前端设计注重用户体验，通过简洁直观的界面和流畅的交互流程，使得不同背景的用户均能快速熟悉并使用系统，从而提高了用户的满意度和系统的实用性。

未来研究与发展方向的拓展：

应用场景的拓展：未来的研究将探索将更多教育相关的活动和记录纳入区块链管理，如在线课程完成证明、学位授予过程等，进一步扩大系统的应用范围。

系统互操作性和扩展性的增强：研究如何通过技术创新提升系统与其他教育或认证系统的互操作性，例如通过实现区块链网络间的跨链通信，支持更广泛的数据共享和认证过程。

通过这些细致的设计、实现和测试，面向高校学分认证的区块链应用系统在技术创新和教育实践中均表现出了显著的优势。本系统的成功开发不仅为教育行业提供了一种全新的解决方案，也为区块链技术在更广泛领域的应用提供了宝贵的经验和示例。

# 参考文献

[1] Gräther W, Kolvenbach S, Ruland R., et al. Blockchain for education: life

long learning passport. ERCIM News. Proceedings of 1st ERCIM Blockchain

workshop 2018, European Society for Socially Embedded Technologies

(EUSSET) (2018).

[2] Li H, Han D. EduRSS: a blockchain-based educational records secure stor

age and sharing scheme. IEEE Access. 2019;7:179273–179289. doi:10.1109/

ACCESS.2019.2956157.

[3] Khandelwal H, Mittal K, Agrawal S, et al. Certificate verification sys

tem using blockchain. In: VK Gunjan, S Senatore, A Kumar, X-Z Gao, S

Merugu, editors. Advances in cybernetics, cognition, and machine learn

ing for communication technologies. Springer Singapore; 2020. p. 251–257.

doi:10.1007/978-981-15-3125-5\_27

[4] Rampell, C. The college degree has become the new high school degree.

The Washington Post. 2014. https://www.washingtonpost.com/opinions/

catherine-rampell-the-college-degree-has-become-the-new-high-school

-degree/2014/09/08/e935b68c-378a-11e4-8601-97ba88884ffd\_story.html

[5] Attewell P, Domina T. Educational imposters and fake degrees. Res Soc

Stratif Mobil. 2011;29(1):57–69. doi:10.1016/j.rssm.2010.12.004.

[6] Bear J, Ezell A. Degree mills: the billion-dollar industry that has sold over a

million fake diplomas. New York, USA: Prometheus Books; 2012.

[7] Bahrami M, Movahedian A, Deldari A. A comprehensive blockchain-based

solution for academic certificates management using smart contracts. 2020

10th International Conference on Computer and Knowledge Engineering

(ICCKE); 2020. p. 573–578. doi:10.1109/ICCKE50421.2020.9303656

[8] Malsa N, Vyas V, Gautam J, et al. Framework and smart contract

for blockchain enabled certificate verification system using robotics. In:

M Bianchini, M Simic, A Ghosh, RN Shaw, editors. Machine learn

ing for robotics applications. Springer Singapore; 2021. p. 125–138.

doi:10.1007/978-981-16-0598-7\_10

[9] Chen G, Xu B, Lu M, et al. Exploring blockchain technology and its

potential applications for education. Smart Learn Environ. 2018;5(1):1.

doi:10.1186/s40561-017-0050-x.

[10] Sharples M, Domingue J. The Blockchain and Kudos: a distributed system

for educational record, reputation and reward. In: K Verbert, M Sharples, T

Klobučar, editors. Adaptive and adaptable learning. Lyon, France: Springer

International Publishing; 2016. p. 490–496.

[11] Skiba DJ. The potential of blockchain in education and health care. Nurs

Educ Perspect. 2017;38(4):220–221. https://journals.lww.com/neponline/

Fulltext/2017/07000/The\_Potential\_of\_Blockchain\_in\_Education\_and.17.

aspx

[12] Berners-Lee T, Hendler J, Lassila O. The semantic web. Sci Am.

2001;284(5):34–43.

[13] Lalingkar A, Ramnathan C, Ramani S. Ontology-based smart learning envi

ronment for teaching word problems in mathematics. J Comput Educ.

2014;1(4):313–334. doi:10.1007/s40692-014-0020-z.

[14] Tsatsou D, Vretos N, Daras P. Adaptive game-based learning in multi-agent

educational settings. J Comput Educ. 2019;6(2):215–239. doi:10.1007/s40692

-018-0118-9.

[15] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized

Bus Rev. 2008;21260.

[16] Crosby M, Pattanayak P, Verma S, et al. Blockchain technology: beyond

bitcoin. Appl Innov. 2016;2(6–10):71.

[17] Wood DD. Ethereum: a secure decentralised generalised transaction ledger.

Ethereum Proj Yellow Pap. 2014;151(2014):1–32.

[18] Szabo N. Smart contracts. http://szabo.best.vwh.net/smart.contracts.html;

1994.

[19] Szabo N. The idea of smart contracts. Nick Szabo’s Pap Concise Tutor.

1997;6(1).

# 致 谢

在本论文的研究、设计和实现过程中，我得到了许多宝贵的指导和帮助。在此，我想对所有给予我支持和帮助的老师、同学和亲友表达我的诚挚感谢。

首先，我要特别感谢我的指导老师高琳导师，他以其丰富的经验和精深的学术造诣，为我的研究工作提供了宝贵的指导。在论文的选题、研究方法的确定以及实验设计等方面，高琳导师都给予了我细致的指导和无私的帮助。在我遇到研究难题和思想困惑时，高琳导师总能耐心地给予解答和指导，使我受益匪浅。

我还要感谢区块链产业学院的所有教师，他们的教诲和言传身教，为我打下了坚实的专业基础，使我能够顺利地完成这项研究。

同时，我也要感谢我的同学和朋友们，他们在论文撰写过程中给予了我很多帮助和鼓励。在数据收集和实验测试阶段给予了我大量的帮助，没有他们的支持，我无法顺利完成实验部分。

最后，我要感谢我的家人对我的学业和生活给予的理解和支持，是他们的鼓励和陪伴使我能够在学术道路上不断前行。

再次感谢所有帮助和支持我的老师、同学和家人，是你们的帮助和鼓励，让我的研究工作能够顺利完成。

作者简介：就读于成都信息工程大学区块链产业学院的一名学生

姓 名：唐建国 性别：男

出生年月：2001年12月22日 民族：汉

E-mail:1539994641@qq.com

# 声 明

本论文的工作是2024 年 2 月至2024 年 4 月在成都信息工程大学区块链产业学院完成的。文中除了特别加以标注地方外，不包含他人已经发表或撰写过的研究成果，也不包含为获得成都信息工程大学或其他教学机构的学位或证书而使用过的材料。

关于学位论文使用权和研究成果知识产权的说明：

本人完全了解成都信息工程大学有关保管使用学位论文的规定，其中包括：

（1）学校有权保管并向有关部门递交学位论文的原件与复印件。

（2）学校可以采用影印、缩印或其他复制方式保存学位论文。

（3）学校可以学术交流为目的复制、赠送和交换学位论文。

（4）学校可允许学位论文被查阅或借阅。

（5）学校可以公布学位论文的全部或部分内容（保密学位论文在解密后遵守此规定）。

除非另有科研合同和其他法律文书的制约，本论文的科研成果属于成都信息工程大学。

特此声明！

作者签名：唐建国

2024年4月28日