

广东财经大学试题纸

2025-2026 学年第 1 学期

课程名称 区块链技术

课程代码 21110062

课程班号 2023 级数管 1/2 班, 2023 级软工 1/2 班, 2023 计科 (20121311- 1/2) 共 1 页

课程论文 (100 分)

试根据本学期《区块链技术》授课内容及提供源代码项目, 组成1-4人的小组, 要求结合小组开发系统, 通过实践一个完整的区块链项目, 理解其技术架构、业务逻辑, 并能够批判性地分析其优劣与适用性。并根据自己小组分工, 查阅相关文献资料, 结合个人的学习兴趣, 阐述独特见解, 根据自己的分工情况独立撰写完成课程论文, 选题如下:

项目一 MetaCoin (以太坊基础通证)

1. 实践任务: 搭建与运行一个基础代币系统

核心目标: 在本地以太坊测试链上部署、发行并交易一个符合ERC-20标准的自定义代币。

具体任务:

- (1) 配置Truffle开发框架、Ganache私有链、MetaMask钱包。
- (2) 分析、编译并部署教材提供的MetaCoin智能合约。
- (3) 通过编写脚本或前端页面, 实现代币的转账、查询余额等核心功能。
- (4) 将合约地址添加到MetaMask中, 并成功进行一笔转账交易。

2. 课程报告要求: 从通证经济视角分析如下几个方面:

- (1) 技术解析: 详细解析ERC-20标准接口 (如transfer, balanceOf) 的代码实现, 并说明其重要性。
- (2) 流程阐述: 完整描述一笔代币转账交易从发起到确认的全过程 (涉及Gas、交易池、区块链确认)。
- (3) 核心分析: 论述“通证”与“货币”的本质区别。MetaCoin作为一个通证, 其价值支撑是什么?
- (4) 安全考量: 分析经典代币合约 (如The DAO) 曾出现过的安全漏洞, 并说明本项目合约如何规避类似风险。

项目二 以太坊通用积分系统

1. 实践任务: 构建一个可发行、消耗和兑换的积分体系

核心目标: 实现积分管理系统, 包含发行、消耗、查询和积分兑换商品等功能。

具体任务:

- (1) 部署积分合约, 并模拟平台方向多个用户地址发行初始积分。
- (2) 实现用户之间积分的转账功能。
- (3) 实现一个简单的消耗接口, 例如: 用户支付一定积分来兑换一个虚拟商品 (如“优惠券”)。
- (4) 在前端页面上清晰展示用户的积分余额和交易历史。

2. 课程报告要求: 剖析中心化与去中心化积分系统的优劣

- (1) 技术解析: 对比本项目合约与MetaCoin的异同, 重点分析新增的“积分消耗/兑换”逻辑及其权限控制 (如onlyOwner)。
- (2) 流程阐述: 描述积分从发行到最终被消耗的完整生命周期在链上是如何记录的。
- (3) 核心分析: 从成本 (Gas费)、效率 (TPS)、用户体验和信任角度, 全面对比基于区块链的积分系统与传统的中心化数据库积分系统各自的优劣。
- (4) 商业模式: 这种链上积分系统更适合哪种类型的商业场景? (如跨平台合作联盟)
- (5) 技术优化: 如何通过Layer 2扩容方案 (如Optimism) 来降低本系统频繁交易的手续费?

项目三 以太坊电子优惠券系统

1. 实践任务：实现一个防伪造、可验证的优惠券系统

核心目标：实现优惠券的创建、领取、验证和核销全流程，确保每张优惠券的唯一性与真实性。

具体任务：

- (1) 部署优惠券合约，商家账户可以创建一批具有固定面额和数量的优惠券。
 - (2) 实现用户领取功能，确保每人限领一张，且总数不超过发行量。
 - (3) 实现商家验证并核销优惠券的功能，确保优惠券不能被重复使用。
 - (4) 开发一个简单的验证页面，模拟商家扫描用户二维码完成核销的过程。
2. 课程报告要求：聚焦于防伪与数字资产的确权
- (1) 技术解析：分析合约如何通过mapping或NFT（ERC-721）来保证每张优惠券的唯一性，并防止重复领取和重复核销。
 - (2) 流程阐述：详细说明“领取-验证-核销”过程中，每一次状态变更在链上产生的交易和事件（Event）。
 - (3) 核心分析：为什么区块链在解决电子券防伪和双花问题上比中心化数据库更具优势？
 - (4) 隐私与成本：讨论将优惠券信息完全公开在链上可能带来的隐私和成本问题，并提出可能的混合架构解决方案（如关键哈希上链，详细信息链下存储）。
 - (5) 互联互通：如何设计该系统，才能让不同商家发行的优惠券在一个统一的平台上进行流转和兑换？

项目四 Fabric社会文物管理平台

1. 实践任务：搭建一个联盟链文物溯源与存证平台

核心目标：在Hyperledger Fabric网络上部署链码，实现文物的登记、流转、鉴定和查询功能。

具体任务：

- (1) 搭建一个多组织的Fabric测试网络（至少包含博物馆、鉴定机构两个组织）。
 - (2) 部署文物管理链码，模拟博物馆登记一件文物（记录名称、年代、图片哈希等）。
 - (3) 模拟鉴定机构对文物进行鉴定，并更新其状态。
 - (4) 模拟文物在多个博物馆之间的流转过程，并确保流转历史不可篡改。
 - (5) 编写客户端应用，实现对文物全生命周期信息的查询。
2. 课程报告要求：探讨联盟链在建立多方信任中的作用
- (1) 技术解析：阐述Fabric的通道机制、隐私数据集合和背书策略在本项目中是如何设计并应用的，以满足不同机构间的数据隐私与共享需求。
 - (2) 流程阐述：详细描述一条“文物从A博物馆流转到B博物馆”的交易，在Fabric网络中从提案到提交的完整流程。
 - (3) 核心分析：对比公有链，为什么联盟链架构（如Fabric）更适合此类文博管理场景？
 - (4) 信任机制：区块链如何解决文物领域长期存在的“真伪难辨”和“流传无序”的信任难题？
 - (5) 链上链下结合：文物的高清图像、3D扫描数据等大文件如何处理？阐述IPFS等存储方案与本系统结合的架构设计。

项目五 Fabric高端食品安全系统

1. 实践任务：构建一个食品溯源系统

核心目标：实现高端食品在生产、加工、物流、销售各个环节信息的上链与溯源。

具体任务：

- (1) 搭建一个包含供应商、加工厂、物流商、零售商的多节点Fabric网络。

- (2) 部署食品溯源链码，定义关键数据结构。
 - (3) 模拟各参与方依次调用链码，更新食品的状态。
 - (4) 实现一个面向消费者的溯源查询界面，通过扫描商品二维码，即可查看其完整的流转历史。
2. 课程报告要求：分析区块链在供应链协同中的价值
- (1) 技术解析：分析链码中如何通过复合键来高效地组织和查询某一批次或某一具体产品的所有相关记录。
 - (2) 流程阐述：以一个具体食品为例，画出其信息在各个环节被写入区块链的序列图。
 - (3) 核心分析：区块链技术如何重塑供应链各参与方之间的协作关系？是解决了“信息不对称”还是“信任不对称”？
 - (4) 如何保证上链的数据本身就是真实的？探讨区块链与物联网设备结合的可能性（如温湿度传感器自动上链）。
 - (5) 商业与监管价值：除了提升消费者信任，该系统对企业的供应链管理和政府的食品安全监管有何具体价值？

研究性题目

本课程论文旨在考查学生对区块链核心技术与前沿动态的深入理解能力、问题分析能力以及学术研究能力。从以下两个题目中任选其一，完成一篇具有独立见解和分析深度的课程论文。

题目一：调研一个真实的智能合约漏洞事件，分析其原因和影响。

1. 核心目标：通过一个真实案例，深入理解智能合约的安全性问题，并掌握漏洞分析的基本方法论。

2. 具体要求：

(1) 案例选择与背景介绍（10%）

选择一个真实发生且具有重大影响智能合约安全事件（如 The DAO 事件、Poly Network 攻击、Parity 多签名钱包漏洞等）。

清晰阐述该合约或平台的设计目标、业务逻辑及其在生态中的重要性。

(2) 漏洞技术原理深度剖析（40%）

漏洞定位：明确指出漏洞的具体类型（如重入攻击、整数溢出、访问控制缺失、逻辑缺陷等）。

根本原因分析：结合代码片段（可使用Solidity代码示例图）和合约状态机，详细解释漏洞产生的技术根源。例如，对于重入攻击，需说明 `call.value()` 与 `fallback` 函数的交互机制为何导致了递归调用。

攻击流程再现：以流程图或序列图的形式，一步步还原攻击者利用该漏洞完成攻击的完整路径。

(3) 影响与后果分析（20%）

直接损失：量化分析造成的经济损失（如被盗资产金额）。

系统性影响：分析该事件对项目本身、所在公链（如以太坊）、整个DeFi生态以及市场信心的冲击。

社区与行业响应：描述项目方、社区以及安全团队是如何应对该事件的（如分叉、白帽黑客干预等）。

(4) 启示与防护方案设计（20%）

技术启示：总结从该事件中应吸取的技术教训。

防护方案：系统性提出防范此类漏洞的技术方案与实践建议。例如：如何正确使用检查-效果-交互模式、推荐使用经过审计的安全库（如OpenZeppelin Contracts）、采用形式化验证与静态分析工具等。

(5) 报告撰写与规范性 (10%)

结构清晰，逻辑严谨，语言流畅；图文并茂，引用规范，数据来源可靠。

题目二：研究以太坊2.0实施过程中遇到的技术挑战和解决方案。

1. 核心目标：系统性地理解以太坊从PoW到PoS的宏大技术变迁，掌握其核心组件的设计哲学与工程权衡。

2. 具体要求：

(1) 以太坊2.0架构概述 (10%)

清晰阐述以太坊2.0（共识层）的分阶段路线图（Phase 0, 1, 2）。

准确描述其核心架构组件：信标链、分片链、执行层（原Eth1）与共识层的合并。

(2) 核心技术挑战与解决方案深度分析 (50%)

选择2-3个最具代表性的技术挑战进行深入分析。建议包括但不限于：

共识机制转变：从PoW到PoS（Casper FFG & LMD-GHOST）的挑战，如何设计激励与惩罚（Slashing）机制以保证网络安全和活性？

分片技术：如何实现安全的跨分片通信？如何分配验证者到不同分片以保证安全性与去中心化？

状态管理：无状态性、状态到期等方案是如何解决状态爆炸问题的？

合并：如何实现PoW链与PoS信标链的“无缝”合并？面临哪些复杂的协调与同步问题？

对于每一个挑战，需详细说明：

挑战的本质：该问题为何难以解决？（如“不可能三角”的权衡）；

采用的解决方案：以太坊基金会和社区提出了何种创新性方案（如委员会机制、BLS签名聚合、Merkle树等）？

方案的评价：分析该方案的优缺点及所做的工程妥协。

(3) 影响与意义分析 (20%)

性能提升：分析以太坊2.0在可扩展性、安全性（抗51%攻击）和能源效率方面的预期提升。

生态与行业影响：探讨此次升级对DApp开发者、用户以及整个区块链竞争格局的深远影响。

(4) 未来展望与潜在风险 (10%)

基于现有方案，展望以太坊在完成升级后仍面临的潜在技术挑战（如量子计算威胁、中心化风险等）。

提出个人对以太坊未来技术发展方向思考。

(5) 报告撰写与规范性 (10%)

结构清晰，逻辑严谨，能够将复杂的技术概念解释清楚；引用权威技术文档、EIP提案和学术论文，信息准确无误。

课程论文提交时间：本学期最后一次上课时间。

课程论文的文本格式：要求按照《广东财经大学普教本科课程考核管理规定（试行）》的文件格式要求。

课程论文基本格式：遵循学术论文格式，包含摘要、关键词、引言、正文、结论和参考文献。

论文名称：题目根据给定选题拟定，字数限20 字（居中）

摘 要：摘要内容（文章中心要点，不超过三百字）（居左顶格）

关键词：（一般控制在五个词以内，关键词之间用空格间隔）（居左顶格）

正文：正文不少于4000字。首先，给出选题意义和研究背景，然后，在论文主体部分进行区块链设计，给出区块链技术相关图表，并用文字说明该图表的功能，图表要给出中文标题；系统实现部分给出自己所负责的主要界面截图和简短关键代码，需要给出相应功能描述和分

析；最后结论部分总结该论文主要内容和后续需要完善功能和改进的部分。

参考文献：给出3-5篇参考文献。

课程论文书写格式：

根据提供答题纸（格式二）模板完成课程论文。

正文中间标题用小二号黑体加粗，正文用四号宋体。文字标点符号规范，修辞精准，内容完整，格式符合规范。