**《区块链与分享型数据库》教学大纲**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程代码** | **DATA0031132996.01** | **课程性质** | | **专业选修** |
| **课程名称：** | **区块链系统与分享型数据库** | | | |
| **英文名称** | **Blockchain System and Sharing Database** | | | |
| **学时/学分** | **72/3** | **其中实验/实践学时** | **36** | |
| **开课单位** | **数据科学与工程学院** | **适用专业：** | **数据科学与大数据技术** | |
| **先修课程** | **计算机系统、操作系统、计算机网络** | | | |
| **大纲撰写人** | **张召** | **大纲审核人** | **钱卫宁** | |
| **课程网址** | **无** | **授课语言** | **中文** | |

注：课程性质选择下列类别之一：学科基础、大类平台、专业必修、专业选修、教师教育

一、课程说明

作为一种由互不可信的多方共同维护的分布式账本，近年来区块链技术受到了越来越多的来自工业界和学术界的关注。本课程作为系统主要从数据管理的角度，剖析区块链系统所涉及到的基本原理与关键技术，以及其与传统分布式数据库之间的关联。具体授课内容包括典型的区块链系统介绍、密码学基本原理、分布式一致性原理、共识协议，以及基于默克尔树的数据存储与组织等。

二、课程目标

本课程的主要目标是使学习者能够全面掌握区块链系统的基本概念、原理和关键技术，并能在此基础上完成基于现有区块链平台的区块链应用系统开发，也能深入理解区块链系统开源代码，对现有开源区块链平台进行功能扩展和性能提升。具体的课程目标包括如下几点：

目标1：能够全面准确了解区块链系统的发展历史、基本概念、架构和工作原理。（支撑毕业要求1，2，3, 5）

目标2：能掌握和理解区块链系统的关键核心部件，以及涉及到的关键核心技术。 （支撑毕业要求2，3, 4, 5）

目标3：能够基于现有的区块链平台开发区块链应用系统。（支撑毕业要求2, 4）

目标4：能够理解开源区块链系统的源代码，并在此基础上对开源平台进行必要的功能扩展和性能提升。（支撑毕业要求2，4，5）

三、课程目标与毕业要求的对应关系

|  |  |  |
| --- | --- | --- |
| **毕业要求** | **指标点** | **课程目标** |
| 1.理想信念坚定 | 具有正确的价值观和道德观，爱国、诚信、守法； | 课程目标1 |
| 具有高度的社会责任感和良好的协作精神； |
| 具备工科学生所需要的科学精神和人文社会科学素养。 |
| 2.专业技能扎实 | 掌握工科学生所必须的数学知识； | 课程目标1,2,3,4 |
| 掌握数据科学与工程的基础知识，包括相关的计算机、统计与应用数学、信息系统的基础知识； |
| 掌握数据分析和机器学习的基本模型和算法。 |
| 3.学科理念先进 | 深刻理解数据的获取、建模、管理、利用的全生命周期，深刻理解数据科学与工程相关技术发展与社会经济发展的关系； | 课程目标1，2 |
| 深刻理解数据对于社会经济发展的赋能作用，了解金融、物流、零售、制造等领域的典型应用的技术问题并掌握主要解决方法。 |
| 4.工程能力全面 | 掌握主要的数据管理和处理工具以及系统平台的使用，熟知它们的特点、系统架构，具备基本的数据系统的设计和开发能力； | 课程目标3，4 |
| 了解大数据应用中需求分析、数据和应用建模、系统选型、应用设计、开发和实施的过程，具备合作进行系统和应用研发能力； |
| 掌握开源软件的设计和开发方法，掌握云计算平台的使用技术，掌握基于云计算的应用设计、开发、实施、运维方法与技术； |
| 具备参与数据系统或数据应用设计、开发、运维工程所需的沟通交流与协作能力，掌握基本的工程管理知识与能力。 |
| 5.研究能力突出 | 了解“数据科学与工程”学科领域，以及相关应用领域的技术发展前沿； | 课程目标1，2，4 |
| 具有初步的从事数据科学与工程研究工作的科学训练，具有从事相关学科科学研究、教学或工程开发的技术工作的能力。 |

四、教学内容与学时安排

1. **绪论 （支撑课程目标1，2）**

学时：理论4、实验4

1. 比特币系统介绍
2. 从数据管理的角度解读区块链系统

学生要求：了解区块链系统相关的基本概念，以及其跟分布式数据库的关系。

实验：使用JAVA语言编写minichain，模拟比特币系统的功能。

1. **以太坊系统 （支撑课程目标1，2，3）**

学时：理论6、实验6

1. 以太坊的架构、基本概念和原理
2. 基于以太坊的智能合约开发

学生要求：掌握以太坊的部署、架构和工作流程

实验：能基于以太坊编写智能合约。

1. **超级账本Fabric （支撑课程目标1，2，3）**

学时：理论6、实验6

1. Fabric的系统架构、基本概念和原理
2. 基于Fabric的智能合约开发

学生要求：掌握Fabric的部署、架构和工作流程

实验：基于Fabric编写链码

**第四章：密码学基础 （支撑课程目标2，4）** 🞛

学时：理论4、实验4

1. 加解密算法
2. 数字签名、国密算法，以及PKI基础介绍

学生要求：掌握加解密算法和数字签名的基本原理，密码学基础设施的工作机制，以及在区块链系统中的使用。

实验：熟悉各种密码学库，并能在区块链系统中熟练使用

**第五章：共识算法 （支撑课程目标2，4）** 🞛

学时：理论9、实验9

1. 分布式一致性原理
2. Paxos和RAFT算法
3. PBFT算法

学生要求：掌握分布式系统的基本原理和各种类型的共识算法

实验：实现RAFT和PBFT算法

**第六章 数据存储与验证 （支撑课程目标2，4）**

学时：理论3、实验3

1. 区块链存储概述
2. Merkle树及其变种的存储结构

学生要求：理解区块链系统的数据存储组织方式

实验：实现Merkle树及其上的可验证查询

**第七章 总结（支撑课程目标1、2、3、4）**

学时：理论4、实验4

1. 课程总结
2. 课程答疑

要求学生：回顾课程内容，梳理课程内容之间的内在逻辑关系

实验：完成课程大项目

五、教学方法

以课堂讲授为主，个别章节会增加讨论环节。理论课程的讲授主要结合多媒体课件，采用线下教学方式，依托钉钉课程群进行课程资源发布、作业收集，课后答疑等。实践部分在线下机房展开，简单讲授实践内容后，同学们进行实践，实践过程碰到问题后再逐个答疑。理论教学结合实践教学，相辅相成，加深对课程内容的理解，提高对知识的运用能力。在讲授过程中采用“回顾”、“启发”、“讲授”、“讨论”、“总结”和“答疑”的序列对课堂内容进行有效组织，着重培养学生的独立思考能力和工程实践能力。

六、考核方式

课程考核由平时成绩和期末大项目组成，分别占50%、50%，详见下表。

|  |  |  |  |
| --- | --- | --- | --- |
|  | **考核方式** | **占该项比例** | **占总评比例** |
| **平时成绩** | 考勤 | 10% | 5% |
| 课堂表现 | 10% | 5% |
| 以太坊编程作业 | 30% | 15% |
| **Fabric**编程作业 | 30% | 15% |
| 底层平台编程作业 | 20% | 10% |
| **期末成绩** | 课程大项目 | 100% | 50% |

课程目标与考核方式对应关系如下：

| **考核方式**  **课程目标** | **考勤** | **课堂表现** | **以太坊智能合约** | **Fabric智能合约** | **底层平台编程** | **期末大项目** |
| --- | --- | --- | --- | --- | --- | --- |
| **课程目标1** | √ | √ |  |  |  | √ |
| **课程目标2** |  | √ | √ | √ | √ | √ |
| **课程目标3** |  | √ | √ | √ |  | √ |
| **课程目标4** |  | √ |  |  | √ | √ |

七、推荐教材和参考资料

1.推荐教材：

《区块链导论——原理、技术与应用》 张召、金澈清、田继鑫、周傲英编著，高等教育出版社 2023。

2.参考资料：

《区块链核心算法解析》，（美）Roger Wattenhofer（罗格.瓦唐霍费尔）电子工业出版社，2017。

《区块链编程》，吉米·宋（Jimmy Song）著，机械工业出版社出版，2020。

## 八、评分标准

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **课程目标** | **评分标准** | | | | |
| **90-100** | **80-89** | **70-79** | **60-69** | **0-59** |
| **目标1：能够全面准确了解区块链系统的发展历史、基本概念、架构和工作原理。** | 能够全面准确了解区块链系统的发展历史、基本概念、架构和工作原理。 | 能够准确地了解区块链系统的发展历史、基本概念、架构和工作原理。 | 能够大致了解区块链系统的发展历史、基本概念、架构和工作原理。 | 能够了解一些区块链系统的发展历史、基本概念、架构和工作原理。 | 完全不了解区块链系统的发展历史、基本概念、架构和工作原理。 |
| **目标2：能够掌握和理解区块链系统的关键核心部件，以及涉及到的关键核心技术。** | 能够深刻掌握和理解区块链系统的关键核心部件，以及涉及到的关键核心技术。 | 能够较好掌握和理解区块链系统的关键核心部件，以及涉及到的关键核心技术。 | 能够基本掌握和理解区块链系统的关键核心部件，以及涉及到的关键核心技术。 | 能够大致掌握和理解区块链系统的关键核心部件，以及涉及到的关键核心技术。 | 不能够掌握和理解区块链系统的关键核心部件，以及涉及到的关键核心技术。 |
| **目标3：能够基于现有的区块链平台开发区块链应用系统。** | 能够基于现有的区块链平台熟练开发区块链应用系统。 | 能够基于现有的区块链平台较熟练地开发区块链应用系统。 | 能够基于现有的区块链平台基本熟练地开发区块链应用系统。 | 能够基于现有的区块链平台大致熟练地开发区块链应用系统。 | 不能够基于现有的区块链平台开发区块链应用系统。 |
| **目标4：能够理解开源区块链系统的源代码，并在此基础上对开源平台进行必要的功能扩展和性能提升。** | 能够深刻理解开源区块链系统的源代码，能很好地对开源平台进行必要的功能扩展和性能提升。 | 能够较好理解开源区块链系统的源代码，能较好地对开源平台进行必要的功能扩展和性能提升。 | 能够基本理解开源区块链系统的源代码，并基本能对开源平台进行必要的功能扩展和性能提升。 | 能够大致理解开源区块链系统的源代码，能大致对开源平台进行必要的功能扩展和性能提升。 | 不能够理解开源区块链系统的源代码，也无法对开源平台进行必要的功能扩展和性能提升。 |