《区块链案例分析与场景设计》教学大纲

课程编号：

课程名称：区块链案例分析与场景设计

英文名称：Blockchain: Case Analysis and Scenario Design

学分/学时：2/32　　课程性质： 选修

适用专业：电子相关大类专业　　建议开设学期： 第二、四学期

先修课程：计算机导论与程序设计　　开课单位：创新创业学院

一、课程的教学目标与任务

数字加密货币的快速发展，吸引了全世界的眼光与关注，逐步引发了区块链市场规模的快速扩张。区块链所代表的安全、可信、数据流通及价值互联的理念正在影响着社会经济形态的发展，以构建信任为核心特征的区块链技术将在未来商业社会中扮演重要角色。区块链的发展必然以联盟链生态作为主体，因为联盟链生态携带了庞大的业务流量和丰富的商业场景。通过区块链技术构筑分布式商业模式，塑造高可信商业环境，同时必然带来具有无限想象空间的应用场景。

本课程通过理论学习和编程实验，让学生了解区块链技术架构，理解 Hyperledger Fabric 联盟链的技术本质及其应用价值。学习在 LinuxONE 上搭建 Hyperledger Fabric 底层业务网络，掌握应用开发的方法。通过案例场景分析，理解联盟链生态在商业社会中的作用。学习和练习相结合，引导思路，逐步具备区块链思维能力，学会识别应用场景，能够使用 Hyperledger Fabric 提供的方法解决实际问题，最终培养学生独立开发区块链系统的能力。

本课程面向电子信息大类二年级、三年级本科生。课程内容整体上分为三部分，第一部分是理论授课，主要内容包括区块链技术的基本概念、发展历史、基本原理，详细讲解其中的技术架构、共识算法、智能合约等关键技术；第二部分课程围绕 Hyperledge 项目展开，学习超级账本的原理和方法，了解其共识机制，通道 Channel 设计，节点作用，智能合约开发方法，相关支撑项目，以及典型应用案例；第三部分是应用实践，主要通过引导学生从浅到深地搭建 Hyperledger Fabric 联盟链系统，进行智能合约开发，基于具体应用场景设计分布式信任方案，开发区块链应用系统。

二、课程具体内容及基本要求

（一）区块链概述(4 学时)

主要内容包括区块链技术产生的背景起源、历史由来、区块链技术架构、区块链特性与分类、区块链思想与价值等。

1.基本要求

（1）了解：区块链的发展史、能解决的行业问题以及未来的发展趋势；

（2）理解：区块链是分布式网络、密码学、博弈论等技术的有机融；

（3）掌握：区块链思想，区块链价值，区块链技术架构。

2.重点、难点

重点：区块链技术原理、区块链技术总体架构；

难点：区块链思想，区块链价值。

3.作业及课外学习要求：

通过网络、图书等媒介查阅信息与区块链技术的发展史和热点动态，阅读《比特币:一种点对点的电子现金系统》。

（二）区块链中的密码学技术(2 学时)

学习区块链中采用的密码技术，包括公钥加密、数字签名、哈希运算、Merkle 树、零知识证明等。

1.基本要求

（1）了解密码学的基本概念与内容，流密码、分组密码、公钥密码、哈希函数、数字签名、零知识证明、安全计算等密码学技术的定义、实现方法、性质与用途，密码学算法编程实践中的注意事项；

（2）熟悉 AES、SHA-2、SHA-3、ECDSA、SM2、SM3、SM4 等常用密码学算法；

（3）掌握常用密码学算法的使用方法。

2.重点、难点

重点：AES、SHA-2、SHA-3、ECDSA、SM2、SM3、SM4 等常用密码算法；

难点：公钥签名算法，密码学算法及其参数的选取。

3.作业及课外学习要求

整理对比常用密码学算法的分类、使用范围、算法参数选取范围与注意事项。

（三）、区块链数据结构和数据库(2 学时)

学习分布式账本数据模型、状态树结构和链上数据持久化方式。

1.基本要求

（1）掌握交易和区块的结构；

（2）掌握 Hash 在区块链结构中的作用；

（3）熟悉区块链使用的键值数据库；

（4）了解分布式账本；

（5）了解世界状态树。

2. 重点、难点

重点：区块链数据结构和数据库。

难点：分布式账本和状态树 MPT。

3. 作业及课外学习要求

通过区块链浏览器查看交易结构。学习以太坊黄皮书：https://ethereum.github.io/yellowpaper/paper.pdf

（四）区块链中的共识算法(2 学时)

区块链平台一般采用的共识算法，这些算法的对比，各自优势，其与分布式一致性算法的关系。

1. 基本要求

（1）了解共识机制的定义、用途与分类方法，PoW，PoS，DPoS，BFT，PBFT，Paxos，Raft，DAG 等共识算法。

（2）熟悉 PoW 共识算法

（3）掌握 PoW、PBFT 共识算法

2. 重点、难点

重点：PoW 共识算法、PBFT 共识算法。

难点：PBFT 共识算法。

3. 作业及课外学习要求

对比区块链中常见共识算法的不同之处及其适用范围。

（五）智能合约(2 学时)

智能合约的一般概念和用途，EVM 虚拟机原理，智能合约在区块链网络中的关键作用。

1. 基本要求

（1）了解智能合约的定义与发展历史，智能合约编程语言及其编译，智能合约的安全性。

（2）掌握智能合约编程语言 Solidity。

（3）了解 Fabric 链码 Chaincode。

2. 重点、难点

重点：智能合约的安全性、Chaincode 开发方法。

难点：Solidity 语言，Chaincode 开发。

3. 作业及课外学习要求

学习了解 Solidity 语法。

（六）Hyperledge 项目介绍(2 学时)

介绍 Hyperledge 主要子项目及其基金会。

1. 基本要求

（1）了解 Hyperledge 开源基金会。

（2）了解 Hyperledge 子项目构成，这些子项目面向的目的和场景。

（3）掌握 Hyperledge Fabric 项目结构。

2. 重点、难点

重点：Hyperledge Fabric 项目结构。

难点：理解 Hyperledge 所有子项目的功能、目的。

3. 作业及课外学习要求

到 IBM 官方网站查找资料，了解 Hyperledge 项目进展。

（七）Hyperledger Fabric 系统架构(4 学时)

讲解 Hyperledge Fabric 底层原理，包括系统架构、网络节点、共识。

1. 基本要求

（1）了解 Hyperledge Fabric 系统整体架构。

（2）了解 Hyperledger Fabric 网络节点的区别

（3）理解 Hyperledger Fabric 不同节点的工作内容、节点网络结构。

（4）理解 Hyperledge Fabric 共识过程，通过共识构建信任。

（5）了解 Hyperledge Fabric 通道机制。

2. 重点、难点

重点：理解 Hyperledge Fabric 节点类型和作用，理解共识算法。

难点：如何通过共识构建信任。

3. 作业及课外学习要求

学习 Chaincode 语法。

（八）联盟链案例分析(6 学时)

介绍联盟链，区块链技术 (Hyperledger Fabric) 在行业中的实际案例。

1.基本要求

（1）理解具体应用案例的痛点需求，区块链系统如何针对这些需求解决问题，比如社会治理、征信系统、电子发票流转、投票系统、资产管理、酒溯源和供应链等案例。

（2）掌握针对行业需求和场景，提供具体的区块链的分布式信任解决方案。

（3）掌握什么情况下应该采用区块链系统解决问题。

（4）掌握不同区块链系统选型原则。

2.重点、难点

重点：通过学习不同的应用案例，加深对超级账本技术的理解。

难点：针对具体应用场景形成的解决方案。

3.作业及课外学习要求：

寻找某一个行业的实际应用场景，进行需求调研，针对场景需求，设计区块链的解决方案。

（九）Hyperledger Fabric 安装与配置(2 学时)

学习 Hyperledger Fabric 的获取方式，编译过程，以及其验证方法。

1.基本要求

（1）了解 Hyperledger Fabric 的工程结构；

（2）理解 Hyperledger Fabric 配置文件的作用；

（3）掌握 Hyperledger Fabric 安装方法。

2.重点、难点

重点：编译 Hyperledger Fabric。

难点：解决编译过程中由环境差异产生的问题。

3.作业及课外学习要求：

完成 Hyperledger Fabric 的获取和编译安装。书写实验报告。

（十）Hyperledger Fabric 网络部署(2 学时)

学习 Hyperledger Fabric 网络的组成，实操在 LinuxONE 上部署 Hyperledger Fabric 网络。

1.基本要求

（1）了解 Hyperledger Fabric 网络节点的区别；

（2）理解 Hyperledger Fabric 不同节点的工作内容；

（3）掌握 Hyperledger Fabric 网络部署方法。

2. 重点、难点

重点： Hyperledger Fabric 网络部署方法。

难点：单主机实验环境部署配置，多主机生产环境网络部署配置，LinuxONE 环境部署配置。

3. 作业及课外学习要求：

完成 Hyperledger Fabric 网络初步部署，熟悉网络运行过程。书写实验报告。

（十一）Hyperledger Fabric 智能合约设计(4 学时)

学习智能合约的编写、部署、调用。针对场景，运用智能合约进行应用设计。

1. 基本要求

（1）了解智能合约的原理；

（2）理解智能合约的编写规范；

（3）掌握 Hyperledge Fabric 链码 Chaincode；

（4）掌握智能合约的部署调用。

（5）针对具体场景设计智能合约。

2. 重点、难点

重点：智能合约的编写、安装、调用。

难点：智能合约的语法。根据场景设计智能合约。

3. 作业及课外学习要求：

完成 Hyperledger Fabric 智能合约部署的例子，尝试设计编写自己的智能合约。书写实验报告。

三、教学安排及方式

总学时 32 学时，其中：讲授 32 学时。

序号	课程内容	学时	教学方式
1	区块链概述	4	授课
2	区块链中的密码学技术	2	授课
3	区块链数据结构和数据库	2	授课
4	区块链中的共识算法	2	授课
5	智能合约	2	授课

6	Hyperledge 项目介绍	2	授课
7	Hyperledger Fabric 系统架构	4	授课
8	联盟链案例分析	6	授课
9	Hyperledger Fabric 安装与配置	4	上机实验
10	Hyperledger Fabric 网络部署	4	上机实验
11	Hyperledger Fabric 智能合约设计	8	上机实验

注：教学方式包括面授和实践，课上讲述，课后实践。

四、考核及成绩评定方式

最终成绩由平时作业成绩、期末成绩和小论文成绩等组合而成。各部分所占比例如下：

平时成绩：20%。主要考核学生对每堂课知识点的复习、理解和掌握程度、课堂参与度。

课程论文成绩：30%。主要考核发现、分析和解决问题的能力，以及语言及文字表达能力。根据任课教师划定范围、学生自拟题目撰写课程学习小论文，并在一定形式下进行宣讲、答辩，最后评定课程论文成绩。

课后实践成绩：50%。主要考核学生使用区块链技术的能力，以及通过这样的编程来解决实际问题的能力。学生需要完成指定的实验内容并撰写实验报告。

过程成绩提交时间和总评成绩计算说明表

序号	成绩提交时间	名称或说明
C1	第 16 次授课后	平时成绩
C2	第 16 次授课后	课程论文成绩
C3	第 16 次授课后	实践成绩
总评成绩 ＝ C1*0.2 + C2*0.3+ C3*0.5		

五、教材及参考书目

教材建议：

《区块链技术指南》，邹均 曹寅 刘天喜编，机械工业出版社，2016。

参考书目：

1. 《区块链：新经济蓝图及导读》，梅兰妮.斯万 著，新星出版社，2016；
2. 《区块链开发指南》，申屠青春著，机械工业出版社，2017；

3. Hyperledger Fabric 技术文档;

4. 《区块链核心算法解析》，Roger Wattenhofer 著，陈晋川等译，电子工业出版社 2017；

5. 《比特币:一种点对点的电子现金系统》，中本聪，2008。

六、说明

（一）与相关课程的分工衔接

本课程通过理论学习和编程实践，让学生掌握区块链关键技术和原理、并可以使用和开发区块链应用系统。先修课程是计算机导论与程序设计。

（二）其他说明

无。

（执笔人：卫佳 詹阳 审核人：裴庆祺 田甜（IBM） ）

2020 年 2 月 10 日