《区块链技术及其应用前景》教学大纲

课程编号：0782602

课程类型：□通识教育必修课 ☑通识教育选修课

□学科基础课 □专业核心课

□专业提升课 □专业拓展课

总 学 时：32 讲课学时：32 实验（上机）学时：0

学　　分：2

适用对象：全校公选课

先修课程：高等数学、计算机基础等

一、教学目标

通过本课程的学习，要求学生掌握区块链的基本概念和基本原理，熟练掌握区块链的基本原理和应用场景。了解区块链各个模块的实现方式。能够利用所学知识去解决一些实际的应用问题（或模拟案例）。

2.思政教育目标

中共中央政治局2019年10月24日下午就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

本门课程主要思政教育目标为：

（1）社会主义职业道德观。作为未来的接班人，一定要遵守从业人员相关道德规范，为将来建立良好职业操守奠定基础。

（2）求实精神。运用区块链技术，在解决产业的实际问题中踏实肯干、实事求是。

二、教学内容及其与毕业要求的对应关系

（一）教学内容

1．知识体系

第一部分：密码学及加密货币概述；

第二部分：区块链去中心化与运行机制；

第三部分：深入分析；

2．核心内容介绍

本课程的核心内容包括了解到所有比特币和其他数字货币相关的知识，对区块链技术具备基础性认识，能够区别那些完全虚构的故事。你将会对于如何与比特币网络进行交互有了基础概念，也可以将区块链的概念整合应用于自己的项目中。

（二）教学方法和手段

根据教学目标，拟采用的教学方法有：课堂讲解基本概念和核心知识，讲授和讨论相结合领会知识要点，案例教学训练解决问题的能力，并邀请行业专家做主题报告了解具体实践。

（三）学习要求

1．为有效学习本课程，要求学生首先具备程序高等数学、设计基础等方面的基本知识，较熟练掌握系统开发设计等方面的完整知识。

自学时应该熟读大纲，提纲挈领地掌握数据区块链的内容，随后，按照大纲熟读教材，通过课后思考和练习题进行多角度和层次的反复学习。

2．专家报告，本门课程有多次领域专家报告，通过专家讲解自己领域对区块链的应用，深入了解区块链在真实世界的价值，更好地掌握区块链的使用方法。

3. 分组实验，让学生根据所学知识，自己搭建一个简易的区块链系统。

三、各教学环节学时分配

以表格方式表现各章节的学时分配，表格如下：

**教学课时分配**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 章节内容 | 讲课 | 实验 | 其他 | 合计 |
| 1 | 密码学及加密货币概述 | 2 |  |  | 2 |
| 2 | 区块链运行机制 | 2 |  |  | 2 |
| 3 | 比特币如何做到去中心化 | 2 |  |  | 2 |
| 4 | 如何储存和使用比特币 | 2 |  |  | 2 |
| 5 | 比特币挖矿 | 2 |  |  | 2 |
| 6 | 比特币匿名性 | 2 |  |  | 2 |
| 7 | 匿名性与共识机制 | 2 |  |  | 2 |
| 8 | 其他挖矿算法 | 2 |  |  | 2 |
| 9 | 社区、政治和监管 | 2 |  |  | 2 |
| 10 | 比特币“平台” | 2 |  |  | 2 |
| 11 | 去中心化机构：比特币的未来 | 2 |  |  | 2 |
| 12 | 分组实验 |  |  | 2 | 2 |
| 13 | 分组实验 |  |  | 2 | 2 |
| 14 | 分组实验 |  |  | 2 | 2 |
| 15 | 分组实验 |  |  | 2 | 2 |
| 16 | 总结 | 2 |  |  | 2 |
| 合计 |  | 24 |  | 8 | 32 |

1. 教学内容
2. 密码学及加密货币概述1

**课程思政切入点**：讲诉密码学的发展与基础知识同时，联系密码学与国家信息通讯安全问题，让学生了解密码学对中国的重要性。

1.1密码学哈希函数4

1.2哈希指针及数据结构14

1.3数字签名19

1.4公钥即身份24

1.5两种简单的加密货币26

第2章比特币如何做到去中心化35

2.1中心化与去中心化37

2.2分布式共识39

2.3使用区块链达成没有身份的共识44

2.4奖励机制与工作量证明51

2.5总结59

1. 比特币的运行机制67

**课程思政切入点**：联系比特币的运行机制，讲解中国央行电子货币的发展，以及中国布局电子货币的重大意义。

3.1比特币的交易69

3.2比特币的脚本73

3.3比特币脚本的应用80

3.4比特币的区块84

3.5比特币网络86

3.6限制与优化93

第4章如何储存和使用比特币99

4.1简单的本地储存101

4.2热储存与冷储存105

4.3密钥分存和密钥共享110

4.4在线钱包和交易所115

4.5支付服务122

4.6交易费126

4.7货币兑换市场128

1. 比特币挖矿135

**课程思政切入点**：联系比特币的挖矿算法及其带来的巨大能源消耗，讲解中国央行电子货币为什么不能采用这种模式。

5.1比特币矿工的任务137

5.2挖矿所需硬件144

5.3能源消耗和生态环保155

5.4矿池161

5.5挖矿的激励和策略169

第6章比特币和匿名性179

6.1匿名的基础知识182

6.2如何对比特币去匿名化188

6.3混币197

6.4分布式混币203

6.5零币和零钞208

1. 社区、政治和监管219

**课程思政切入点**：联系比特币的社区和监管，谈论我国近些年在反腐倡廉方面做出的努力以及取得的成果。

7.1关于比特币的共识221

7.2比特币核心钱包软件223

7.3利益相关者：谁是掌权者227

7.4比特币的起源230

7.5政府对比特币的关注233

7.6反洗钱237

7.7监管239

7.8纽约州比特币牌照243

第8章其他挖矿算法249

8.1算法的基本要求251

8.2反ASIC解谜算法253

8.3有效工作量证明262

8.4不能外包的解谜算法269

8.5权益证明和虚拟挖矿273

第9章比特币“平台”281

9.1比特币作为一个只能被添加的记录283

9.2比特币作为一个“智能资产”291

9.3多方参与的安全博彩系统297

9.4比特币作为一个公共的随机源300

9.5预测市场和真实世界的数据源310

1. 另类币和加密货币生态系统321

**课程思政切入点**：联系区块链生态系统，给学生讲解我国的金融生态、社会生态，让学生理解融入生态的重要性。

10.1另类币的历史和诱因323

10.2几种另类币的详细介绍329

10.3比特币和另类币的关系333

10.4另类币的夭折与共同挖矿336

10.5不可分割的交叉链互换342

10.6侧链——基于比特币的另类币345

10.7以太坊和智能合约349

第11章去中心化机构：比特币的未来？359

11.1区块链作为去中心化的工具362

11.2通往区块链融合之路365

11.3去中心化的模板368

11.4什么时候适合去中心化374

五、考核方式、成绩评定

本课程的考核分为平时考核及期末大作业两种形式。本课程平时成绩占30%，期末考试成绩占70%。

平时考核主要以课堂练习与考勤衡量。

期末大作用形式为实验报告，描述分组实验的结果。

六、主要参考书及其他内容

[1] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016.

[2] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder。区块链：技术驱动金融. 中信出版社， 2016.

执笔人： 闫志强 教研室主任：　高静　　　系教学主任审核签名：