2023-2024学年《区块链基础及应用》

1 版本1

1. 判断题不用多说，简单的概念。
    - 数字人民币支付与区块链比特币是否相同
    - 给了一个交易输出让你判定一些信息
    - 忘记了...
2. OP 指令与智能合约填写，都是教材中的，不难
3. 数学证明
4. 画图说明 double spending attack
5. CPU 挖矿伪代码（好像是本学期学过的唯一一个伪代码？）以及第八章的一个伪代码
6. 虚荣地址与零知识证明
7. 还有一个书面作业原题

2 版本2

大题，顺序有误

二、双重支付攻击、画图解释
三、H (X xor Y) 是否能作为谜题。23 年 stanford 作业第一题
四、homework 第一题
五、哪一年全年比特币总和少于 1
六、书上智能合约和标准解锁脚本填空
七、cpu 挖矿算法、asic 限制挖矿算法伪代码
八、虚荣地址、schnorr 零知识证明方案

3 版本3

印象中的期末考题：
选择题 10 道，2 分一个，都是概念
印象中有，智能合约是否图灵完备的
解答题

1. 分析该哈希谜题是否合理（10 分）
2. 挖矿奖每四年减半，何时全年的挖矿奖励不足 1 比特币
3. 作业题。证明交易在 merkletree 上；二叉树三叉树哪个好
4. 填空：智能合约，P2PKH (都是作业里的，就两句话)（各 5 分）

5.cpu 挖矿的伪代码（8 分）还有一个设计什么挖矿的伪代码（7 分）

6. 设计生成伴随地址（7 分）

设计零知识证明（3 分）