

区块链技术及应用中期末大作业

本项目通过 Python 模拟 PoW 区块链在不同网络环境下的行为，重点分析以下三种情境：

- 诚实节点下的区块增长速率
- 自私挖矿策略的收益变化
- 分叉攻击的成功概率

文件结构说明

pow.py

功能：模拟在全为诚实节点的网络中，随着出块概率或节点数量变化，区块链的增长率情况。

- 支持指定节点数量、出块成功率、难度等参数
- 每轮中所有节点尝试出块，选择最长链作为主链
- 输出最终链增长速率，衡量系统吞吐能力

fork_attack.py

功能：模拟多恶意节点联合尝试构造替代主链（fork attack），分析其攻击成功率。

- 设置恶意节点比例，初始化诚实与恶意矿工群体
- 每轮诚实与恶意节点同时尝试出块
- 若恶意链成功替换主链，记录为一次攻击成功
- 输出不同恶意比例下的攻击成功概率

selfish_mining.py

功能：实现自私挖矿策略模拟，评估在不同算力比例下自私矿工能否通过策略获利。

- 模拟自私矿工维护私有链并伺机发布区块
- 当私有链领先一定长度时触发链竞争或同步
- 最终统计主链中自私矿工占比作为收益率

运行说明

每个文件均可直接运行：

```
python pow.py
python selfish_mining.py
python fork_attack.py
```