区块链期中大作业

李佳航

May 7, 2024

1 项目介绍

本文利用了 Python 语言实现了一个 PoW 的仿真程序，模拟一定数量的节点生成区块链的状态。分为三个部分：测量区块链增长速度、分叉攻击、自私挖矿。本文介绍了代码思路，在此基础上分享了代码实现过程以及最终结果：

- 通过设置节点数量、每个轮次出块的成功率等参数统计了区块链的增长速度
- 测量了不同恶意节点比例（10%-40%）条件下，以攻击 6 个长度的分叉为目标，统计分叉攻击成功的概率
- 这些恶意节点比例下，自私挖矿收益比例

最后，本文可视化了不同出块成功率下区块链的增长速度以及不同恶意节点比例下分叉攻击成功率和自私挖矿收益比例，对结果做了一定的分析。

2 代码思路

2.1 计算区块链增长速度

先定义一个 `BlockchainSimulation` 的类，在该类中使用 `simulate_round` 模拟每一轮中是否节点生成块，如果生成块，标记是恶意节点生成块还是诚实节点生成块，将这些标记存在一个名为 `blocks` 的数组中，最终该数组长度我们认为是生成的总块数。对于区块链增长速度，我们使用生成的总块数比上轮次总数来定义。我们总共跑 1000 轮（rounds 等于 1000）

2.2 统计分叉攻击成功概率

然后我们实现了不同恶意节点比例下的交叉攻击。用 `similate_attack` 函数记录了从第一轮开始由恶意节点和诚实节点生成的块数之差。如果下一个块由恶意节点生成，则差值加一，反之，则差值减一。由于题目中要求实现长度为 6 的分叉攻击，所以我们在差值为 +6 的时候输出 True 代表攻击成功，如果直到最后一轮结束，差值总是小于 6，我们认为攻击失败，无法做到长度为 6 的分叉攻击，返回 False. 同样的，我们设置 `attack_rounds` 为 1000 轮。

2.3 统计自私挖矿收益比例

我们使用恶意节点自私挖矿收益与恶意节点正常输出块的收益（不藏块）之比作为自私挖矿收益比例。在 `simulate_selfish_mining` 函数中，我们统计 1000 轮（即 rounds 等于 1000）恶意节点挖出一个块之后的情况：如果下一个块还是恶意节点挖出，那么该情况下收益为 2；如果下一个块由诚实接电脑挖出，那么恶意节点需要用原来的块和诚实节点挖出的块竞争，我这里使用随机数 `random.random`，如果得到的结果（闭区间 0 到开区间 1）小于 0.5，我们认为竞争成功，收益为 1，反之（大于 0.5），我们认为恶意节点竞争失败，收益为 0（藏的块成为废块）。最后我们用总收益与轮次数相除（正常输出块的话每轮收益固定为 1，所以总轮次数等于收益），得到自私挖矿收益比例。

2.4 代码整合与可视化

我们在 `run_simulation` 中设置了总轮数和分叉攻击轮数,调用之前写的 `BlockchainSimulation` 类中的 `simulate_round`，`similate_attack` 和 `simulate_selfish_mining` 来实现上面三个任务，并且使用 `matplotlib` 库来实现可视化。迭代恶意节点比例，将每次得到的该情况下的分叉攻击成功率和自私挖矿收益比例分别保存在 `success_attack_ratio_list` 和 `selfish_mining_profits_list`，然后 x 轴为恶意节点比例，y 轴分别为分叉攻击成功率和自私挖矿收益比例，得到了分叉攻击成功率和自私挖矿收益比例随恶意节点比例的变化情况。

3 实验结果分析

3.1 区块链增长速度

我设置了四个不同出块成功率 5e-4,1e-3,5e-3,1e-2, 得到了的对应的区块链增长速度如图1:

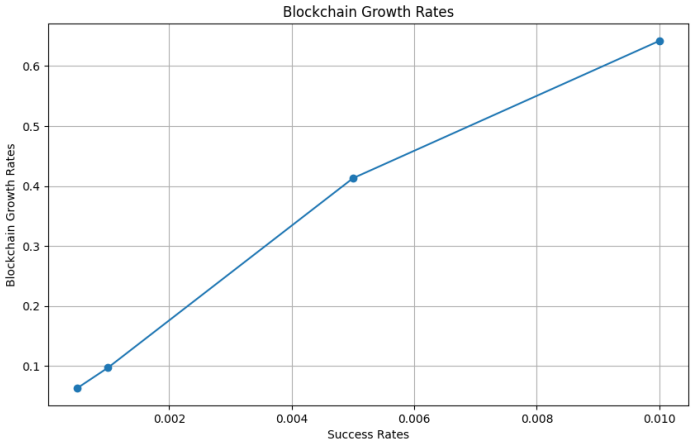

Figure 1: 区块链增长速度

我们可以看到随着出块成功率的增长，区块链增长速度也在增长，开始是一个正比例，后来随着出块成功率高于一定值后，每轮能出不止一个块，而我们假定每轮至多出一个块，所以区块链增长速度的增加就变慢了，最后随着出块成功率继续增长，区块链增长速度将达到最大值 1。(所以为了满足定义，需要设置较小的出块成功率。)

3.2 分叉攻击成功率

我测量了恶意节点比例分别为 0.1, 0.2, 0.3, 0.4, 0.5 时的分叉攻击成功率。我们设置的攻击轮数 `attack_round` 是 1000，即如果一千轮之前我们找到了某段链中恶意节点生成的区块数比诚实节点生成的区块数大 6，那么我们认为分叉攻击成功。为了保证我的实验结果（即攻击成功率）稳定，我们测试了 `round` 等于 1000 轮。实验结果如下图2所示：

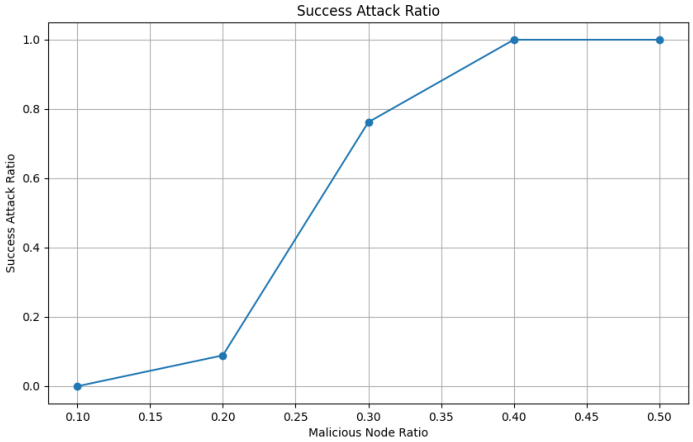

Figure 2: 攻击轮次为 1000 轮的分叉攻击

对于分叉攻击成功率的变化，我们可以看到恶意节点比例为 0.1，0.2 时，分叉攻击成功率较低，当恶意节点比例从 0.2 到 0.3 时，分叉攻击成功率显著提升，超过了百分之 75，当恶意节点比例达到 0.4，0.5 时，攻击轮次 1000 轮的分叉攻击达到了百分百的成功率。

我意识到不同的 `attack_round` 也会有不同的分叉攻击成功概率，我尝试了 `attack_round` 等于 100 的情况，如下图3

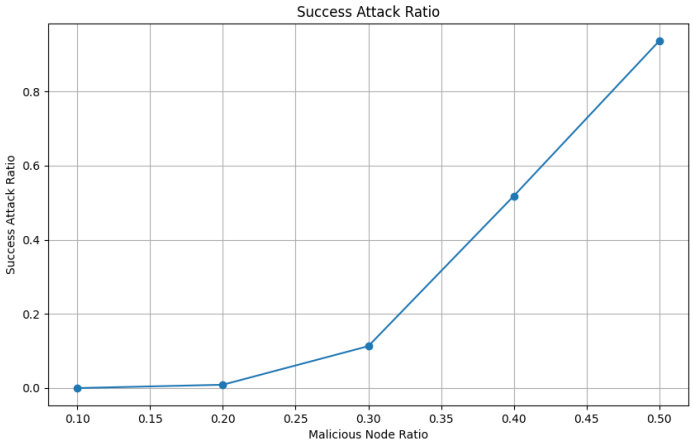

Figure 3: 攻击轮次为 100 时的分叉攻击

发现各恶意比例的分叉攻击成功率都有所下降，所以我们可以知道分叉攻击成功率与恶意节点比例以及攻击轮次都是正相关!

3.3 自私挖矿攻击的收益比例

最后，我测量了不同恶意节点比例下自私挖矿攻击的收益比例，即将自私挖矿收益是与正常挖矿收益相比。我使用的参数不变，仍然是恶意节点比例 0.1, 0.2, 0.3, 0.4, 0.5，节点数 `node_cnt` 为 100，出块成功率 `success_rate` 为 0.001，然后我们进行 1000 轮实验取平均值来减小误差，提高测量精度。实验结果如下图4所示:

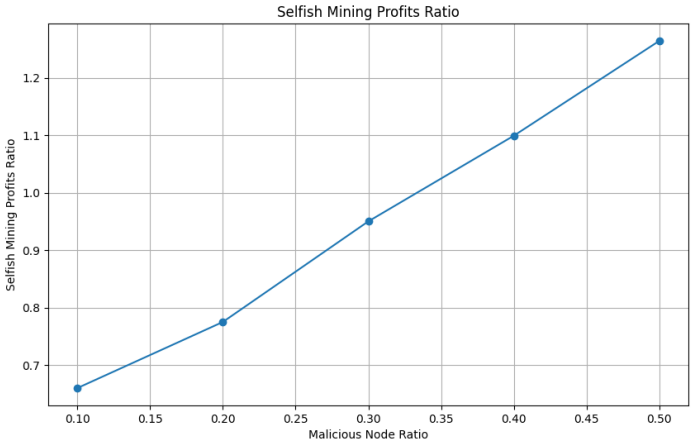

Figure 4: 自私挖矿收益比例

我们可以看到自私挖矿的收益比例与恶意节点比例基本是一个一次函数的关系，这个收益比例的变化和恶意节点比例变化的比值是 1.495（统计了恶意比例为 0.1 和 0.5 的收益比例的差值与 0.5-0.1 作商），也较符合 1.5 的理论比例！

4 总结

在本文中，我展示了 POW 仿真代码的代码思路，参数的选择以及展示了实验结果并进行了可视化，最后对可视化结果进行分析。我们分别探索归纳了以下几点结论：

- 探索了影响区块链增长速度的因素：出块成功率
- 影响分叉攻击成功率的因素：恶意节点比例和攻击轮次数
- 影响自私挖矿收益比例的因素：恶意节点比例

总而言之，在这次大作业中，我通过 Pow 仿真代码对课上讲的知识进行了复习，加深了对区块链的了解，将区块链知识落到实践中去了。