# 区块链技术及应用
# 期中大作业报告

姓名：...　　学号：...

## 1　作业要求

利用 (Python/Go/Rust) 等语言实现一个 PoW 的仿真程序，模拟一定数量的节点生成区块链的状态。

1. 设置参数包括：节点数量、每个轮次出块的成功率;
2. 测量区块链的增长速度。

设置一定数量的恶意节点实施攻击。

1. 测量不同恶意节点比例（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。
2. 测量不同恶意节点比例（10%-40%）条件下，自私挖矿收益比例。

## 2　PoW 仿真及结果

PoW（Proof of Work）是一种用于确认区块链中交易有效性的机制。在 PoW 中，节点（也称为矿工）需要通过解决一个难题来证明他们在生成新的区块时付出了努力。这个难题通常是一个要求具有一定数量前导零的哈希值的问题。通过找到满足条件的哈希值，矿工可以证明他们已经进行了一定的计算工作，并有权创建新的区块。

在本项目中，我采用了一个简化的 Backbone 协议来进行 PoW 仿真实验。这个协议模拟了区块链网络中节点之间的信息传递和区块链的增长过程。协议采用 flat model，每个节点（诚实或者恶意）都拥有相同的算力，每个节点可以挖矿，创建新的区块，然后通过一定的规则来选择哪个区块链是有效的。仿真实验的核心目标是观察不同的挖矿难度对区块链增长速率的影响。

1. Block 类用于表示区块，其中包含了创建区块的 node 的 id 和前一个区块的信息。这个类的实例用于构建区块链。

2. Node 类用于表示网络中的节点，每个节点有一个唯一的节点 ID，一个成功生成区块的概率和一条区块链。在每个轮次中，节点尝试生成新的区块，如果成功则将新区块添加到自己的区块链中。

在每个轮次结束时，选择网络中最长的链作为主链，并将所有节点的区块链更新为主链。这确保了所有节点都采用同一条最长的链，从而维护了区块链的一致性。

然后，通过模拟多个轮次来进行区块链增长的仿真。在每个轮次中，节点尝试生成新的区块，并选择最长的链作为主链。最后，计算了链的增长速率，并输出结果。

## 2.1 实验结果

在仿真实验中，我们探究了不同成功率（$10^{-7}, 10^{-6}, 10^{-5}, 10^{-4}$）下有 500 个节点的区块链的增长速率和不同节点数量（$100, 500, 1000, 2000$）下以 $10^{-7}$ 作为成功率的区块链的增长速率。每次进行 2000 轮仿真实验，并记录区块链的增长率。程序运行结果如图 1 所示，将其整理得到表 1，2。

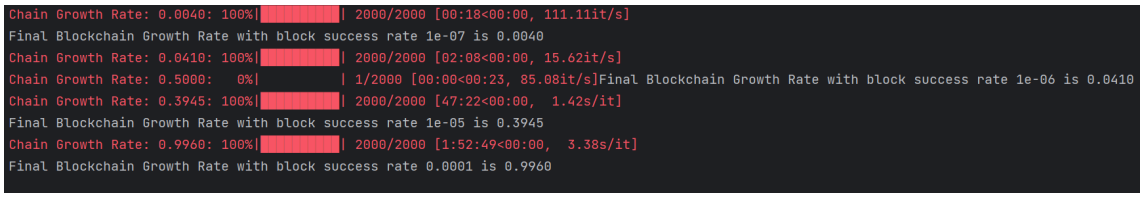


Figure 1: PoW 仿真实验结果

| Block Success Rate | Chain Growth Rate |
|---|---|
| $10^{-7}$ | 0.0040 |
| $10^{-6}$ | 0.0410 |
| $10^{-5}$ | 0.3945 |
| $10^{-4}$ | 0.9960 |

Table 1: 不同成功率下的区块链增长速率

| Number of nodes | Chain Growth Rate |
|---|---|
| 100 | 0.0000 |
| 500 | 0.0040 |
| 1000 | 0.0085 |
| 2000 | 0.0170 |

Table 2: 不同节点数量下的区块链增长速率

通过对不同成功率和不同节点数量下的区块链增长速率进行实验，可以得出以下结论和总结：

1. 成功率的提高会显著加快区块链的增长速率。较高的成功率意味着节点更容易生成新区块，从而促进整个区块链的增长。

2. 当成功率较小时，区块链增长速率相对较慢，但随着成功率的增加，增长速率呈现出指数级增长的趋势。然而，当成功率足够大时，几乎所有节点都能够成功生成新区块，导致区块链增长速率趋近于 1。

3. 随着节点数量的增加，区块链增长速率也以线性增长的趋势增加。当节点数量较小时，区块链增长速率相对较慢。

4. 此外，我观察到较高的成功率会导致计算时间显著增加。这可能是因为在高成功率下，节点需要更频繁地尝试生成新区块，从而增加了计算的负载和时间消耗。

# 3 分叉攻击及结果

分叉攻击是一种常见的区块链攻击方式，其目标是在区块链网络中创建分叉，使网络出现不一致状态。攻击者通过在原有链的某一点分叉，并试图在分叉点之后生成更长的链，以取代原有的主链。这种攻击可能导致双重支付等问题，破坏了区块链的一致性和安全性。

在分叉攻击中，我同样采用了 Backbone 协议，引入了两种类型的节点，恶意节点和诚实节点。正常节点遵循 Backbone 协议，它们努力挖矿并创建新的区块，以维护网络的一致性。恶意节点则尝试在某个区块上创建一个分叉，然后尝试在这个分叉点之后生成更多的区块，使得他的替代链比原始链更长，从而导致区块链网络的不一致状态。

## 3.1 实验结果

在这个实验中，主要关注不同比例的恶意节点对分叉攻击的影响。为了模拟不同强度的攻击，我使用了不同比例的恶意节点（10%，20%，30%，40%）来模拟不同强度的攻击。攻击的目标是在每轮尝试中创建一个长度为 6 的分叉。恶意节点在每轮仿真中持续尝试创建分叉，即在当前主链的某一点进行分叉，然后试图生成比当前主链更长的分支。如果分叉成功并且新分支的长度达到 6 个区块，那么我们认为攻击成功。

通过对不同比例的恶意节点进行实验，我记录了成功创建长度为 6 的分叉的概率。结果如图 2 所示。将结果进行整理得到表 3。

| Malicious Rate | The probability of a fork with a length of 6 |
|---|---|
| 0.1 | 0.0000 |
| 0.2 | 0.0100 |
| 0.3 | 0.0560 |
| 0.4 | 0.2390 |

Table 3: 分叉攻击仿真实验结果

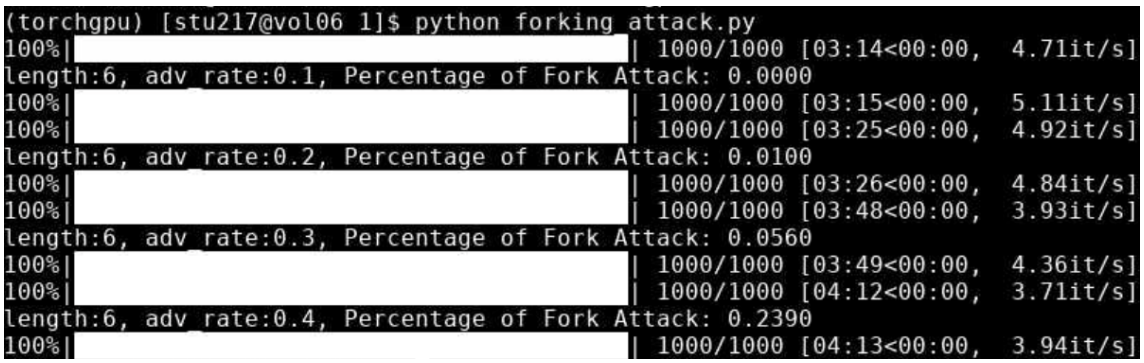


Figure 2: 分叉攻击仿真实验结果

根据实验结果和观察，可以得出以下结论：

1. 随着恶意节点比例的增加，成功创建长度为 6 的分叉的概率呈现显著上升趋势。这表明恶意节点的比例对于区块链网络的安全性和稳定性具有重要影响。

2. 在恶意节点比例很小 (如 10%) 时，成功创建长度为 6 的分支的概率可视为 0。

3. 在恶意节点比例较高时，网络面临分叉攻击的风险陡增。攻击者通过控制足够数量的节点，可以有效地干扰网络的正常运行，导致网络出现不一致状态，甚至可能引发双重支付等安全问题。

# 4 自私挖矿及结果

自私挖矿是一种区块链攻击方式，攻击者试图通过隐藏挖矿活动并延迟将新区块广播到网络中来最大化自身的利益。在自私挖矿中，攻击者找到新的块时，不会选择立即将新区块广播到整个网络，而是将其保留在私有链上，同时继续挖掘下一个区块，以获得更多奖励。这种攻击可能对区块链的公平性和安全性产生潜在威胁。

为了研究自私挖矿攻击的效果，我设计了一个区块链仿真实验，并使用了自私挖矿算法。在实验中，我模拟了不同比例的自私矿工与诚实矿工在区块链网络中的行为，并统计了自私挖矿收益比例。

我的自私挖矿仿真代码实现了两种类型的节点：诚实节点（HonestNode）和自私节点（SelfishNode）。诚实节点遵循正常的挖矿规则，即在找到新区块后立即广播到网络中。而自私节点采用自私挖矿策略，延迟将新区块广播，以尽可能获取更多奖励。

在每轮仿真中，根据预先设定的自私节点比例，生成自私节点和诚实节点，并模拟它们的挖矿行为。当自私节点找到新的区块时，它们会将其保留在私有链上，并继续挖掘下一个区块。自私矿工会根据私有链和公共链的长度差异来决定是否切换链，以最大化私有链上的区块数。

## 4.1 实验结果

我模拟了 10%, 20%, 30%, 40% 自私节点比例下，自私矿工的收益比例. 实验结果如图 3 所示，将结果进行整理得到表 4。

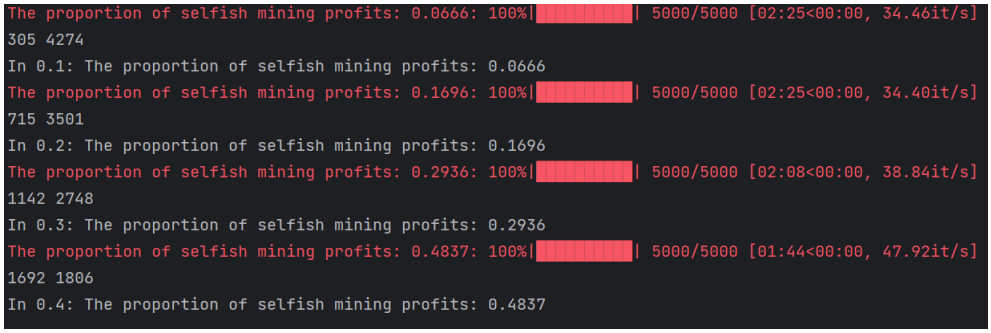


Figure 3: 自私挖矿仿真实验结果

| Malicious Rate | The proportion of selfish mining profits |
|---|---|
| 0.1 | 0.0666 |
| 0.2 | 0.1696 |
| 0.3 | 0.2936 |
| 0.4 | 0.4837 |

Table 4: 自私挖矿仿真实验结果

根据实验结果和观察，可以得出以下结论：

1. 随着自私节点比例的增加，自私矿工的收益比例也随之增加，且增加幅度也随之增大。

2. 当自私节点比例较低 (如 10%) 时，自私挖矿攻击可能会减少自私矿工的收益比例。

# 5 总结

在本次作业中，我实现了基于 Python 的 PoW 仿真程序，并进行了分叉攻击和自私挖矿的实验，以探究这些在区块链领域中常见的攻击方式对系统的影响。

首先，通过对不同成功率和不同节点数目下的区块链增长速率进行实验，我观察到成功率对区块链增长速率的显著影响。随着成功率的增加，区块链增长速率呈指数级增长。随着节点数量的增加，区块链增长速率以线性速度增长。其次，我对分叉攻击进行了实验，观察了不同比例的恶意节点对攻击成功概率的影响。最后，我研究了自私挖矿攻击，并观察了自私节点比例对攻击成功的影响。实验结果显示，自私节点比例的增加导致自私挖矿攻击的收益显著增加。

总的来说，本项目通过对区块链中的 PoW 共识机制、分叉攻击和自私挖矿行为的仿真和分析，得到了合理的仿真结果，帮助我深入理解了这些关键概念在区块链系统中的作用和影响。