区块链技术与应用
期中大作业报告

吴舒文

1 PoW 仿真

在区块链技术中，工作证明（Proof of Work，简称 PoW）是一种关键的共识机制。这一机制的主要目标是确保区块链网络的安全性和一致性。PoW 通过要求网络中的节点（也称为矿工）解决复杂的计算问题，从而证明他们为网络做出了有意义的工作。这项工作通常涉及到寻找一个满足一定条件的哈希值，以创建新的区块并验证交易。只有通过解决问题的节点才有权利创建新的区块，这种机制有效地抵御了恶意行为，确保网络的安全性。

在本项目中，我使用了一个简化的 Backbone 协议来进行 PoW 的仿真实验。该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。协议采用了 flat model，即每个节点（无论是诚实的还是恶意的）都拥有相同的算力。每个节点都可以进行挖矿，创建新的区块，并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（由区块生成率控制）对区块链增长速率的影响。

代码包括两个关键类：Node 和 Block。Node 类代表了网络中的节点，每个节点都维护着自己创建的区块链。Block 类代表区块，每个区块包括创建者的 ID 和前一个区块的哈希值。

PoW 模拟程序的主要逻辑是节点尝试挖矿，创建新的区块，并同时受到挖矿难度和 Oracle 查询次数的限制。程序通过比较不同节点的区块链长度来选择最长的区块链，并将其他节点的区块链更新为最长链的副本，以保持一致性。

在仿真实验中，我设置了一些参数。例如，区块链节点的总数被设置为 500。我选择了四个不同的区块生成概率 $(10^-7, 10^-6, 10^-5, 10^-4)$ 进行了 2000 轮仿真实验，并记录了最长有效区块链的长度以及区块链的增长率。

从实验结果可以得出以下结论：

表 1: PoW Simulation

Block generation probability	**Max Valid Chain Length**	**Chain Growth Rate**
10^{-7}	11	0.005
10^{-6}	96	0.0475
10^{-5}	872	0.4355
10^{-4}	1990	0.9945

1. 随着区块生成概率的增大，Chain Growth Rate 增大，有效链长度增大。
2. 区块生成概率每增大 10 倍，Chain Growth Rate 也接近增大 10 倍，呈现出线性关系；但 Chain Growth Rate 最大只能为 1，当区块生成概率为 10^{-4} 时，Chain Growth Rate 稳定在 1 附近。
3. 在实验过程中，Chain Growth Rate 动态变化，但总体保持稳定，说明区块链整体运行稳定。

2 分叉攻击

分叉攻击（Forking Attack）是一种对区块链网络的潜在威胁，它可能导致网络一致性的破坏、交易的混乱和不确定性。攻击者的目标是通过制造竞争性的区块链分支来破坏网络的一致性，从而可能导致双重支付等恶意行为。

在分叉攻击中，我采用了 Backbone 协议，并引入了两种类型的节点：正常节点（HonestNode）和恶意节点（MaliciousNode）。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。而恶意节点的行为旨在制造分叉，它们通过不断挖矿来增加其分叉链的长度，试图干扰网络的正常运行。

在本实验中，我们主要关注不同恶意节点比例（10%、20%、30%、40%）对分叉攻击的影响。通过改变恶意节点的比例，我们模拟了不同的攻击强度，从低强度到高强度进行实验。每个实验包括多轮仿真，节点根据 Backbone 协议选择主要分支。我们记录了在不同条件下成功创建分叉的概率以及主要分支的长度期望值。

表 2: Malicious Rate Length Probability

Malicious Rate	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0.1	0.091	0.023	0.008	0.001	0.0	0.0	0.0	0.0	0.0	0.0
0.2	0.202	0.086	0.054	0.031	0.034	0.012	0.007	0.008	0.007	0.001
0.3	0.299	0.206	0.159	0.129	0.103	0.076	0.06	0.04	0.037	0.036
0.4	0.37	0.331	0.317	0.292	0.255	0.237	0.229	0.204	0.187	0.198

根据实验结果，我们可以得出以下几点结论：

1. 在相同的恶意节点比例下，要求生成的分叉链长度越长（length 越大），攻击成功的概率就越小。在恶意节点比例很小（10%）时，当 length 为 6 或者更长时，攻击成功的概率都变为 0。这表明了系统的安全性。

2. 随着恶意节点比例的增加，分叉攻击成功的概率明显上升。这意味着随着恶意节点比例的增加，系统的安全性下降，恶意节点更容易成功地发起分叉攻击。

3. 当 length=1 时，分叉攻击成功的概率几乎和恶意节点比例相同，符合理论结果。这表明在分叉链长度为 1 的情况下，恶意节点几乎总能成功地发起分叉攻击。

根据以上结论，我们可以得出关于系统安全性和恶意节点比例以及分叉链长度之间的关系。这些结果在设计和保护分布式系统中具有重要的参考价值。

实验结果还表明，在恶意节点比例较小时，系统的安全性相对较高，可以有效抵御分叉攻击。然而，随着恶意节点比例的增加，系统的安全性会逐渐下降，恶意节点更容易成功地发起攻击。因此，在设计分布式系统时，需要采取适当的安全机制和防御策略来减轻恶意节点的影响，确保系统的可靠性和稳定性。

此外，分叉链长度对系统安全性也有重要影响。较长的分叉链要求攻击者在一定时间内生成更多的分叉块，增加了攻击的难度。因此，适当增加分叉链长度可以提高系统的安全性。然而，需要权衡系统的性能和安全性之间的关系，避免过长的分叉链导致系统的延迟增加或吞吐量下降。

综上所述，恶意节点比例和分叉链长度是影响系统安全性的重要因素。通过实验和分析，我们可以更好地理解它们之间的关系，并采取相应的措施

来保护分布式系统免受恶意节点的攻击。

3 自私挖矿

自私挖矿（Selfish Mining）是一种区块链攻击行为，其目标是最大化攻击者（自私矿工）的奖励，而不遵守共识规则的公平性。自私挖矿的核心思想是通过隐藏已挖出的区块，延迟其公开，然后在私有链上继续挖矿，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。

自私挖矿收益比例是指在区块链网络中，自私矿工（Selfish Miner）相对于诚实矿工（Honest Miner）获得的总区块奖励的比例，通常以数值表示。这个比例反映了自私挖矿策略的成功程度，即自私矿工是否能够通过采用自私挖矿策略获得更多的奖励。具体定义如下：

$$\text{自私挖矿收益比例} = \frac{\text{自私矿工获得的总区块奖励}}{\text{诚实矿工获得的总区块奖励}} \tag{1}$$

在本项目中，我建立了一个自私挖矿的简化模型，包括三个关键角色：诚实矿工、自私矿工和区块链系统。诚实矿工按照共识规则挖矿，将挖出的区块立即添加到公共链上。自私矿工试图最大化自己的奖励，拥有公共链和私有链两条链。私有链上的区块不会立即公开，而是被隐藏。

程序模拟了自私挖矿的过程，包括自私矿工和诚实矿工的行为。自私矿工选择挖矿的概率，并将挖出的区块添加到私有链上，不立即公开。诚实矿工按照正常协议挖矿，挖出区块后立即添加到公共链上。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。程序会根据链的长度来选择主链，以确保公共链包含最多的区块。

程序模拟了不同恶意比例的情况（10%、20%、30%、40%），并输出各个恶意比例下自私矿工获得的收益比例。实验结果如图 4 所示，将结果进行整理得到表 3。

可以看出，随着恶意比例的增大，自私挖矿收益比例增大，且恶意比例越大，收益比例增加的幅度变大。

表 3: 自私挖矿模拟结果

Malicious Rate	**Selfish Mining Revenue**
0.1	0.07039947609692207
0.2	0.17943287445581832
0.3	0.3138815207780725
0.4	0.5429187634795112