区块链技术与应用

期中大作业报告

王鑫*
电子信息与电气工程学院

2023 年 10 月 27 日

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。

- 设置参数包括：节点数量、每个轮次出块的成功率;
- 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。

- 测量不同恶意节点比例（10%-40%）条件下，统计分叉攻击成功的长度;
- 测量不同恶意节点比例条件下，自私挖矿收益比例。

2 项目结构

本项目使用 Python 进行编写，目前代码已开源在 GitHub中。项目结构如图1所示。

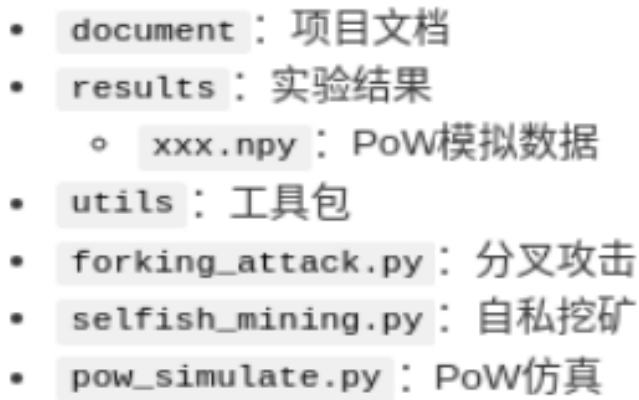

图 1: File structure

*520021910700, wangxin.1@sjtu.edu.cn

3 PoW 仿真及结果

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。其主要目标是确保网络的安全性和一致性，通过要求网络中的节点（即矿工）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。PoW 的核心思想在于，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。

在本项目中，我使用了一个简化的 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（由区块生成率（block_gen_rate）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，每个节点都维护着一个区块链，用于记录自己创建的区块。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包括节点尝试挖矿，创建新的区块，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。

参数设置上，区块链节点总数设置为 500；我一共选取了 4 个区块生成概率（10^{-7}、10^{-6}、10^{-5}、10^{-4}），每次进行 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。程序运行结果如图2所示，将其整理得到表1。

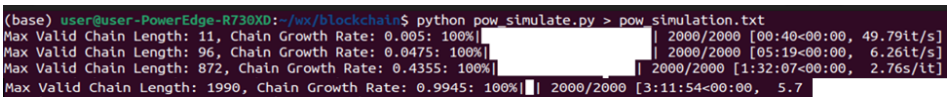

图 2: PoW 仿真实验结果

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

表 1: Pow 仿真实验结果

从实验结果可以得出以下结论：

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。

4 分叉攻击及结果

分叉攻击 (Forking Attack) 是一种对区块链网络的潜在威胁，它可能导致网络的一致性受损，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，可能导致双重支付等恶意行为。

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：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的长度，试图干扰网络的正常运行。

在本实验中，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来模拟不同的攻击强度，从低强度到高强度依次进行实验。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，结果如图3所示。将结果进行整理，得到表2。

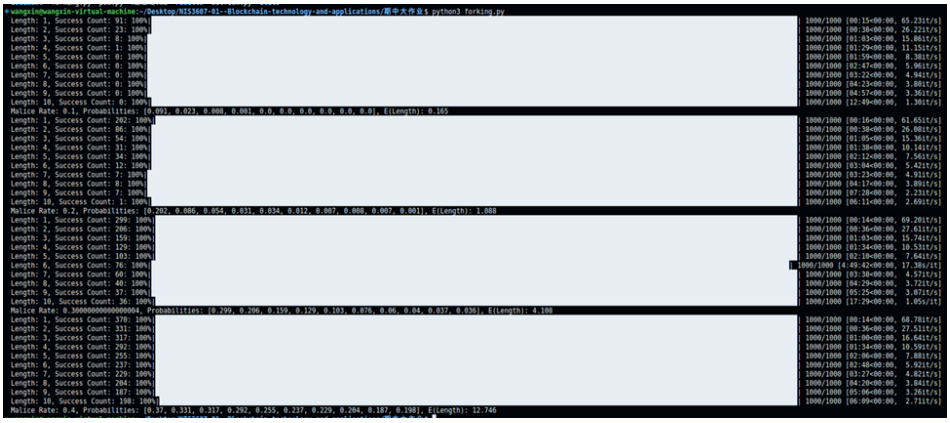

图 3: 分叉攻击模拟结果

表 2: 分叉攻击概率表格

Malicious Rate	**Length**	**Probability**									
		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，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，length 为 6 或者更长时成功概率都变为 0。
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。
3. 当 length=1 时，分叉攻击成功的概率几乎和 malicious rate 相同，符合理论结果。

5 自私挖矿及结果

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：

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

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 malicious rate 的增大，自私挖矿收益比例增大，且 malicious rate 越大，收益比例增加的幅度变大。

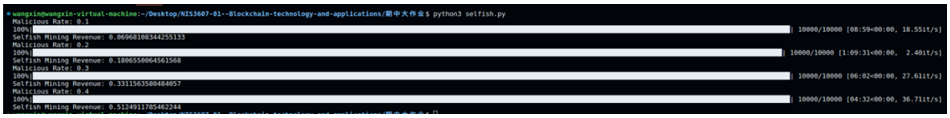

图 4: 自私挖矿模拟结果

Malicious Rate	Selfish Mining Revenue
0.1	0.06968108344255133
0.2	0.1806550064561568
0.3	0.3311563580484057
0.4	0.5124911785462244

表 3: 自私挖矿模拟结果

6 总结

本项目针对作业要求，使用 Python 编写了区块链仿真程序，模拟了 PoW 共识机制、分叉攻击和自私挖矿行为，并得到了相应的实验结果。PoW 仿真通过简化的 Backbone 协议观察了不同

区块生成率对区块链增长速度的影响，发现随着生成率的增加，区块链增长速度也增加，呈现出线性关系。分叉攻击模拟研究了不同恶意节点比例对攻击成功概率的影响，得出了攻击成功概率与恶意节点比例和分叉长度的关系。最后，自私挖矿部分探讨了自私挖矿的策略和收益比例，发现恶意节点比例增加会导致自私挖矿收益比例上升。

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。