区块链 作业三

> TRY 计算机科学与技术

1. 如何对比特币矿池发起 DoS 攻击?

DoS(Denial of Service)，即拒绝服务。DoS攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，使目标系统服务系统停止响应甚至崩溃。

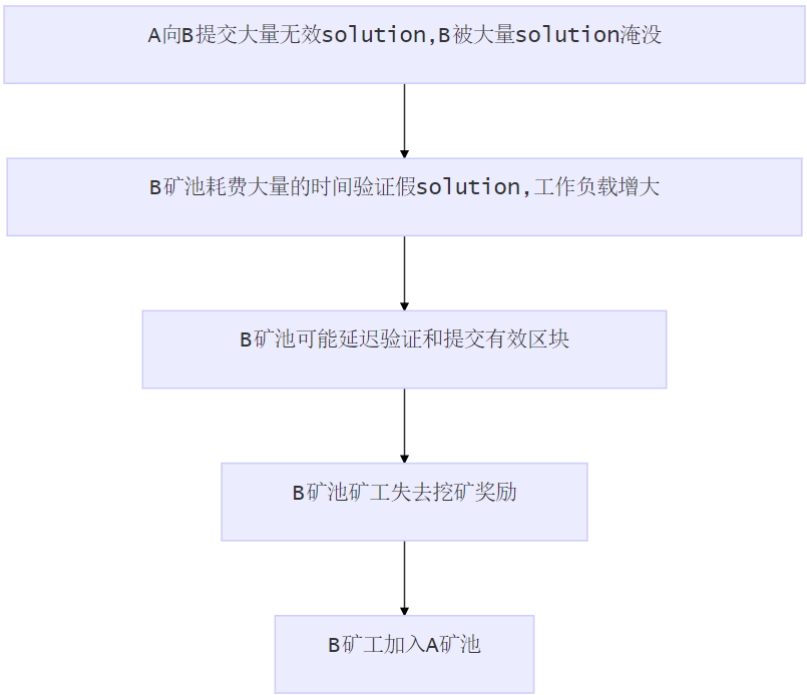
> 现假设A矿池要对B矿池发动DoS攻击

- **理想的DoS攻击**

  A矿池可以往B矿池内提交大量的无效solution，但是B矿池无法判断这些solution是否为自己的"顾客"还是"闹事的地痞流氓"，一样傻乎乎的去辨别solution的有效性，进行极其消耗算力的哈希运算。

  当A发给B的solution提交过多的时候，B矿池即victim池被大量solution淹没，工作负载过大，B的manager就会耗费大量的时间验证这些solution，真正的solution验证有效反而被延迟，提交有效区块时间变长，最后失去挖矿的奖励。此时，B的矿工在工作后拿不到奖励，就会自然而然加入A矿池，获得奖励。

  以下呈现DoS攻击的流程图：



- **DoS攻击策略：**

  然而，不是简单采用上面所说的策略就可以获益的，需要有一定的攻击策略，承担相应的亏损风险：

  - 若A矿池要对B矿池进行DoS攻击，需要选择攻击等级，等级越高，对方矿池越容易被攻破，但自己的成本也会越高，导致当次收益越低
  - 根据利益迁移的矿工可能会因为攻击成本过高收益过低而不迁移到A矿池。即B矿工可能会迁移到什么也没做的C矿池内，类似于鹬蚌相争。

- 对于攻击方来说，其攻击策略需要不断调整，因为对手可能学习你的攻击策略，以其人之道还治其人之身。

2. 如果对基于 $PBFT$ 共识类型的区块链发起 DoS 攻击，造成什么后果?

$PBFT$算法，即实用拜占庭容错算法，其解决的问题是：如何让个体不带条件地相信彼此并达成共识。$PBFT$的本质是利用通信次数获取信用，方法为各个节点各自与其他节点进行两两通信；是联盟币的共识算法的基础。

如果在此区块链中混入一个恶意的攻击者，其可以不断地发送确认指令，让其他节点判断其是否为叛徒，消耗区块链内服务资源，实现DoS攻击。 这对于区块链的不同层次，会有不同影响：

- **数据层**：问题不大，底层的加密机制、数据结构等都是按照原先方式运作。
- **网络层**：可能会给网络层带来巨大的负担。$PBFT$共识机制本质上是通过通信次数来获取信用。若涌入大量的信息需要验证，P2P网络将承载大量的流量。
- **共识层**：DoS攻击对$PBFT$共识机制可能会带来巨大打击，因为此漏洞可能会导致区块链的节点因此放弃使用此共识机制，转向其他机制。
- **激励层**：DoS攻击会造成不良的激励效果。如上所说，受害矿池中的矿工会不断迁移至攻击池，甚至有可能什么都不做的矿池最终获利。这会导致区块链的工作没有矿工愿意承担，造成恶性循环。
- **应用层**：在下层遭受DoS攻击时，软件将受阻于大量的计算与通信，从而不能给用户提供即时高效的服务。