区块链第三次作业

- 米家龙
- 计算机学院
- 18342075

调研

> 如何对比特币矿池发起 DoS 攻击？请用文字、绘图，甚至伪代码，描述一种可能的方案。

1. 压力测试：
   攻击者可以通过引入女巫身份来利用比特币系统的低吞吐量发动 ddos，即同一个对手也可以控制多个钱包，使用这些身份，攻击者可以在他控制的各种女巫身份之间发出几个**粉尘交易**（例如，每笔交易0.001 BTC）。通过在短时间内引入大量小值的交易，网络将因为创建包含那些交易的块而拥堵，并且将拒绝对网络中的合法用户提供服务。由于这种**拥堵**，对手也可能发动其它攻击：例如，双重花费由于拥堵而未被打包的令牌交易。
2. 内存池泛洪攻击：
   该攻击是在密码的内存池（mempools）上进行的，以增加采矿费用。假设 mempools 充当未经证实的事务的缓存。尽管加密货币的块大小有限，但是内存池没有大小限制。即使用户会计算内存池的大小以确定其事务的优先级，但如果内存池中有更多交易，那么采矿竞争就会变得很激烈。为了优先处理交易，用户开始**支付更多**采矿费作为矿工的激励措施。在这种低成本的攻击中，攻击者和伪造的女巫节点可能会使未经证实的事务充斥内存池。用户在这种攻击下产生了恐慌，于是，在攻击者的交易没有被开采的情况下，用户会倾向于支付更高的采矿费来优先处理他们的交易，最终导致了真正的 DDoS 攻击。

总结

> 如果对基于 PBFT 共识类型的区块链发起 DoS 攻击，会造成什么后果？(可以从区块链的不同层的角度阐述一下)

在基于PBFT的私有区块链中，如果对手控制 ≈33% 的副本，则可以发起 DDoS 攻击。在专用区块链中，参与节点知道网络的大小，这允许攻击者计算它需要在网络中引入攻击的女巫节点的数量。假设攻击者控制f女巫节点使得总网络大小为 $n < 3f + 1$，则攻击者将能够发起DDoS攻击以停止验证过程。对于主要发送的每个事务，女巫节点将不会回复其批准。由于主节点需要至少 $3f + 1$ 个节点的批准，因此它将无法处理任何事务，系统活动将停止，从而导致 DDoS 攻击。

攻击发起后，弱势合约阻止退还给合同的旧领导者并使攻击者成为新的领导者。此外，它取消了其他投标人发送的所有请求，并使攻击者成为拍卖的领导者。在以太坊智能合约中另一种形式的 DoS 攻击涉及利用合约设定的Gas限制，在以太坊中，如果执行时智能合约消耗的总气体超过天然气限制，则合同交易失败。攻击者可以通过**添加多个具有退款需求的地址**来利用此功能。执行后，退还这些地址所需的 Gas

可能超过总 Gas 限额，从而取消最终交易。