1. **女巫问题**

问题描述：

在对等网络中，但节点通常具有多个身份标识，通过控制系统的大部分节点来消弱冗余备份的作用。

***八卦一下这个名字的来路：***

*根据Flora Rhea Schreiberie在1973年的小说《女巫》（Sybil）改编的同名电影，是一个化名Sybil Dorsett的女人心理治疗的故事。她被诊断为分离性身份认同障碍，兼具16种人格。我的那个天。高度精分一枚。*

女巫攻击是在P2P网络中，因为节点随时加入退出等原因，为了维持网络稳定，同一份数据通常需要备份到多个分布式节点上，这就是数据冗余机制。女巫攻击是攻击数据冗余机制的一种有效手段。

如果网络中存在一个恶意节点，那么同一个恶意节点可以具有多重身份，就如电影了的女主角都可以分裂出16个身份，那么恶意节点比它还能分。这一分可好，原来需要备份到多个节点的数据被欺骗地备份到了同一个恶意节点（该恶意节点伪装成多重身份），这就是女巫攻击。

解决方法：

1.工作量证明机制，即证明你是一个节点，别只说不练，而是要用计算能力证明，这样极大地增加了攻击的成本。(兰花协议使用的是算力,即奖章规则)

2.身份认证（相对于PoW协议，女巫攻击是基于BFT拜占庭使用容错协议的Blockchain需要考虑的问题，需要采用相应的身份认证机制）。

认证机制分为二类：

1）基于第三方的身份认证

每加入一个新的节点都需要与某一个可靠的第三方节点进行身份验证。

2）纯分布式的身份认证

每加入一个新的节点都需要获得当前网络中所有可靠节点的认证，这种方法采用了随机密钥分发验证的公钥体制的认证方式，需要获得网络中大多数节点的认证才能加入该网络。