讨论总结

1. 质押机制

共识协议中质押机制要与网络规模、共识过程、共识节点性能等相结合，最终确定发行价格和介个动态调整。

质押的金额可以根据代码规则设置一个虚拟账号：全0或者全F都行。所有质押的金额都存放在这个虚拟账号中。通过一个解质押机制，根据质押时发起的质押交易和UTXO交易模型生成的质押哈希，从质押列表中取回质押的金额。

2. 区块链

2.1 共识节点数量

区块链的类型如果是公链至少需要500个以上，必须是分散的。但是节点太多会因为网络负载造成比较大的网络压力。网络通信会指数级增长。

2.2 区块上链

区块上链之前需要尽可能多的节点对区块和区块中所有的交易进行全局检查，随后再上链。就算这个过程耗时长，耗能多也要做全面细致的检查，最终检查成功再上链。

3. 签名

3.1 签名作假

签名作假如何防止？通过公钥进行验证

3.2 签名时间作假

签名时间作假问题，可以通过与区块时间戳和其他交易时间戳以及其他节点签名的时间戳比较，可以检查出签名节点时间戳是否作假。

3.3 签名数量

签名的数量通常在理论分析中需要过半，但是在工业实际中，若是需要过半节点签名，则会造成很大的网络负载，最终可能会导致无法对区块达成共识，或者区块达成共识所耗费的网络时延会比较大。

15000个节点，选择1000个节点达成共识，需要10s/20s左右的时间，且存在断网的风险。

可以测试不同数量的签名达成共识的成功率。

4. 女巫攻击

通过质押机制防止女巫攻击。质押机制与币的发行有关。

5. 节点同步

在系统运行初期，节点可以同任意节点同步最新区块链。但是区块链超过一定高度或者系统中节点数量超过一定阈值，则需要向比较可信的节点同步最新区块链。

同步的时候，需要考虑拜占庭问题，防止同步到错误区块链信息。共识节点的 $\frac{2}{3}$ 都由相同视图才行。

盈利

盈利主要采用以下几种方式：

- 需要机群：卖矿机
- 小型设备无法打包和存储交易，需要公网提供打包和存储服务；
- 公网节点签名获得奖励；
- 智能合约。

考虑的点

主要需要考虑几个方面：

- 技术点：高效性
- 经济：合理性
- 人性：贪婪、懒惰

设计的时候尽可能减少漏洞，否则容易被攻击者利用漏洞薅羊毛。因此，上链的区块一定要进行全局检验，验证成功才能上链。即使牺牲部分性能也是可以接受的。