区块链原理与技术作业

比特币的共识机制

第 2 次作业

姓名：郝裕玮
班级：计科 1 班
学号：18329015

1、比特币设计简单，但是它能顺畅运行，背后有什么原因？

答：（1）比特币总量恒定为 2100 万个，避免了通货膨胀；

（2）正如第 1 次作业中所说，比特币去中心化，避免了第三方的监管问题，同时通过非对称加密的方式保证了个人的财产安全；

（3）比特币特有的共识机制 PoW（工作量证明）保障了比特币的安全性：①挖矿难度高，如果有恶意攻击想要破坏当前有效的最长区块链，就必须掌握超过 51%的算力才能造出对自己有利的更长的区块链，在当前的情况下，这种方案几乎不可能实现；

②正如白皮书中激励部分所说：greedy attacker ... ought to find it more profitable to play by the rules.（贪婪的攻击者...会发现遵守规则会获得更多利润），所以大多数人最终会遵守规则选择努力挖矿，并从中获取奖励；

2、Monoxide 提出的共识机制与比特币的共识机制有哪些不一样？

答：**对于比特币共识机制：**

（1）比特币共识机制无法突破“不可能三角”。比特币重视的是去中心化和安全性：为了安全性，所有节点要复制其他节点的账本信息。为了去中心化，则需要挖矿参与门槛低，对于带宽、CPU、内存等要求较低，否则会有节点参与不进来。所以这样就导致了吞吐量，带宽，TPS 等有瓶颈，最终无法保障可扩展性；

（2）比特币共识机制需要消耗大量能源，不够环保（比特币网络一年能源消耗量相当于哥伦比亚一年用电量）。

对于 Monoxide 共识机制：

（1）Monoxide 突破了“不可能三角”，同时满足了去中心化，安全性和可扩展性；

（2）对于可扩展性的补充：可扩展性指的不是任务的可扩展性，而是指我们可以把任务切分成多个块，让多个相同的较低性能的电脑参与进来完成任务。这样我们就无需造出一个性能非常高的超级计算机；

（3）采用了异步共识组的思想，将整个区块链网络划分为多个共识组，且共识组之间地位，功能相同。他们并行工作，分摊全网的吞吐、计算、存储的压力，分摊全网状态的维护工作。

同时由于共识组之间完全并行、异步也无需锁定和同步，所以即便某一个共识组发生拥塞也不会干扰其它共识组的吞吐和出块，从而大幅提升了区块链的吞吐量和容量；

（4）Monoxide 采用了“全分片”的方法：将网络通讯（网络）、合约计算（CPU）、状态表达（内存）和交易归档（磁盘）这个四个方面的工作量全部分片；

（5）Monoxide 采用了连弩挖矿机制：连弩挖矿将矿工的有效算力放大，并同时放大单位物理算力可以获得的出块奖励。所以对于同样的物理算力和能源消耗，当你参与到越多的共识组进行挖矿时，你所获得的出块奖励也会越多。

所以最终全网会收敛到主流的矿工都会采取连弩挖矿的方法并参与到所有的共识组当中。从而使得全网的有效算力达到 n*H，单个共

识组的有效算力达到 H。这样使得攻击者对于某特定共识组的算力聚焦攻击必须根据协议将放大后的有效算力平均分配到各个共识组，使得对单个共识组的攻击仍然需要全网的51%物理算力(如果是普通的n个共识组，只需要集中H/n的算力就可入侵该共识组)。

3、连弩挖矿机制存在什么样的潜在问题？

答:(1)参与更多的共识组会线性增加开销，对于个人矿工来说不利，但对于专业的矿池组织来说不是问题;

(2)对于矿工来说，执行连弩挖矿时，他们和普通区块链一样，需要存储所有分组的账本，同时矿工必须确保自己正在扩展的各个分组账本不与其他分组账本的数据发生冲突;

(3)连弩挖矿会降低挖矿难度。因为在各个分组区块奖励相同的情况下，矿工始终会优先选择挖矿难度低的分组，这会使不同分组的挖矿难度最终会收敛到相同等级。