区块链原理与技术 作业2

姓名：TRY

专业：计算机科学与技术

学号：

题目： 比特币设计简单，但是它能顺畅运行，背后有什么原因?

比特币中有“**共识机制**”，是比特币中一种多方协作机制，用于协调多参与方达成共同接受的一种结果，且保证此过程难以被欺骗，持续稳定运行。它具有有效性、容错性和完整性的特点，在身份确认、交易服务、记录管理、信任规则等方面都有重要应用。

比特币的共识机制涉及**三个观点**：**规则的共识、历史记录的共识、比特币价值的共识。**其中，“规则的共识”确保交易或块有效的机制，是比特币运行的核心协议、数据结构。“历史记录的共识”指每个用户都记录了所有已发生的交易，就他人未使用的比特币数量达成了共识。“比特币价值的共识”指比特币可以通过美金结算，保证了比特币的交易有效性和需求性。

实际上，比特币设计者意识到了很难同时达到共识的三个方面，因为不可能在分布式、匿名的全球范围的系统中保证共识。但是，比特币以某种方式将这三种共识观点结合在一起，使得他们互相支持。

由**数学**概率知识可知，挖矿是高难度的，即挖掘相同数量的块需要很多的计算能力，这使得分叉攻击更难，保证了比特币网络更加安全，免受攻击。

从**挖矿的安全性**分析，假设比特币的大部分算力是掌握在诚实的矿工手里，可以防止恶意节点伪造交易获利以及恶意节点double-spending的现象的发生，同时避免selfish-mining。具体来说，如果恶意节点想要自私挖矿（即不发布已挖到的矿），反而可能会浪费已挖到的块，这样还不如“落袋为安”，赶紧发布获取奖励。而人们为了金钱奖励会变得诚实起来，保证了假设的成立。并且，合谋发动51%-forking攻击必须要占据系统超过半数以上的计算力才能成功，这几乎是不可能的，也保证了安全性。**POW机制**是一个无记忆性的过程，无论从任何时候开始挖成功率都是一样的，这样可以防止“预挖矿”的发生。

从**挖矿的激励与策略**分析，挖到矿的矿工在制造新的比特币，且有出块奖励作为激励，因此他们有动力去维护比特币的生态发展。矿工可以自由选择挖矿的策略，如选择将哪些交易放进他的区块里，选择在哪个区块上进行挖矿，在同一高度的多个区块中进行选择，在何时宣布新的区块。矿工的自由性也保证了比特币的顺利运行。

从**社区**的角度分析，矿工花费美金得到比特币的奖励，保证了矿工会投入大量算力，且由于用户普遍相信区块链的安全性，保障比特币的价值持续高稳，人们对比特币的安全也越有信心。安全性、生态健康和比特币的价格三者相互依赖、相互作用，维护了健康的挖矿生态，保证比特币的顺利运行。