2019~2020 学年冬学期《区块链与数字货币》课程作业 2

应承峻 3170103456

1. 请指出 Litecoin 在 Bitcoin 技术上做过哪些改动？分析这些改动会产生什么后果？

- 莱特币采用了 scrypt 算法来进行工作量证明，该算法相对于比特币采用的 SHA256 算法，使得定制的比特币机器和 AMD GPU 在并没有在莱特币挖矿中具有更大的优势（scrypt 自身需要大量的内存，每个散列作为输入的种子使用的，然后与需要大量的内存存储另一种子伪随机序列，共同生成序列的伪随机点而输出哈希值），也就是说莱特币的挖矿更依赖于 CPU 和内存，降低了硬件的准入门槛，能够给普通人也提供挖矿的机会，使得莱特币能够更容易在普通计算机上挖掘到。
- 比特币出块速度为 10 分钟/块，而莱特币对比特币的算法进行了修改，使得莱特币的出块速度是比特币的 4 倍，即 2.5 分钟/块，每笔交易的验证时间也下降为原来的四分之一，因此莱特币可以提供更快的交易和验证，更易于使用、更具有潜力。
- 莱特币预期产出 8400 万个莱特币，发行量是比特币的 4 倍。

2. 智能合约宣传是图灵完备的，什么是“图灵完备”?

在解释“图灵完备”这一概念之前，先解释“智能合约”和“图灵机”这两个概念。

“智能合约”是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。在区块链中，当预先制定好的条件被区块链上的交易所触发时，就会自动地执行相应的条约，从区块链中读取数据或向区块链中写入数据。

“图灵机”是图灵提出的一种抽象数学模型：它提供了一条无限长的纸带，纸带分成了无数的小方格。在每个时刻机器头都会从当前纸带上读入一格信息，然后通过自己的内部状态查找程序表，将程序的运行结果输出到方格上，然后转换状态并移动。

图灵完备指的是能够通过某种语言来模拟出图灵机，即能够解决所有的可计算问题。由于现实世界的复杂性，比特币的脚本语言远远无法满足未来区块链中的更多应用场景，因此以太坊的优势就在于其能够实现“图灵完备”的语言，从而最大程度上满足现实应用场景。

图灵完备的特点之一就是能够支持循环，即程序能够不断地执行下去，然而在这种情况下，矿工难以判断一个程序何时会结束因为图灵停机问题已经证明了“证明一个程序能不能终止”是不可能的，因此“智能合约”语言需要能够保证程序不出现死循环。通过在以太坊语言中加入 gas 能够使得程序每个运算过程都会消耗一定成本，从而不会无限制地执行下去。