

## 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?

第一，不同于比特币使用的 SHA256 挖矿算法，LTC 采用 scrypt 算法。scrypt 算法使用 SHA256 作为其子程序，而 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。在 BTC（Bitcoin）的开采依靠单纯的显卡挖矿过于艰难，各种价格不菲挖矿机的出现提高了普通人通过挖矿获得 BTC 的门槛，而 LTC 在使用 PC 显卡挖矿上具有一定优势。与比特币算法依赖高性能显卡不同，LiteCoin 排除了 GPU 和定制处理器，因此不过于依赖少量专业矿。更依赖于 CPU 和内存，从而降低了硬件进入门槛。

第二，莱特币的总量是比特币的四倍，8400 万枚，总数量更多。

第三，莱特币的区块时间是 2.5 分钟，是比特币的四分之一，即每 2.5 分钟出一个区块。莱特币对算法进行了简单修改，使挖矿速度比比特币速度快了四倍，每笔交易的验证时间也相应下降为前者的 1/4，比比特币能够更快的确认真伪，更能够应用到实际的交易场景。

莱特币是先于比特币进行隔离见证和扩容的数字资产，并没有发生硬分叉。

## 2. 智能合约宣传是图灵完备的，什么是“图灵完备”？

在可计算性理论里，如果一系列操作数据的规则（如指令集、编程语言、细胞自动机）可以用来模拟单带图灵机，那么它是图灵完备的。

图灵完备意味着这个语言可以做到能够用图灵机能做到的所有事情，可以解决所有的可计算问题。

图灵完备语言最显著的一个特点是支持循环，所谓循环，就是程序能不断执行下去。那么在区块链支撑的分布式环境下，矿工如何判断一个程序何时结束呢？而图灵计算理论，也有人证明过，要证明一个程序能不能终止是不可能的（图灵停机问题），所以这种“智能合约”语言需要保证所写出的程序不能存在死循环。

以太坊语言会加入 gas（汽油），程序每个运算过程都会消耗一定成本，从而不会无限地执行下去。