在开始之前，我们补充一点基础知识。

第一个概念是哈希。简单理解，哈希是一个函数。它的作用是将任意长度的数据作为输入，转变为固定长度的一个字符串作为输出。这个函数有两个主要特点：

过程不可逆

对输入做微小改动，输出就会完全不一样。

哈希函数有好多种，但都满足上面的特点。几乎任何加密货币都会用到哈希算法，以太坊采用的哈希算法是ethash算法。

第二个补充知识是，以太坊的区块结构。一个以太坊区块包含区块头和区块内容。

区块内容就是区块所包含的交易列表。而区块头中包含了如下信息：

前一个区块的哈希、区块序号（n）、随机数（nonce）、目标值（target）、时间戳（timestamp）、难度值（difficulty）、矿工地址（address）等内容。

好了，介绍完上述基础，我们正式开始本文的内容。

以太坊共有四个阶段，即Frontier（前沿）、Homestead（家园）、Metropolis（大都会）、Serenity（宁静）。以太坊前三个阶段采用的是POW共识机。第四个阶段将采用自己创建的POS机制，名为Casper投注共识，这种机制增加了惩罚机制，并基于POS的思想在记账节点中选取验证

首先介绍以太坊前三阶段使用的POW机制。我们在上节课中讲到，POW机制的基本原理是下面这个公式：

计算值