什么是比特币挖矿？了解比特币的人或多或少都知道&quot采矿&quot。挖矿是参与维护比特币网络的节点，通过帮助生成新块，获得一定量的新比特币。当用户发布交易时，需要有人确认交易并将其写入区块链。，形成新的区块。

在一个互不信任的系统中，应该由谁来做？比特币网络采用&quot采矿&quot来解决这个问题。目前，每10分钟左右就会生成一个大小不超过1MB的块。，串联在最长链条的末端，每一个区块的成功提交者可以获得系统中12.5个比特币的奖励，以及用户在交易中附加的支付服务费。

以比特币为例，挖掘的具体过程是：参与者根据前一个块的哈希值、10分钟内验证的交易内容、自己猜测的一个随机数x，使新块的哈希值小于比特币网络中的一个给定数字。。数字越小，越难计算。每两周系统会根据上一周期的挖矿时间调整挖矿难度，使生成区块的时间稳定在10分钟左右。为了避免冲击，每次调整的最大幅度为4次。

It&#039；这很自然。有人会想，如果我算力很强，所有的块都是我算的，我拒绝认别人&#039；的交易内容，会不会破坏比特币网络？的确，有了51%的计算能力，就可以攻击整个网络。

那么有什么办法保护它呢？除了尽可能避免把计算能力放到同一个组织手里，如果一个矿池的计算能力太大，矿工应该主动把矿池换成矿。为了解决这个问题，有人提出了PoS。因为PoW机制的安全性只能来自于区块开采的收益，而矿工的激励来自于避免失去区块收益的风险，所以PoW是靠大量激励保证的巨量计算能力来运作的。

PoS打破了这种对称性。不是靠收入来保证安全，而是惩罚。矿工必须支付一大笔

保证金，获得一笔小的奖励，以补偿自己保证金的冻结和节点运行的成本，但逆转交易的最大成本来自于比收益大几百倍到几千倍的惩罚(保证金被消耗)。。PoS的哲学不是&quot安全来自耗电&quot，但是&quot安全来自存款&quot。

众所周知，比特币的总数固定在2100万左右，但是如何获取比特币，一定是很多人会好奇的事情。也许很多人都听说过&quot采矿&quot，但什么是&quot采矿&quot？比特币的区别&#039；s&quot采矿&quot以及我们对&quot采矿&quot？

(在传统的理解中，&quot采矿&quot一般指黄金、宝石等稀有金属行业和石油、天然气等能源资源行业的开采步骤。)

首先，&quot采矿&quot是产生比特币的唯一途径，也是市场上比特币的唯一来源途径。。用传统思维去理解，埋藏比特币的区块链网络相当于一座矿山，用于开采的机器称为矿机，一般是计算机软件，一般由开源社区或个人开发者提供。

前期挖掘期参与者少，全网计算能力很低。个人可以通过电脑显卡甚至CPU轻松挖到比特币。但在大量矿工的参与下，整个网络的计算能力不断提升。个人通过普通电脑直接挖到比特币的概率迅速下降。目前个人通过普通电脑挖到比特币的概率趋于0。

采矿的一个关键工具是&quot矿机&quot。矿机的目的是设计和优化挖掘算法的硬件。因为矿工人数的急剧增加和加入矿业的个人数量的增加，特殊的矿业芯片应运而生。矿机的竞争已经深入到电脑芯片的设计和制造。目前市场上的矿机成本都比较高，一般都是由公司整体运营，对外销售或租赁。。

即使有专用矿机，单个矿商或机构也很难独自获得比特币。因为在形式上，比特币的记账权一次只能由一个矿工获得。一旦有人获得许可，其他参赛选手将一无所获。

所以个体采矿的成本是巨大的。为了改变这种状况，有人提出了&quot矿井池&quot。集中大量设备和矿工共同挖矿，然后根据计算能力分配到各个电脑上，最大限度降低挖矿比特币失败的风险。