区块链领域常提到的挖矿，其实最早的是工作量证明(Proof Of Work，简称POW)。

所谓的工作量证明，就是用来确认你做过一定量的工作。监测工作的整个过程通常是极为低效的，而通过对工作的结果进行认证来证明完成了相应的工作量，则是一种非常高效的方式。

比如现实生活中的毕业证、驾驶证等等，也是通过检验结果的方式(通过相关的考试)所取得的证明。

区块链挖矿是什么意思

挖矿是通过消耗计算资源来处理交易，确保网络安全以及保持网络中每个人的信息同步的过程。这个过程因为同淘金类似而被称为“挖矿”，因为它也是一种新的临时机制。POW每年的确消耗了非常多的资源，这是事实，但直到目前为止POW仍然是经过实际证明的很好的方案。

一、挖矿原理

最初的时候，我们用电脑CPU就可以挖到比特币，比特币的创始人中本聪就是用他的电脑CPU挖出了世界上第一个创世区块。然而，CPU挖矿的时代早已过去，现在的比特币挖矿是ASIC挖矿和大规模集群挖矿的时代。

回顾挖矿历史，比特币挖矿总共经历了以下五个时代：

CPU挖矿→GPU挖矿→FPGA挖矿→ASIC挖矿→大规模集群挖矿

挖矿芯片更新换代的同时，带来的挖矿速度的变化是：

CPU(20MHash/s)→GPU(400MHash/s)→FPGA(25GHash/s)→ASIC(3.5THash/s)→大规模集群挖矿(3.5THash/s*X)

挖矿速度，专业的说法叫算力，就是计算机每秒产生hash碰撞的能力。也就是说，我们手里的矿机每秒能做多少次hash碰撞，就是算力。算力就是挖比特币的能力，算力越高，挖得比特币越多，回报越高。

在比特币的世界里，大约每10分钟会记录一个数据块。所有的挖矿计算机都在尝试打包这个数据块提交，而最终成功生成这个数据块的人，就可以得到一笔比特币报酬。最初，大约每10分钟就可以产生50个比特币的比特币报酬。但是该报酬每4年减半，现在每10分钟比特币网络就可以产生25个比特币。

而要成功生成数据块，就需要矿工需要找到那个有效的哈希值，而要得到正确的哈希值，没有捷径可以走，只能靠猜，猜的过程就是计算机随机hash碰撞的过程，猜中了，你就得到了比特币。

二、挖矿方法

挖矿芯片经历了CPU挖矿到GPU挖矿到FPGA挖矿，如今走入了ASIC挖矿时代。然而挖矿的方式也经历了从一两台矿机挖矿到小矿机作坊，再到如今走入了大规模矿场挖矿的时代。