区块链-挖矿

# 秒懂比特币挖矿

1.我手上现在有一张面值100元的人名币。（比特币）

2.谁关注公众号我就给谁。

3.但是需要在评论里面猜出这张钱的编号才行。（挖矿，随机填充数值求解）

### 自己想尽办法猜，猜中得100元全款——个人挖矿

### 出钱召集一些人来一起猜——矿场

### 召集认识不认识的人一起来猜，通过猜测的次数，按比例分配这100元——矿池

以上是一个简单的类比例子，当然，你们关注并猜出了我兜里100块钱的编号，我保证给你。

# 区块链（Block Chain）网络

区块链节点：

矿工：运行于强大或专用的硬件（比如ASIC）之上，主要目的是挖矿。

挖矿：

在全网中和其他节点竞争计算（解一个难题）的过程。

证明自己是非恶意节点。

获得的权利和义务

记账权-把交易

区块链-共识机制

**拜占庭将军问题**-共识机制之一

**POW（Proof of Work）**-工作量证明

理性人都是逐利的，POW抑制了节点的恶意动机。

区块链-交易确认

每一项交易被链上的区块收录后。

区块链-区块生成

矿工在挖矿之前要组建区块

区块链-区块验证

相邻节点收到

区块链-分类

公有链、联盟链、私有链

区块链-篡改账本

双花问题

**比特币挖矿机**

**比特币挖矿机**，就是**用于赚取比特币的电脑**，这类电脑一般有专业的挖矿芯片，**多采用烧显卡的方式工作**，耗电量较大。

几个概念：

矿场、矿池

其实，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。当然，现在也可以用家用电脑的CPU、GPU挖矿，只是收益非常低了。 CPU挖矿的时代早已过去，GPU挖矿也早已不是主流，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）

算力就是计算机每秒产生哈希碰撞的能力，算力越高，挖到比特币的概率越大，挖得比特币也就越多，回报越高。

然而挖矿的受益并不是稳定且有保障的，电费将成为持续挖矿最大的成本之一，所以，有廉价电力的地方便成了旷工的最爱。

# 知乎提问：

最近翻译了**中本聪先生发明比特币**的论文，在这篇论文中他说**比特币的产生由挖矿者计算最优散列值计算得到，第一个计算得到这一散列值的也就是block的第一人将会获得比特币。别的人无功而返。**看了一些其他的参考资料也是这样。但是我自己挖矿了好像不是这样，经过一段时间的挖矿过程后我产生了微量的比特币，那么既然我没有造出这一block，这些币是如何来的？是不是现在最优block的计算已经不是一个人了，而是一群人？然后计算出来以后根据每个人的能力付于他一定值的比特币？

**你应该不是自己在挖矿，而是加入了某一个矿池。**矿池会集合许多矿工的计算能力来挖矿。当挖到block的时候，根据每个人的算力占总算力的比例来进行分红。所以你才会得到微量的比特币。

# 区块链技术

**区块链技术是比特币的底层技术**，但在早期并没有太多人注意到比特币的底层技术。但是当比特币在没有任何中心化机构运营和管理的情况下，在多年里非常稳定的运行，并且没有出现过任何问题。所以很多人注意到，该底层技术技术也许有很大的机制，而且不仅仅可以在比特币中使用，也许可以在许多领域都能够应用这种技术。所以从某个角度来看，**比特币可以看成是区块链第一个应用，而区块链更类似于TCP/IP这样的底层技术，以后会扩展到越来越多的行业中**。