# 比特币原理

# 比特币

1. 比特币：电子货币，基于密码学的货币
2. 2008年11月1日，中本聪发表在数学上的一篇论文，没人知道中本聪是谁，点对点的电子现金系统。
3. 比特币无疑是一场革命，去**中心化电子记账系统**

交易中最重要的就是记账，查看账户中是否有足够的金钱，现在是银行记账，我们信任银行，是因为我们相信国家不会倒闭，所以，银行说你有钱，你就有钱，说你没有，你就没有。（账本公开，每个人都有账本）

1. 优点，改良了传统货币由银行说了算，相比较下来，比特币更安全可靠
2. 分布式记账系统
3. 区块链，区块链的内容主要是账本信息（交易信息），我们将这些信息进行打包，打包成一个块-叫区块（大小1M，4000条），将这个块连接到以前的块上成为一个链条，区块链
4. 需要解决的问题，以谁为准（大家都记账），为什么我要记账，如何防伪

为什么记账，有奖励（比特币）[手续费，打包奖励]

奖励是多少

没10分钟打包一个，前4年，大一包50,接下来4年，25

50\*6\*24\*364\*4（1+1/2+1/4.....) = 2100W

以谁为准，做一个数学题--（工作量证明）-一个数一个数进行比对，解答出来，就有资格进行打包（挖矿）

# 挖矿原理

哈希函数（散列函数）-将字符串转换为标识

sha256->256位二进制

基本不可逆，只能枚举

比如区块链已经连接到了某个位置

区块链有很多的信息，区块链的头部，时间，账单

很多人都在打包交易信息，要把数据接到区块链中，但在接区块链之前要获取资格，计算题（一个特殊的256二进制数，要求前6位为0）

**字符串**=->前块的头部-》账单信息-》**随机数**

**sha256(sha256(字符串）） = 要求前6位是0，通过改变随机数**

**我为啥要去计算，既然要求是前几位为0，我直接生成字符串不就可以了**

# 难度的确定

二进制概率

1/2\*1/2\*1/2..... = (1/2)^n 难道由前n位为0的难度

难度：保证每10分钟出一个块，调整n的大小

# 保证交易记录

传统的身份认证可以拷贝

电子签名

使用非对称加密

双重支付

只有打包的才能添加到块上，其他的放弃