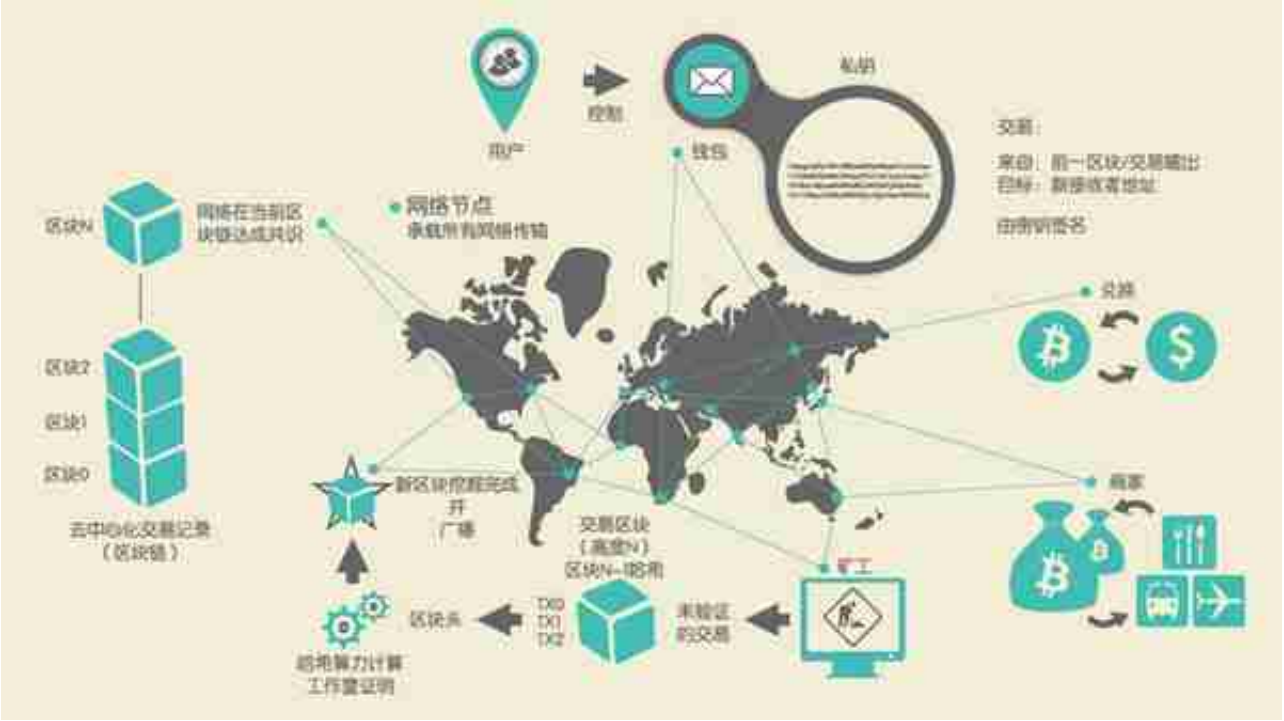


相信很多读者都对第一笔比特币的来历不甚了解，那么我们就先科普一下整个系统中的第一笔比特币（50个BTC）是如何产生的。2009年中本聪挖出了创世区块（区块高度#0），区块中仅有一笔交易，这是笔特殊交易，称为创币交易或者Coinbase交易（用来奖励记账者）。
创币交易特殊之处在于没有交易输入，而是被一个Coinbase数据替代，矿工（记账者）可以在其中随意填充任何数据，交易输出则是指向矿工地址的50枚BTC（每四年减半一次）。这样系统中的第一笔比特币就产生了，并奖励给了中本聪本人。

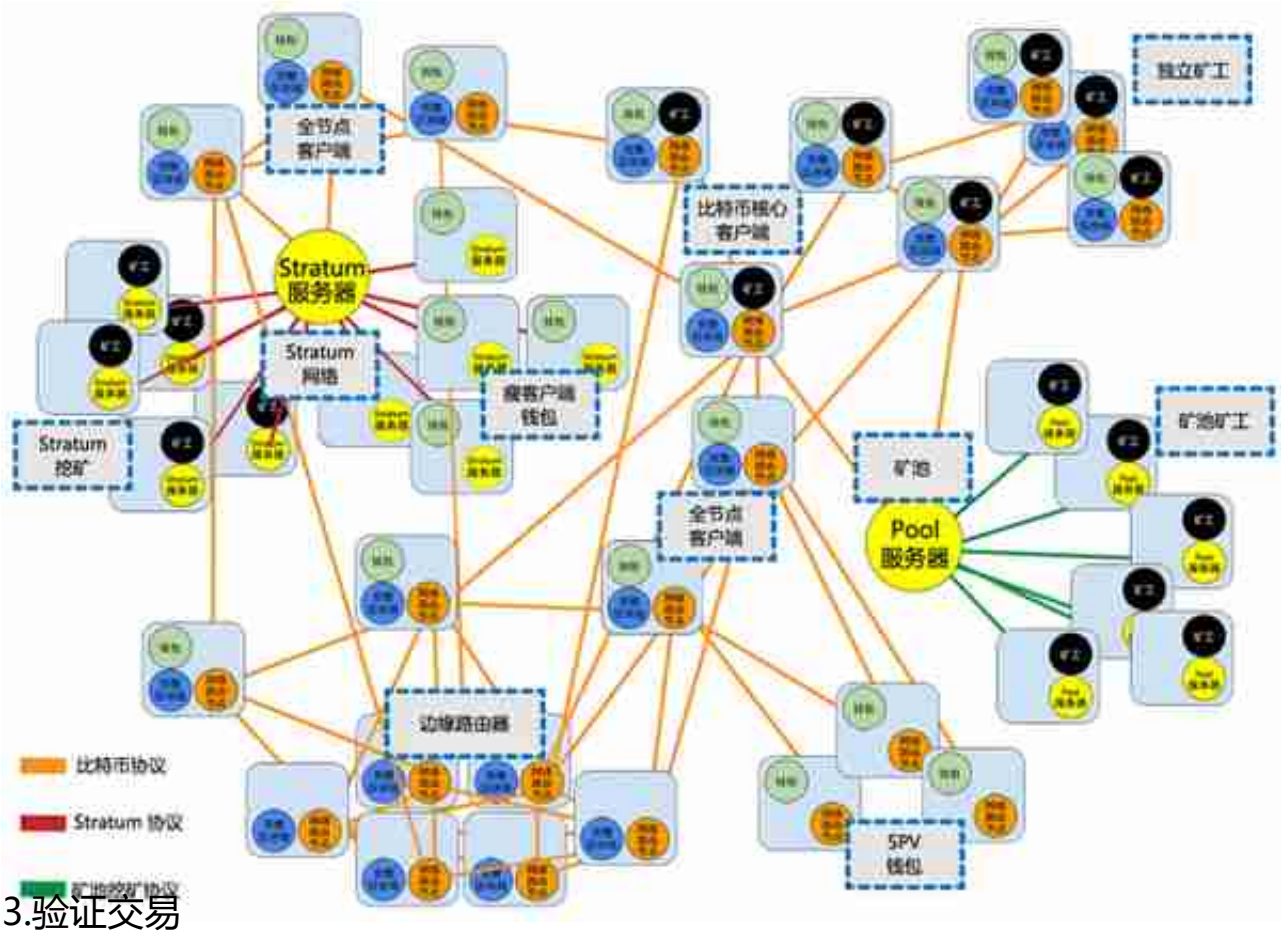
当时金融危机的风波愈演愈烈，于是中本聪在创世区块的Coinbase中写下了这样一句话：“The Times 03/Jan/ 2009 Chancellor on brink of secondbailout for banks”。这句话是泰晤士报当天的头版文章标题，引用这句话，既是对该区块产生时间的说明，也可视为对传统金融体系的一种无声嘲讽，由此宣告了比特币时代的到来。

创世区块启动后，比特币开始在系统中流通起来，接下来我们聊聊比特币具体是如何流通的。简单来说比特币的完整交易过程可以划分为创建交易-广播交易-验证交
易-竞争记账-
广播区块-验证区块-
写入区块链（交易成功）这7个阶段，下面来依次介绍每个阶段的详细过程。

1.创建交易

用户A（付款者）可在自己的比特币钱包中发起转账，需要输入比特币数量（并写下愿意支付的交易手续费，大多数钱包自动计算并计入交易费）和收款地址（付款地址钱包会自动处理），然后用自己的私钥进行加密签名（签名是为了标识这笔比特币的所有权，其他人只要通过发起者的公钥即可校验真实性），这样一笔交易就创建成功了。

这里提下UTXO，它是比特币交易的基本单位，是未经使用的一个交易输出，易于理解的说就像是账户的余额。UTXO不能再分割，1 个UTXO可以是 1 “聪” 的任意倍，就像美元可以被分割成“美分”一样，“分”就不可以再分割了。UTXO被记录于区块链中，比特币网络监测着所有可用的UTXO。



3.验证交易

每一个节点在校验每一笔交易时，都需要验证很多数据，主要有交易输入、交易输出、交易签名等。
交易验证通过后，每个比特币网络节点会将这些交易添加到自己的内存池中，内存池也称作交易池，用来
暂存尚未被加入到区块的交易记录。
而挖矿节点除了收集和验证交易以外，还会定期到自己的交易池中把收集到的交易一并取出来（按优先级取出，交易的优先级是由所花费的UTXO “块龄” 决定的，

输入值高、“块龄”大的交易拥有更高的优先级），将其打包到一个候选的区块中。

4.竞争记账

区块打包完
后，矿工就要开始争夺
记账权了，也就是我们常说的挖矿。
挖矿的目标是找到一个使区块头hash值小于难度目标的Nonce（区块头中存在一个随机数）
，即POW工作量证明机制（工作量证明的难易程度是由hash值0的个数N来决定的，比特币系统会根据当前整体的运算速率来进行调整N，从而保证平均每10分钟生成一个新的区块）。

挖矿节点通常需要尝试数十亿甚至数万亿次的hash运算，才能找到一个满足条件的Nonce值。找到后矿工会立即向全网进行广播，让其余节点进行验证，同时获得记账奖励的BTC（这里存在一个区块成熟时间，指矿工产生一个新区块得到25BTC收益后，要等过了100个块后，才能使用这些币）。

比特币的相关内容就说到这里了，相信大家已经对比特币有了自己独到的认识。那么从下期开始我将带领大家进入区块链的世界，揭开这个“超级颠覆者”神秘的面纱。

（本文来自得得号：夜里不懂天的白，下期预告：《重塑价值—初识区块链》）