这篇文章写给想弄明白比特币到底是什么，但又看不懂白皮书的朋友。这不是一篇爽文，但是也不难懂，有初中数学基础就够了。花10分钟读完之后，很多问题你会有自己的答案，比如：

“比特币有什么用？”

“要不要去梭一把？”

比特币到底是什么？99.99%的人说不清楚这个问题

每顿饭吃完都要用现金分账的话，太繁琐，而且八戒又经常忘带钱。悟空就提议：以后大家之间的经济往来，统一先记到一个账本上，月底发了工资再统一结算。比如今天大家一起喝酒，师傅买单，花了400块。老规矩，AA，账本上就记下这三笔：

悟空 要付给 师傅 100元

八戒 要付给 师傅 100元

沙僧 要付给 师傅 100元

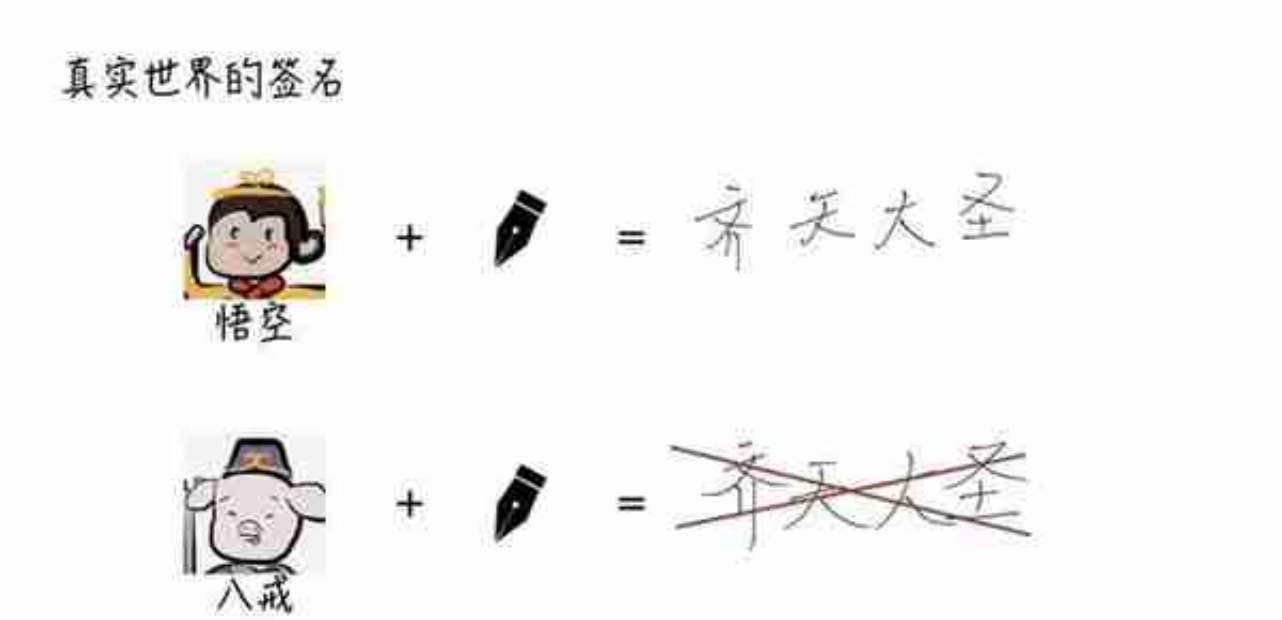
明天大家一起捏脚，沙僧买单，花了800块，也记上：

悟空 要付给 沙僧 200元

八戒 要付给 沙僧 200元

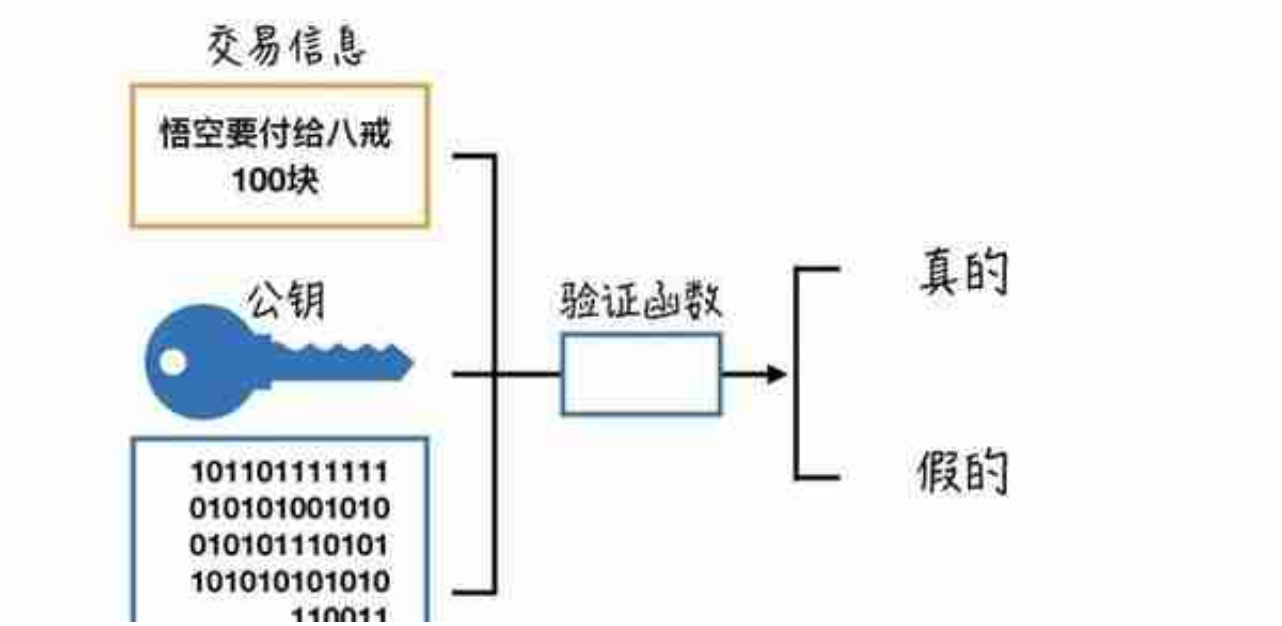
师傅 要付给 沙僧 200元

到月底了，大家把账本上的记录一汇总，再用现金结清就好了。如果这个月就两笔（这是不可能的），现金结算是这样的：



电子签名就不同了。理论上，电子签名就是一串0和1构成的字符，电脑是可以直接复制的，别人就可以仿造你的签名。

如果你想对一笔交易签上你的名字，表示你认可它，你需要做如下操作：以这笔交易包含的信息和你的私钥为两个变量，输入签名函数，得出的结果就是对应这笔交易的签名，一个256位的二进制数字。



理论上说，这个验证函数提供了一丝伪造签名的机会。你可以拿各种可能的组合去试，输入到验证函数中，撞上结果为真，那这个签名就对了。

问题在于，这是一个256位二进制数的签名，可能的组合数是2的256次方，大概是10的80次方，差不多和全宇宙的原子数是一个量级，一秒试一万次，你算到宇宙灭亡也算不完。

所以，如果经过验证这个签名为真，给出签名的这个人肯定是交易的主人没跑了（或者上帝本人）。

悟空说，有了电子签名，以后每笔交易都需要交易的主人签上自己的签名才算有效。

比如这条交易：沙僧 要付给 八戒 1000元 交易的主人是沙僧 那就得沙僧拿自己的私钥去生成针对这条交易信息的签名并且签上去，这条交易才算有效。其他人可以用沙僧的公钥去验证，看这个签名是否为真。这样一来谁都不能作弊了。

另外，为了督促八戒改邪归正，悟空还加了一条，大家先交1000的保证金，之后谁的账户余额降到0了，就不能继续交易了，也就是不能透支。

问题解决了，几个月过去，大家发现在新规则下，每个月不用现金结算也可以了，这个账本变成了小银行，账本上的余额就是每个人在银行账户里的钱。只要不透支，不需要现金大家也可以互相交易了，借钱还钱都可以靠记账解决。不妨把这个账本上的钱叫做西游币，兑换起来就是1元=1西游币

到这里，你会发现，账本在某种程度上已经扮演了货币的角色。系统规则也演变成了2.0版本：

1.每个人都能在账本上记一笔交易，不过必须交易主人签名才有效

2.不能透支

有一天，师傅突然给悟空出了个难题，现在这个系统虽好，但是也有隐患，如果控制账本所在的网站的人想作弊，谁去监督他呢？有没有可能每个人都有一个账本，各自记各自的，然后互相同步，互相监督？

八戒提出质疑，那要是大家记得账不一样，以谁的为准呢？

众人陷入了沉思。大家都记账的确可以免除对特定中心的依赖，但是如果有人作弊，导致大家的账本不一致，这时候怎么解决争端呢？

只见一片紫气东来，中本聪现身了。他丢下一张8页纸的天书，飘然而去。悟空拿起书，却见书中写道：

谁的算力大，谁说话算话。

悟空被瞬间点醒，开始给大家讲新方法：

咱们先分头记账，每隔一段时间，咱们就碰头核对下账本。怎么核对呢？玩一个数学游戏，就是找到一个对应账本的幸运数字，唯一的方法就是靠猜，谁的计算力大谁就更有可能猜中，而且猜中有奖励。猜中之后，这次核对的账本才算确定了，大家都以这个账本为准。

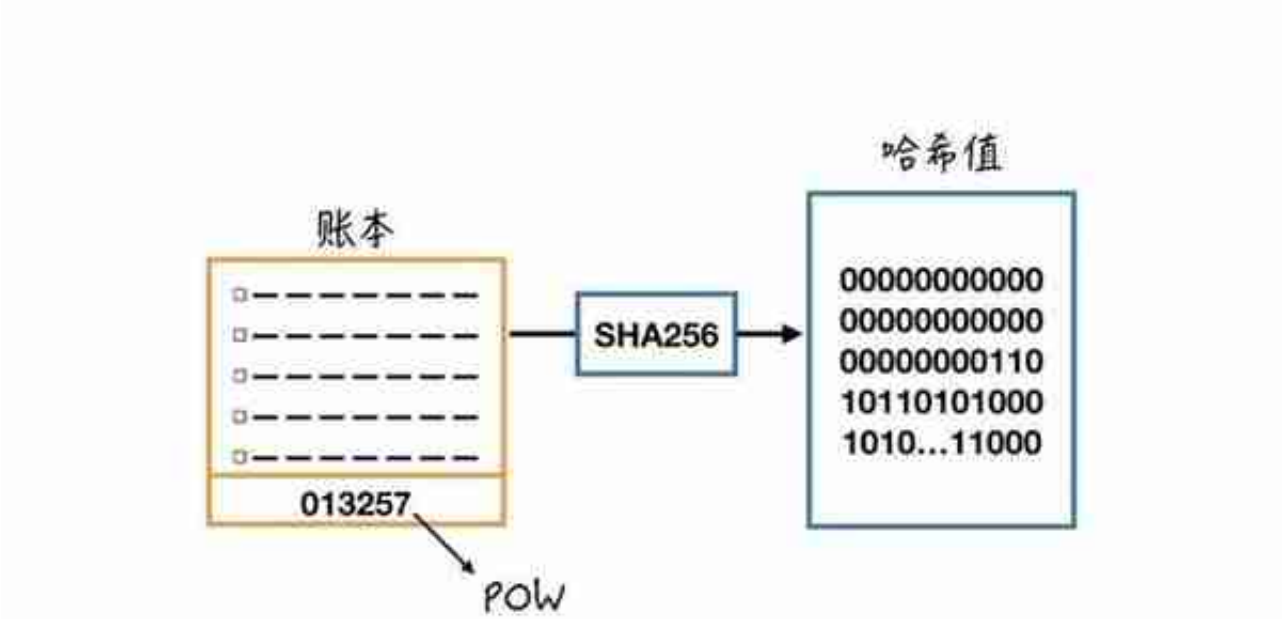
如果核对的时候，发现八戒写的账本有个地方和其他人都不一样，怎么办？没关系，还是玩这个猜数字的游戏，只要作弊的那一方拥有的算力没有过半，没有作弊的一方就会获胜，因为它的算力更大。最后大家还是会以游戏胜利者也就是正确账本为准。

大体就是这样，具体细节是怎样的呢？到这里，我们已经准备深入到比特币的核心思想了。为了彻底搞明白，我们需要先介绍几个不那么常见但是非常有用的概念。

先来介绍关键的大杀器：SHA256算法。

SHA256是一种密码哈希函数，输入任意一段信息，运行SHA256函数，输出的结果会是一串256位的2进制数，这个数字就是这段信息的哈希值或者摘要，可以理解为这段信息的特定ID。

世界上所有信息都有自己特有的哈希值，一一对应，绝不重复。



如此一来，由于SHA256的特性，找到这个数字只能靠试错，成功机会又特别低，2的30次方分之一，也就是说，大概 得试上十亿次，才能成功一次。靠买彩票中五

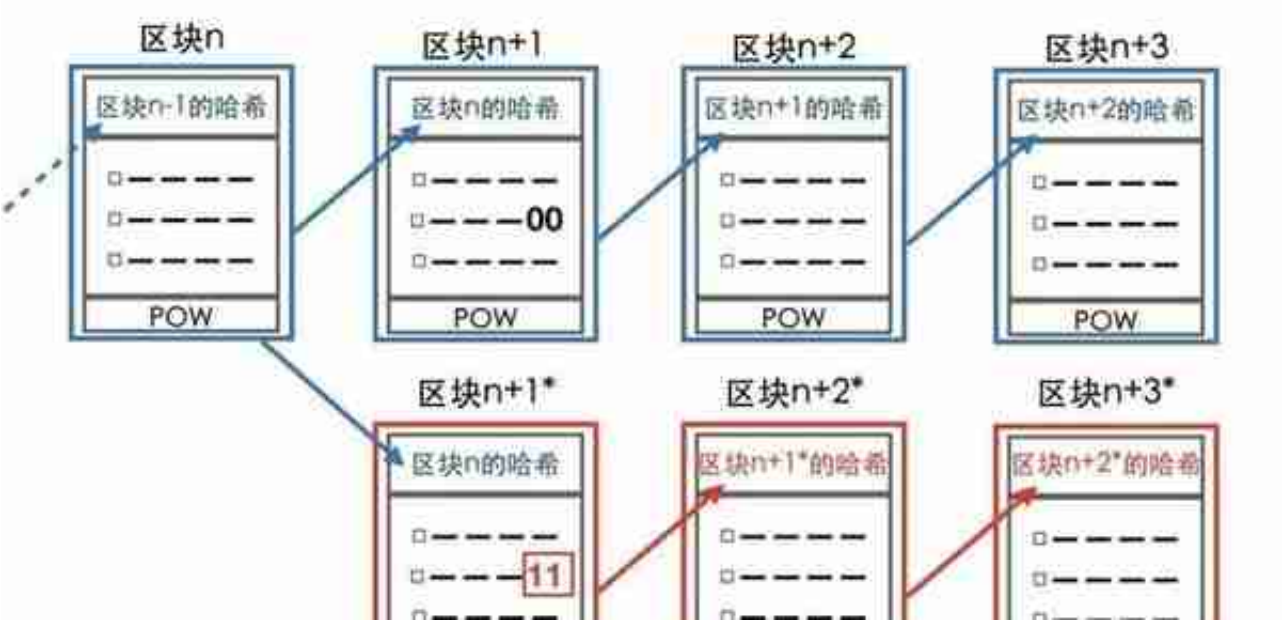
百万就是这个游戏的翻版，不过中五百万的几率还是不错的。

一旦有人找到了这个数字，其他人要想验证这个数是否正确，只需要算一遍就可以了，非常简单。这一点和买彩票也很像，你有没有中奖，查一下就行。

这个幸运数字就叫Proof of
work
，工作量证明。如果你能找到这个特定数字，就说明你投入了足够的时间和算力（因为也没有其他方法了），同时其他人还能很简单的验证这件事情，不用重新花力气再算一遍。那么为什么会有人愿意投入时间、机器和电费来玩这个游戏呢？因为我们设计了奖励机制，猜中这个数字的人会获得一定数目的比特币作为奖励，那一页账本上会加一条，谁谁谁获得2个比特币。

有了这种游戏，人们就会自发的去验证比特币网络里的交易是否有效，而且唯一的方法就是投入时间和计算力去猜。初看起来可能并不高明，浪费这么多资源就为了玩数字游戏？别急，一会你会发现别有洞天。

最后要介绍的是blockchain，区块链。这个词是怎么来的呢？比特币把账本分成了很多块，每块上记录一定数量的交易，每一块叫做一个block，区块。每个区块的底部会附上对应的幸运数字，工作量证明。同时，在区块的顶部，还会附上前一个区块所包含信息的哈希值。于是区块就连成了一条链。其实区块链就是一种结构比较特殊的账本，改变其中一页，整本都会出问题。



第二，不同区块之间的位置代表了不同交易发生的先后顺序，如果改变区块的位置，因为同样的原因，整条链也会变得无效。这一点保证了交易时间记录的准确性。

最困难的部分介绍完了，我们可以歇口气回顾一下：

一个大杀器：

SHA256算法可以让我们输入任意一段信息，得到一个对应的数字，这个数字就是这段信息的哈希值，就像个人ID一样独特。反过来，通过哈希值来算出对应的信息，只能靠猜，而且很难猜。

一个数字游戏：

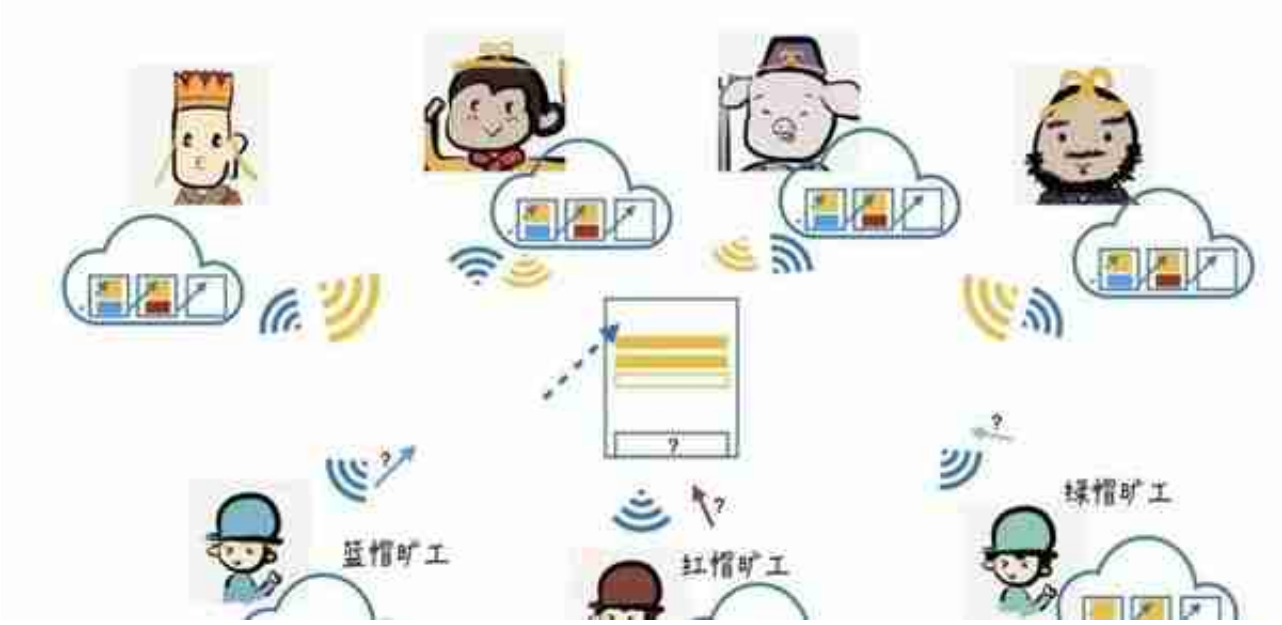
对每一页账本，我们可以找到一个幸运数字，使得它的哈希值前30位都是0。这个数字很难猜，猜中的会获得比特币作为奖励。和买彩票很类似。

一个设计精妙的结构：

区块链就是把整个账本分成许多区块，前一个区块的哈希值写到下一个区块的顶部，以此把所有区块关联成一条链，改变任意区块的信息或者位置，都会影响整条链。

说完这三件事，我们可以来具体看看比特币是怎么运行的了。

对于普通用户来说，完成一笔交易，就把这笔交易的信息广播出去。同时，有一些用户会不断收听整个网络里的交易信息，把这些交易信息打包成区块，然后飞快的猜那个幸运数字。一旦有一个人猜到这个幸运数字，就会获得几个比特币作为奖励。这个区块也被证明有效，并再次广播到全网，被大家记下来。这些不断猜数字的用户就是我们常听到的“矿工”，猜数字的过程就叫“挖矿”。



矿工需要收听全网的广播信息，普通用户则只需要收听矿工广播出来的验证过的区块，同步到自己保存的区块链上。如果收听到两个区块不一致，到底听谁的呢？中本聪给出的方法是，算力为王，哪个区块背后的算力更大，或者哪个区块所在的链更长，就听谁的。

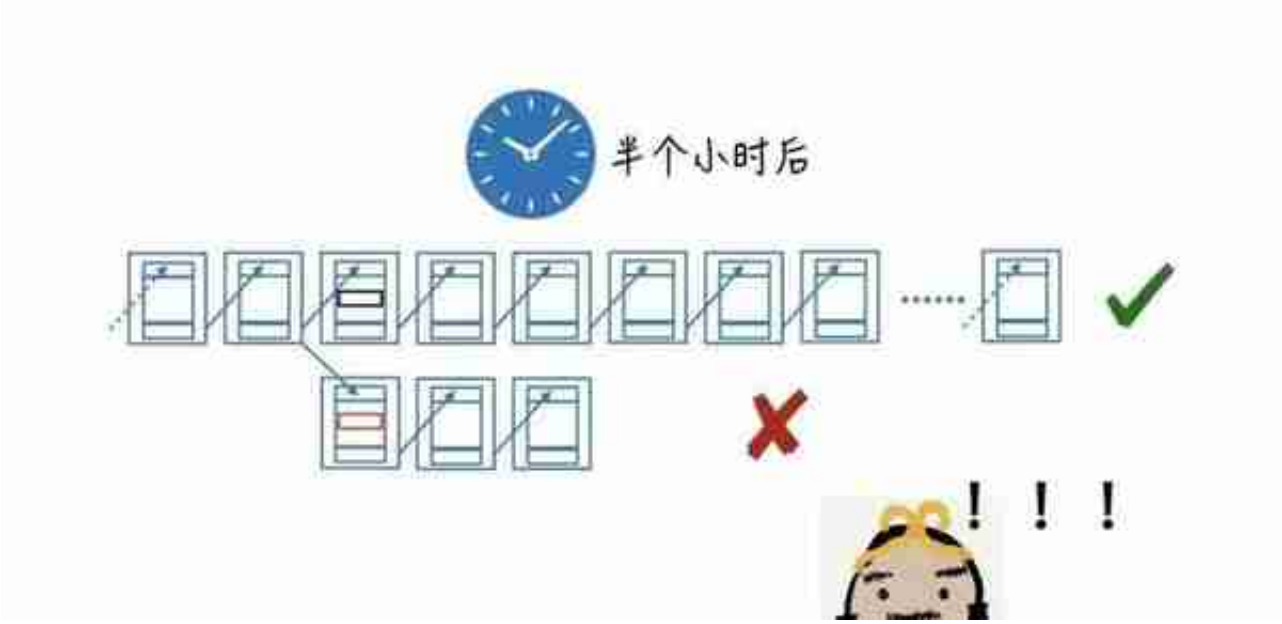
为什么这么做有效呢？我们再次绕后从反面来破解这个问题。想想看，如果你想在比特币网络中作弊，具体过程是怎样的？需要什么条件才能实现？

假设八戒想作弊，大家一起吃了饭，师傅买单，按道理八戒应该给师傅100块。其他矿工都在区块里记上了这一笔：

八戒 要付给 师傅 100元

同样是矿工，八戒却在区块里抹掉了这笔账，打包出了一个“不一样”的区块，验证之后发给了老实的沙僧。

沙僧那边收到的消息在这个节点上开始分裂了。八戒发给他的区块单独形成了一条链，其他矿工的区块则形成了另一条链。



也就是说，当你收到两个不一样的区块时，先别急着决定听谁的，让区块链再飞一会，等到其中一条领先另一条至少六个区块以后，基本就板上钉钉了。

当然，如果八戒自己掌握了全球一半以上的算力，自己成了多数派，那这个系统就崩溃了。但是由于各种复杂的现实原因，这个条件很难达成。

比特币的这个算力为王的机制，有点像投票表决。大家意见不一致的时候就通过投票来达成一致，票数为王，少数服从多数。如果你想作弊，不是不可以，但必须获得过半数的票。

到这里，比特币的完全体诞生了，系统规则3.0版：

1. 只要投入算力和时间，每个人都能记账和验证

2. 区块链分裂时，保留算力大的那条链

以上就是比特币的基础运行原理了。我们从原始的现金交易，到电子签名和中心化账本，再到更先进的分布式账本+POW+区块链，短短十分钟走完了人类货币演化史。未来人类的货币金融体系会如何演化，比特币的儿子孙子命运如何，也许你我都有一个模糊的答案。

来源：橙皮书