

这段时间，估计你已经看了不少关于区块链应用前景的解读，可能还琢磨了一些区块链概念股的行情走势。

但如果没猜错的话，你可能还是不太清楚，区块链它到底是个什么链。

今天，咱们就从区块链呱呱坠地那一刻说起，把它搞得清清楚楚、明明白白。

神秘极客的天才设想

说到区块链，不得不提它的孪生兄弟——比特币。



时光倒流回整整11年前。2008年 11月 1 日，世界正笼罩在金融危机的巨大阴影中。那天，一位自称“中本聪”的神秘极客群发了一封电子邮件。

邮件中附着一篇论文，标题是：“比特币：一个点对点电子现金系统”。

中本聪在邮件中说，他正在研究一种新的电子现金系统，这种系统完全是点对点的，无须任何可信的第三方。大约半个月后，中本聪又马不停蹄地公布了比特币系统

的源代码。

2009年1月3日，一个有趣的发明横空出世。中本聪在服务器上生成了第一个比特币区块，这就是所谓的“比特币创世区块”。从此，比特币系统正式开张。

说到这里，不妨停下来想一想，咱们在现实生活中是怎么进行现金交易的。

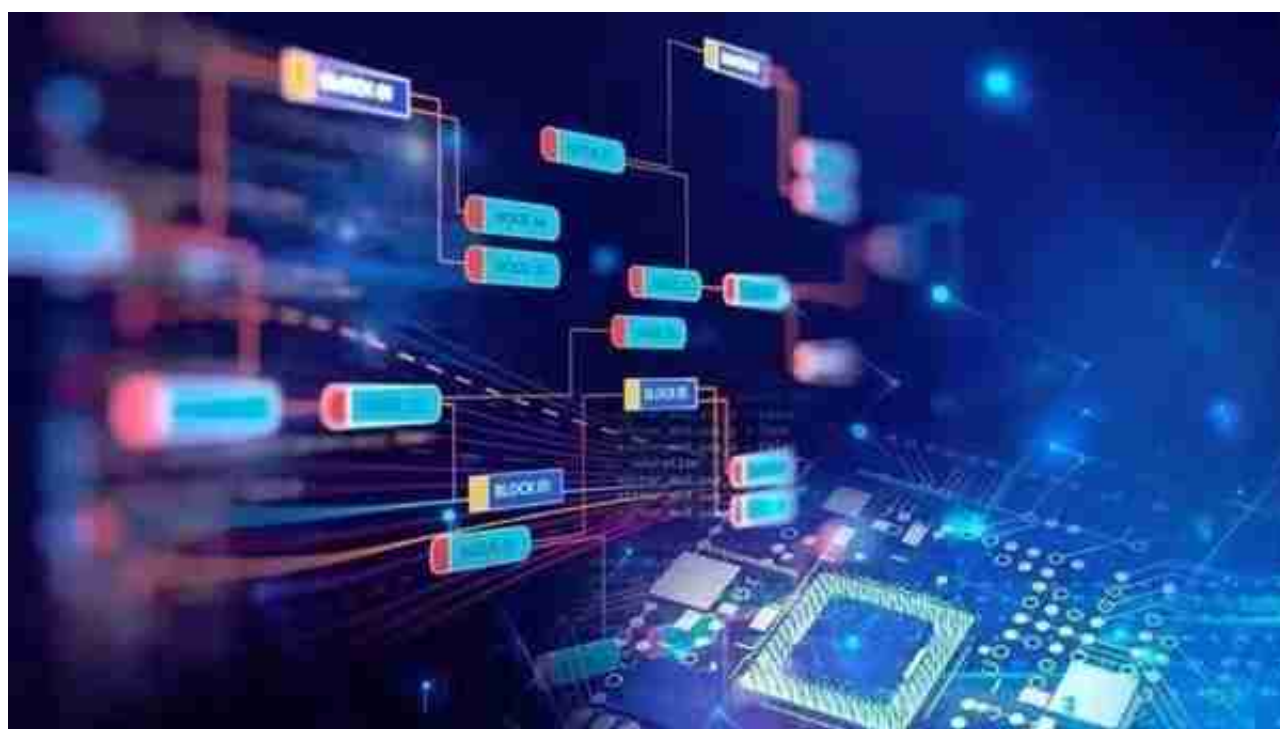
假设你向朋友借了1万块钱，并答应一个月后还钱，你可能会选择用银行卡转账还款。银行负责在你的存款账户中减掉1万块，在你朋友的存款账户中增加1万块。

在这里，银行是负责记账的机构。你之所以选择银行转账，潜在原因是你相信它比较可靠，会帮你把1万块钱转给朋友。

可是，在数字世界里，发明一套货币，就是另一回事了。

比特币游戏的幕后英雄

下面，我们来看看中本聪是怎么设计这个数字货币游戏的。



首先，中本聪希望点对点直接交易，绕开银行这个第三方。这个问题好办，那就不设银行呗，用户通过一套独特的机制自己发行货币，相互之间直接交易。

但这又带来另一个问题，没有银行作为可靠的中介负责记账，用户又相互不认识，

怎么保证交易时没人耍赖呢？

比如，在数字世界里，电子文件可以轻松复制，10块钱的数字货币，动动鼠标复制粘贴10次就变成100块，岂不乱套了？

解决这个问题，就需要提供一个让大家互相信任的机制。

比特币系统采用的方法是，让所有交易过程都按照时间顺序公开透明地记录下来，这些记录是永久性的，不能篡改。这样就没办法做一些偷偷摸摸的事了。

凭借这些机制，比特币系统成功运转起来。

这个系统以数据块为单位存储数据，这就是区块（Block）。大约每隔10分钟，就会有新的区块增加上去。每个区块都记录着比特币的详细交易过程，而且带着时间戳。不同区块之间按照时间顺序、通过某种算法相连，这就是链（Chain）。

它们合起来，就被称为“区块链”（Blockchain）。

就这样，区块链伴随比特币的诞生，落地生根了。如果说比特币是受到瞩目的台前明星，区块链就是负责在底层技术上提供信任机制的幕后英雄。

记账方式的全新变化

虽然身居幕后，区块链的才华很快被挖掘出来。

用专业术语来讲，区块链是一种分布式账本技术。要想理解它，咱们还是举个最简单的例子吧。

假设原来你家是这样记账的：你和爸爸、妈妈分别有一个账本，你们各自记各自的花费，每个月底一起统计家庭总开销。

但爸爸喜欢买烟，妈妈喜欢屯化妆品，你喜欢买零食，你们可能都会有意无意地少记几条，有时还会在账本上涂改。所以月底核对账本时，总是和家里的实际支出有点出入。

为了改变这种情况，你们重新买了一个新账本，你和爸爸、妈妈三人共同用一个新账本记账，并且互相提醒、监督，一起核对每一项花费。

同时你们还约定，一旦把花费核对清楚记上去后，就不许涂改和删掉。尝试了几个

其实，在咱们身边，已经有很多场景用上了区块链。

比如，平时去菜市场买东西，你可能会担心鱼虾、蔬菜是否安全。有的公司从中看到商机，把养殖户和鱼塘的数据搬到区块链上。这样你就能知道买的鱼来自哪个鱼塘，会吃得更加放心。

再比如，朋友圈经常会出现为重病患者筹款的链接，在捐款时，你可能多少有些顾虑：患者情况真实吗？捐款真能送到病人手里吗？

为了消除这些顾虑，有些互联网公益机构用上了区块链，让你清清楚楚地查看捐款的使用步骤。假如审核发现患者情况不属实，区块链系统将自动把捐款退还你的账户。

未来，区块链可以给我们的生活带来哪些改变？

可以想象的是，当社会的各个领域广泛用上了区块链，它将成为信息时代的重要基础设施，能解决很多当前令我们头疼的事儿。

比如，区块链将使无数信息的孤岛被“链”在一起，看病不必因为换个医院就重复检查，创业者不必为了办一个手续跑多个部门；很多交易不再需要第三方担保，消费者不再担心押金无法退还，创作者不必担心作品被盗用却一无所得.....

10年前横空出世的区块链，

10年后将开辟出什么样的新世界？

冰山才露一角，

咱们继续期待！