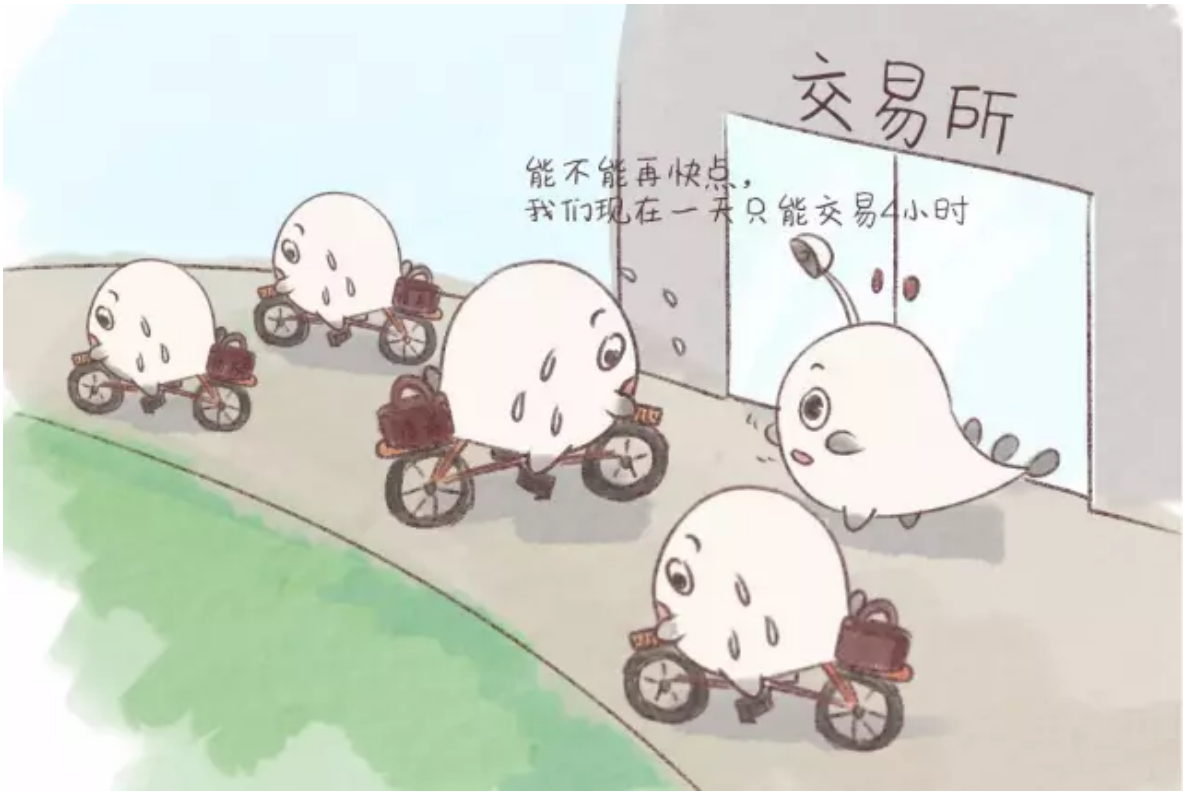
图解区块链是什么

> 中共中央政治局2019年10月24日下午就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。
>
> 有观点认为，区块链与人工智能、大数据是金融科技三大支柱，区块链或许会是10年后的“互联网”
>
> 下文用简洁的语言和图片，向大家解释究竟什么是区块链技术。

近年来，包括摩根大通、花旗集团、高盛集团、纳斯达克等在内的金融巨头，都表达了对区块链技术的热衷。这些巨头们热衷的区块链技术，又被称为分布式账本，那么分布式账本究竟是什么呢？我们先从另外一件事说起。

区块链与骑自行车的人



华尔街上骑自行车的人

在纳斯达克成立之前，人们用自行车驮着装满债券的包，在华尔街骑来骑去，目的就是尽快完成清算。后来业务越来越多，自行车就忙不过来了。20世纪60年代，华尔街每周只交易4天，每天4个小时，就是为了能让清算速度跟上交易量。

这样发展下来，大家觉得不行啊，自行车肯定跑不过计算机。1971年，有人就开会说，咱们想想办法吧，于是提出了DTC（美国存管信托公司）清算系统。这个系统的办法就是所有的交易都要在系统内进行，包括经纪人也要接入这个系统，现在纳斯达克还在用。

中心化的DTC清算系统

这个系统提高了交易的效率，但是并没有改变交易的中心化结构。当交易足够多、经纪人足够多的时候，这个系统也有瘫痪甚至崩盘的危险。

于是专家们想，自治式、分布式的系统会不会好一点呢？答案是肯定的。**区块链就是一个分布式的账本，每个节点都可以显示总账，然后维护总账，而且不能篡改账本，**除非你控制了超过51%的节点，但这是不可能的。

再简单一点，假如你们家里有个账本，让你来记账。在以前，就是爸爸妈妈把工资交给你，让你记到账本上。中间万一你贪吃，想买点好吃的，可能账本上的记录会少十几块，然后你想买个手机，账本上就少记录几千块。这只是举一个例子，我相信小时候大家都想从爸爸妈妈的口袋里拿点钱来花。

中心化的家庭账本

有了分布式账本后，上述说的问题就不会有了，因为你在记账，你爸爸也在记账，你妈妈也在记账，他们都能看到总账，你不能改，爸爸妈妈也不能改，这样想买烟抽的爸爸和想贪吃的你都没办法啦。

分布式家庭账本

区块链本质上是一个去中心化的分布式账本，其本身是一系列使用密码学而产生的互相关联的数据块，每一个数据块中包含了多条经比特币的网络交易有效确认的信息。

中心化与去中心化

前面我们说到了区块链的本质是一个去中心化的分布式账本，那么，所谓的中心化又是什么呢？我们首先思考这样一个问题，你要在网上买一本书，交易流程是什么？

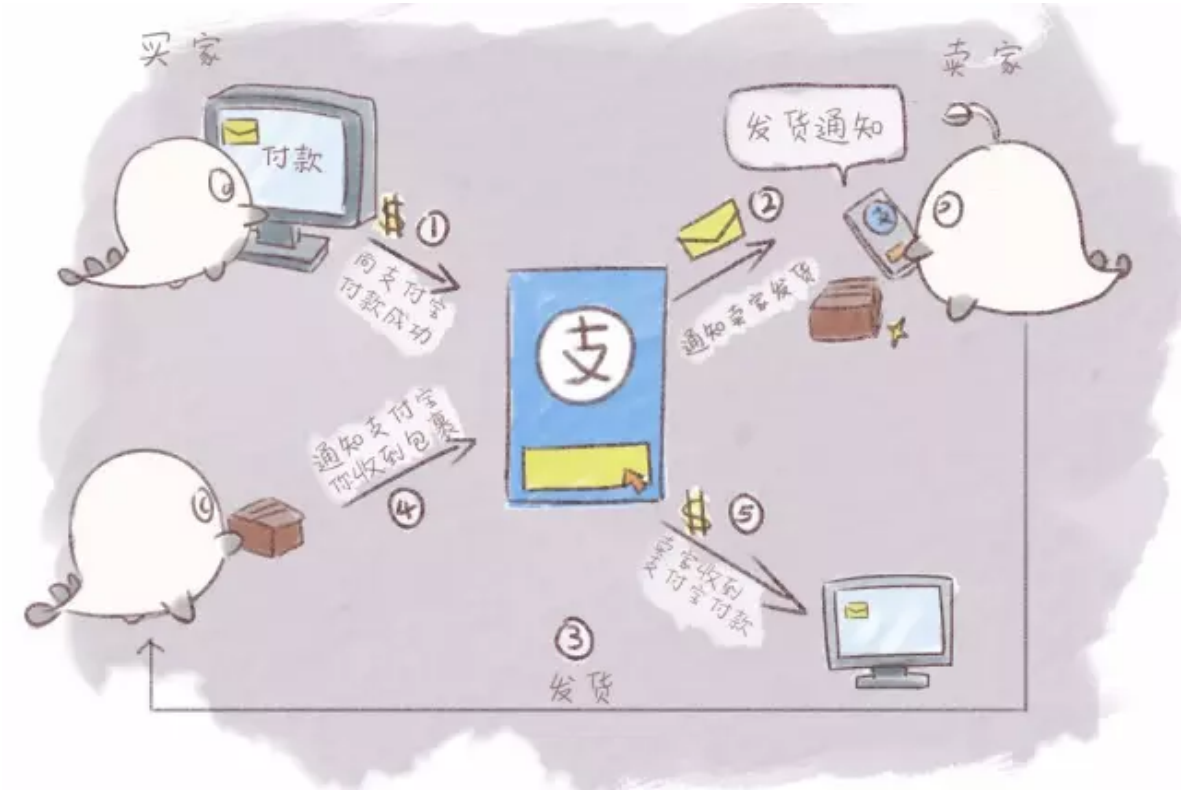
第一步：你下单之后把钱打给了支付宝。

第二步：支付宝收款后通知卖家可以发货了。

第三步：卖家收到通知后给你发货。

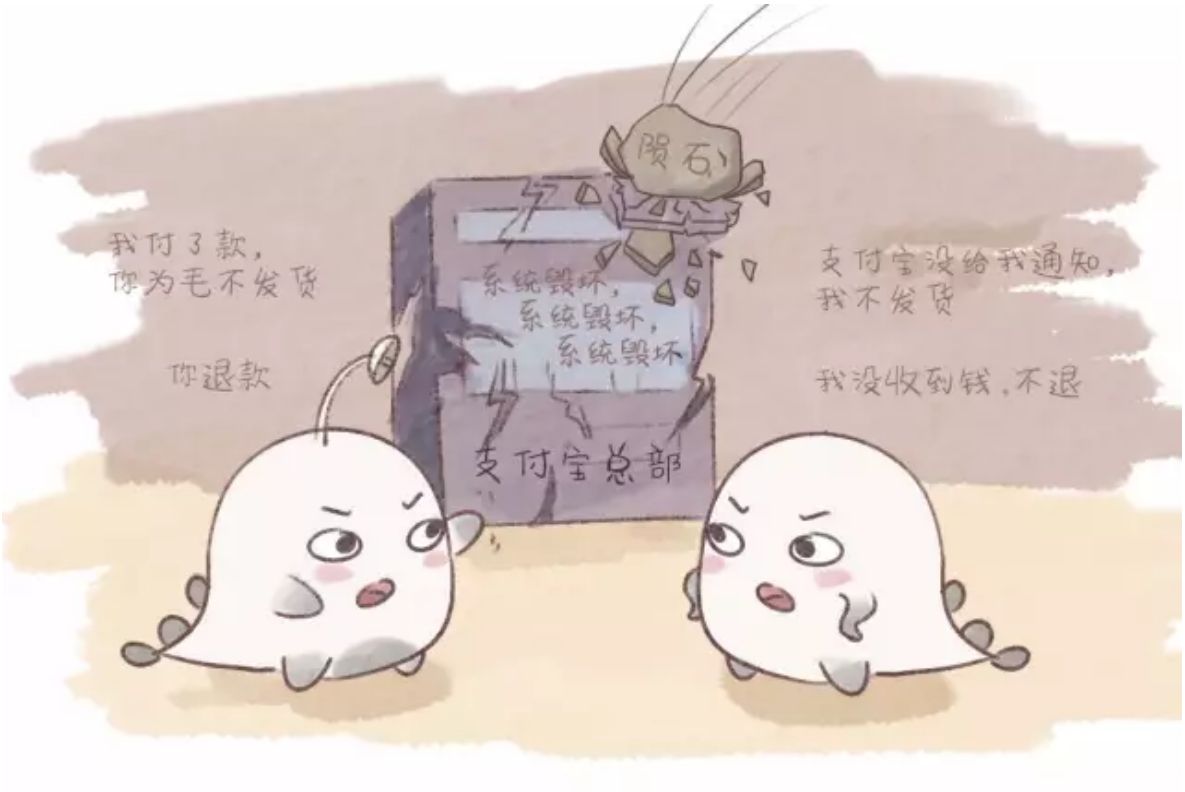
第四步：你收到货之后很满意，于是确认收货。

第五步：支付宝收到了你的通知并打钱给卖家。



中心化的交易流程

我们可以看出，在这个过程中，虽然你是在和卖家交易，但是整个交易都是围绕支付宝展开。因此，如果支付宝系统出了问题，比如天上降下来一块陨石，把支付宝的服务器全砸了，或者由于全球经济危机支付宝倒闭了，无奈的支付宝只好淡然地表示不存在这笔交易，那么这笔交易就会以失败告终，到时候买家卖家就会纠缠不清，双方无法自证。



中心节点毁坏会导致交易失败

模拟一个区块链小城市

为了说明去中心化的区块链是如何运行的，我们先把整个去中心化的分布式结构简化为一个极端的情况来探究。我们假设有一个去中心化的小城市，在这个城市里有5个可爱活泼的小伙伴，他们互相借钱的时候，是这么干的：

假设B向A借了1块钱，这个时候，城市里的人怎么办呢？A在人群中大喊：“我是A，我借给了B1块钱！”B也在人群中大喊：“我是B，A借给了我1块钱！”

此时城市里的其他人C、D、E都听到了这些消息，他们拿出了手中的小账本并默默记下：“某年某月某日，A借给了B1块钱。”

去中心化城市的记账

当我们把一个去中心化的模型极度简化之后，我们就会发现，在这个只有5个人的城市中，已经建立了一个去中心化的系统，这个系统不需要银行，也不需要支付宝。这个模型不需要信任关系，也不需要一个拥有公信力的组织。当分布式结构中的每个人都记账的时候，篡改账本是不可行的。比如B突然不认账了：“我不欠A的1块钱！”这个时候，人民群众C或D或E就会站出来说：“不对，我的账本上明明记录了你在某年某月某日向了A借了1块钱，并且没有查到你还款的记录。”

去中心化账本无法篡改

说到这里，你有没有发现一个问题，在这个模型中，所谓的1块钱根本不重要，也没有人在意，“1块钱”已经变成了一个变量，它可以被替换成任何概念，只要大家承认这是一个有价值的东西即可。

比如A在这个城市中大喊一声：“我创造了一个巴拉拉能量！”城市中的其他人都听见了，于是大家纷纷在自己的小本子上记下“某人有一个巴拉拉能量”，大家甚至不用知道巴拉拉能量是什么，A竟然真的有了一个巴拉拉能量。

A还能干什么呢？A可以再大喊一声：“我给了B一个巴拉拉能量。”只要城市中的B、C、D、E，即城市里的所有人都承认了这个交易，那么这个交易就真的成立了，虽然现实生活中并没有巴拉拉能量。

巴拉拉能量的流通

小城市里的几个问题

当然，区块链的世界不会这么简单，它还有其他的规则来相互制约，我们先来解决下面这几个问题：

问题一：凭什么帮你记账？**

凭什么你对着天空大喊一声，别人就要帮你记账，别人的时间不要钱吗？别人的小本子不要钱吗？于是，为了让大家都帮我记账，我增加了一条新的规则，我决定给第一个听到我喊话并且将其记录在小本子上的人奖励。奖励机制也很简单，第一个听到我喊话并记录下来的人，可以得到一个巴拉拉能量的奖励。

这个巴拉拉能量不是白给的，是对你劳动的报酬，就像打工可以挣钱一样，你帮我记账，整个系统都会给你报酬。你要做的事情，有这样几点：

首先，你要抢在所有人之前听到了我的喊话并记在了自己的小本子上；

记录之后，你还要马上告诉整个城市里的人——这句话我记录完了，你们再记录也没有用了，别人就会放弃这笔赚钱的生意；

与此同时，你还要做一件事，就是给自己的记录加一个独一无二的编号，然后把记录和编号一起喊出来，于是，下一个人再记录的时候，就会带着这个记录和独一无二的编号继续下去。

记账获得奖励

在这条新的规则开始实行之后，一定会有这样一些人，他们为了得到巴拉拉能量，开始屏气监听周围发出的各种声音，只为了能在第一时间记下一条新的记录。

这个时候，对区块链有所了解的读者是不是想到了这样的名词——“比特币挖矿”。没错，这就是比特币挖矿的简单说明。

关于比特币挖矿的话题，知乎用户“玲珑邪僧”的一篇文章举过一个更生动的例子，大致是这样的：单身男士们要找女朋友，“国民岳母”说，我有好多肤白貌美、乖巧可爱的女儿，这样吧，我给你们出一个旷世难题，解出一个就给你们其中一个姑娘的微信号。

“国民岳母”的旷世难题

于是，单身男士们疯狂竞争，想破脑袋去解这道旷世难题。只要其中一位单身男士解出一道题，就立马得意扬扬地昭告天下，示威全部单身男士，这个姑娘的微信号是我的啦，先到先得，你们放弃吧。其他单身男士虽然已经算到一半了，但是没有办法，速度不够快啊，只好立马去解下一道题。

解出难题获得奖励

同时，首个成功破解旷世难题的幸运的单身男士不仅不用付一二十万元的彩礼，被其才华征服的“国民岳母”还会给这位单身男士一笔巨额财产做嫁妆，也就是比特币挖矿中的比特币奖励。

问题二：分叉问题听谁的？**

在这一段的论述中，我们引用了知乎用户“汪乐-LaiW3n”的说法。在这个广阔的小城市里，一定还会存在这样的问题，B和C几乎同时记录完了，于是同时向天空大喊了一声，“这个编号89757的巴拉拉能量归我了”。但是，由于这个城市太广阔了，有的人会认为这个编号89757的巴拉拉能量归B，也有的人认为这个编号89757的巴拉拉能量归C，但是编号89757的巴拉拉能量只有一个啊，只有一个人能得到，怎么办呢？一人一半？当然是不可能的，这个时候我们会采用更原始简单的规则来解决，谁长听谁的。

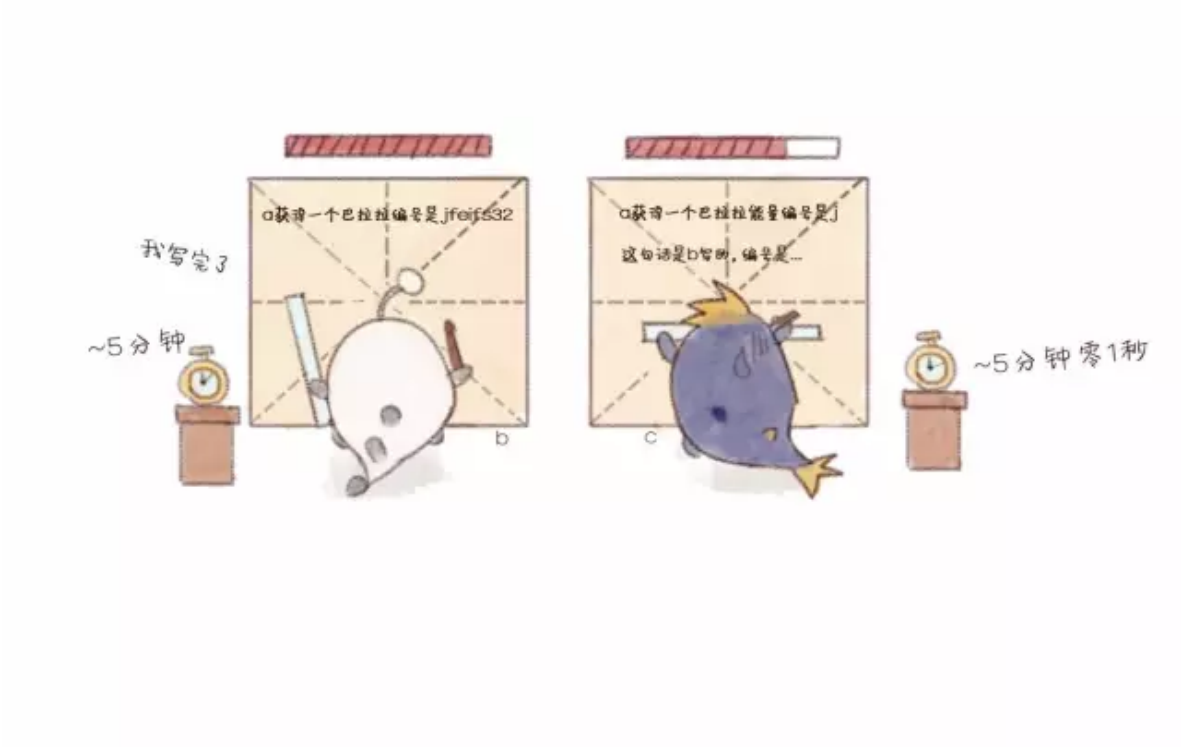
在不加任何限制条件的情况下，这件事件会发展成这样：一部分人认为这句话是B说的，在听到这句话之后开始记账，之后他们所做的所有事情都是基于B有了编号89757的巴拉拉

能量这个事实，并且随着这个信息一次次地传下去，这条信息链会越来越长；而另外一群认为C先说这句话的人，也会按照这样的趋势发展。

分叉问题听谁的?

这下事情严重了，原本是一条唯一的、编号顺序严谨的总信息链，在B和C喊出“这个编号89757的巴拉拉能量归我了”这句话之后，硬生生地分叉了！这还得了，要是这种情况延续下去，每个人手里的账本都变得不一样了，而且根本没法确定哪个是真的！

为了解决这个问题，小城市又追加了新的区块链规则，记录的时候必须顶格写，而且要保证，中心在离田字格上边缘0.89757毫米的位置上，于是，每个人写字的时候都要拿刻度尺量好之后再写，这非常困难，每个人的记录需要5分钟才能完成，因此，写这句话所用的时间变得不同了。于是，只要有人高喊“我写完了！那句话是某某某写的”，其他正在写这句话的人便会停笔，然后在小本子上重新开始写“那句话是某某某写的，上一句的编号是×××”。



每次记账的规则都很复杂

问题三：双花问题**

双花问题是指一笔数字现金在交易中被重复使用的现象。

如果我同时向B和C都喊了一句，我给你一个巴拉拉能量，怎么办呢？巴拉拉能量只有一个，如何保证一个巴拉拉能量在实际的交易中只被支付了一次呢？

我们以比特币为例，中本聪在《比特币白皮书》第五小节中是这样说的，运行比特币网络的步骤如下：

1.新的交易向全网进行广播；

2.每一个节点都将收到的交易信息纳入一个区块中；

3.每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；

4.当一个节点找到了一个工作量证明，它就向全网进行广播；

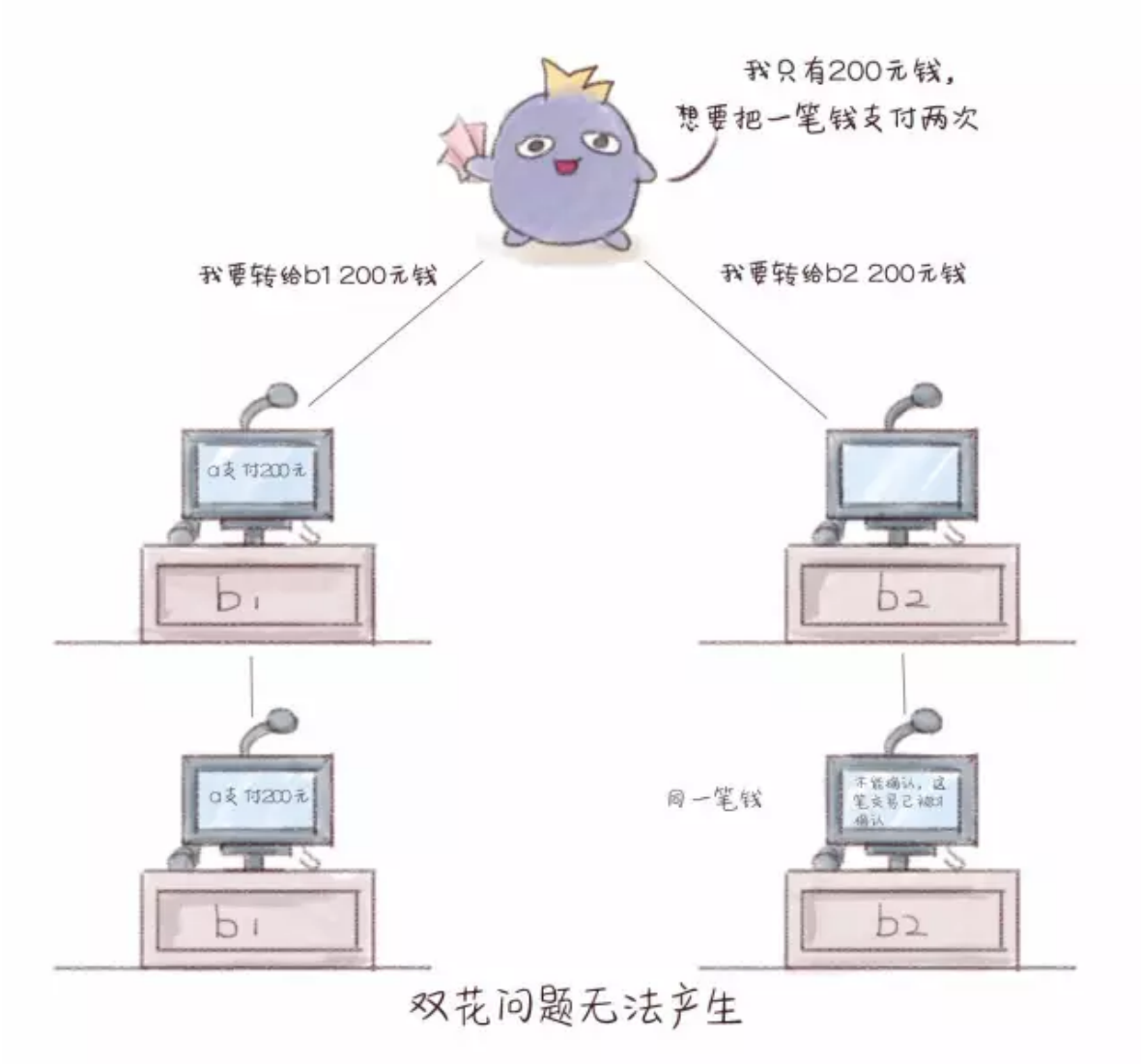
5.当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性；

6.其他节点表示他们接受该区块，而接受的方法则是跟随在该区块的末尾，制造新的区块以延长该链条，并将该区块的随机散列值视为新区块的随机散列值。

也就是说，交易发生的一刻起，比特币的交易数据就被盖上了时间戳；而当这笔交易数据被打包到一个区块中后，就算完成了一次确认；在连续进行6次确认之后，这笔交易就不可逆转了；在比特币中，每一次确认都需要“解决一个复杂的难题”，也就是说每一次确认都需要一定的时间。

6次确认后不可逆转

在这种情况下，当我试图于把一笔资金进行两次支付交易的时候，因为确认时间较长，后一笔交易想要与前一笔交易同时得到确认几乎是不可能的，而这笔资金在第一次交易确认有效后，第二次交易时就无法得到确认。区块链的全网记账需要在整个网络中达成共识，双花问题是无法产生的。


我只有200元钱，
想要把一笔钱支付两次
我要转给b1 200元钱
我要转给b2 200元钱
a支付200元
b1
b2
a支付200元
b1
同一笔钱
不能确认，这笔交易已被对确认
b2
双花问题无法产生

双花问题无法产生