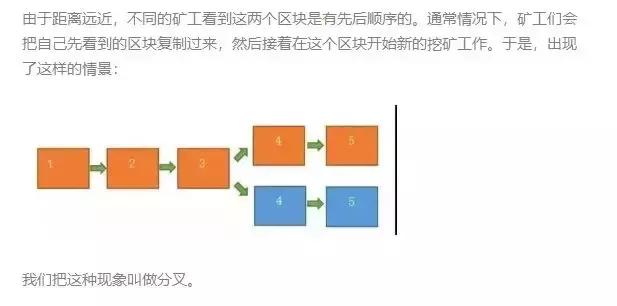
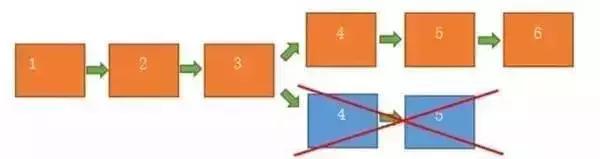
比特币采用的是工作量证明，就是让旷工相互竞争计算Hash，那么就会有一个问题：两个旷工同时算出了结果，这时要怎么办呢？

在任何区块里，第一条交易记录都是没有转出地址的，就是所谓的**CoinBase(挖矿交易)**。没有任何人付给矿工这笔钱，矿工只是理所应当的写上自己应当获得的比特币，比如12.5比特币，并且所有节点都认可矿工这样写，因此矿工就得到了挖矿收入。不同的矿工在填写区块的时候，数据一定是不一样的，因为每个矿工的第一条肯定不一样，矿工只会把挖矿收入转入自己的地址。

由于每个矿工的区块数据都不一样，所以他们解题得出的结果也是不一样的，都是正确答案，只是区块不同。于是，区块链在这个时刻，出现了两个都满足要求的不同区块。那么，全体矿工这时该怎么办呢?



在以工作量证明机制为共识算法的区块链系统中，这个问题是这样被解决的：从分叉的区块起，由于不同的矿工跟从了不同的区块，在分叉出来的两条不同链上，算力是有差别的。形象地说，就是跟从两个链矿工的数量是不同的。由于解题能力和矿工的数量成正比，因此两条链的增长速度也是不一样的，在一段时间之后，总有一条链的长度要超过另一条。当矿工发现全网有一条更长的链时，他就会抛弃他当前的链，把新的更长的链全部复制回来，在这条链的基础上继续挖矿。所有矿工都这样操作，这条链就成为了主链，分叉出来被抛弃掉的链就消失了。



这样，最终只有一条链会被保留下来，成为真正有效的账本，其他都是无效的，所以整个区块链仍然是唯一的。

注意，能够让区块链保证数据唯一性的前提是：所有矿工都遵从同样的机制。

还有一种情况，就是矿工不遵从同样的机制，那么也会出现分叉。这种分叉又有两种情况：

一、由于整个**区块链系统软件的升级，一部分矿工没有来得及升级，出现了遵从不同机制产生的分叉**。当这部分矿工升级系统后，这个分叉就会消失，我们称这种分叉为软分叉。

二、是**由于矿工之间出现分歧，一部分矿工决定采用不同的机制，产生出来的分叉是不会消失的**。我们一般把这种分叉称为硬分叉。

软分叉很好理解，我们重点谈谈硬分叉。

区块链圈里第一个有影响力的硬分叉应该是以太坊的分叉事件。以太坊上一个著名的项目The DAO由于其自身漏洞，导致黑客窃取了当时价值约6000万美元的以太币。2016年7月，以太坊开发团队通过修改以太坊软件的代码，在第1920000个区块强行把The DAO及其子DAO的所有资金全部转到一个特定的退款合约地址，从而“夺回”黑客所控制的DAO合约币。

由于一部分矿工并不认同这个修改，于是形成两条链，**一条为以太坊(ETH)，一条为以太坊经典(ETC)**，各自代表不同的社区共识以及价值观。当以太坊发生了这次硬分叉后，产生了两条区块链。由于这两条链在发生分叉之前的数据都是一样的，一个非常有意思的现象出现了：原本持有以太币(ETH)的人，发现自己除了持有原有的ETH外，又有了相同数量的ETC。也就是说，凭空的多出了一些资产。

这些资产的价值具体怎样，还要看市场交易情况。但总的来说，区块链的硬分叉，没有减少资产，反而让人手里多了一种资产，看上去总归是一件不亏的事情，于是**区块链分叉就成了一种资产凭空增加的方式**。

在2017年8月1日，由ViaBTC领导的矿工团体创建一个比特币分叉——Bitcoin Cash(简称BCC或BCH)。这次分叉，让大量的比特币持有者凭空的增加了一种新的数字货币(BCH)。

硬分叉这种创造货币的方式和ICO非常类似，于是一个新的名词诞生了——**IFO(Initial Fork Offerings)。矿工团队在创造分叉的同时，可以在分叉发生的区块中，利用自己的特权，分配一些货币给自己或其他人(直接写成CoinBase交易即可)，然后再开放让所有人都可以参与挖矿。**

随着越来越多的硬分叉发生，比特币的公信力是否还能像以前一样?IFO会不会成为比特币的杀手?还需要时间的考验。