

1.1 接触区块链的小故事

有个封闭的山村，叫玉石村，村民的主要工作就是挖玉石，村里的财富也是以玉石来计算。大家挖到的玉石堆放到一起，由村长清点记账。张三、李四、王五各自的财富，都记录在村长的账本上，他们可以依此去换取其他生活用品。

可是村长这个人有点不厚道，记账时，看到貌美农妇，多记两笔；遇到刺头，则少记一块。然后账本保管，也经常出问题，有的地方受潮模糊，还有的地方被老鼠啃掉。更过份的是，村长的儿子赵六还常常偷偷涂改账本。

于是村民决定将不干活、白吃饭、还老出错的村长废除掉。那谁来记账呢？



村民们想了一个办法：每个人都带一本账本，谁挖到玉石时，自己记录的同时用村口的大喇叭通知所有人，大家都在各自的本子写下同样的内容，每个村民都保管各自的账本。以后村民之间的物品换取、交换玉石，也通过这种方式记账。这样既节省了一个记账的劳力，还避免了账本受潮等问题。即使小寡妇涂改了张三的账本，但大家拿李四、王五、孙六的账本出来对比，就能马上发现问题并更正。

只要村民数量足够多，即使小寡妇性能再强大，也无法篡改过半人的账本。这就是去中心化的分布式记账。

李四提出了一个新的问题，**“我把已经记录的玉石，拿来再记一次，财富岂不就很快翻倍再翻倍了？”**

村民为了解决李四的弄虚作假，想了一个办法。给每块玉石都做标记，记录挖掘到的时间、地点和人物，以及上一块被挖到的玉石的信息。因此，每个村民的账本，都记录了每块玉的完整信息。每块玉都与上一块玉有信息关联，形成一个链条。李四既无法凭空捏造，也无法更改之前的记录。这就是区块链——P2P分布式记账。



上面的故事中，分布式记账，每挖到玉石，村民都需要停工，将账目更新一次，反而降低了生产效率。但在互联网的计算机中，这都是一瞬间可以完成的事情。区块链的**去中心化、防篡改、公开透明、共识**等思想都在故事中体现出来了。

1. 首先是区块链去中心化的思想，改革以后，玉石村的每一个村民手里都拥有一个账本。
2. 其次是防篡改的思想。在每个村民的账本里头给每块玉石都做标记，记录了玉石挖掘到的时间、地点和人物，以及上一块被挖到的玉石的信息。
3. 再次是交易信息公开透明的思想。在村民挖到玉石之后，在自己的账本记录的同时通知所有人，大家都在各自的本子写下同样的内容。
4. 最后是共识的思想。当某个村民发现有一笔玉石信息记录错误了，需要更正。这个时候需要至少51%的村民同意，才可以修改这笔记录。

Q：上面的故事是否有体现区块链的匿名性呢？