作者： 风说贴

最近，身边亲历两位朋友，因为买入打着区块链概念的虚拟货币而血本无归。

其中一位朋友家资颇丰，半年前投入80万买了三种虚拟币，至今在以比特币，以太坊为首的币圈一路暴跌的行情下，仅剩20多万。

另一位朋友收入较低，四个月前投入手中全部资金7万块买了国内一种新发行的虚拟币，哪知被套路，遭遇割韭菜，所买的币一路暴跌，最后跌到一个币仅仅只有几分钱。

因此，这几天专门撰写两篇文章。

第一篇主要通过分析区块链技术，让大家了解区块链到底是个什么东东？拨开它神秘的面纱，照出它的本来面目，只有认清了它的技术本质和实用范围，才不会上当受骗。

第二篇主要讲述当今社会上众多打着区块链旗号，发行虚拟货币割韭菜圈钱的骗术套路。

今天是第一篇，区块链技术浅析。

拨开云雾现天日，扯下面具现本尊

2018年就要过去了，如果说这一年在IT技术领域有些什么新鲜的名词，“区块链”绝对是可以排在前列的。

去年一路暴涨的比特币，不仅将“区块链”一词传遍了中国，伴随而来的还有很多既牛逼又装逼的其他名词“去中心化”、“账本”、“节点”、“智能合约”、“加密货币”、“代币”、“钱包”、“共识机制”...

就像说着中文不吐几句洋词就不会说话的某些文艺青年一样，在币圈或者链圈，谈论到区块链，如果不夹杂着几个让别人听到之后云里雾里的词汇，就不足以显示身上金光闪闪的逼格。

技术分析型的文章一般都比较枯燥，下面我尽量用简单通俗的语言来讲解，区块链到底是个什么东东。

假如有一个与外界隔绝的村子，村子里的村民都用铜板在交易物品。

今天，

张三买了李四一颗大白菜，

张三给了李四10个铜板；

明天，

李四买了王麻子一只鸡，

李四给了王麻子50个铜板；

后天，

刘小二买了朱大明一头牛，

刘小二给了朱大明500个铜板；

大后天，

朱大明买了张三一间屋，

朱大明给了张三10000个铜板；

……

这就是村子里的日常，这还只是简单的以货币交换物质，还没有涉及到借钱，欠账，放贷、与外村交易等等更复杂的金融行为。

村民们发现，这样十分不方便，至少有两点：

1.铜板携带太不方便，特别是交易额大的时候。

2.借了钱不认账不肯还，收了钱不承认不给东西的现象时有发生。

那怎么办呢？

正好，村长在村子里开了个钱庄，钱庄里有账房，账房里有专门的账房先生在账本上记账。

于是，大家出于对村长权威的信任，就都把手里的铜板都存到了村长的钱庄里面。

谁借了谁的钱，利息多少，什么时候还；

谁给了谁多少钱，买了什么东西，什么时候给；

谁手上有多少个铜板存在钱庄

谁今天从钱庄取走了多少个铜板

…

账房先生都在账本上一一记上。

这就是典型的中心化。

大家都相信一个权威(村长的钱庄)，并给予它足够的信任(村长、账房先生的人品没有问题、账房建的十分牢固等等)。

就如同大家把钱存在银行，银行的服务器则记录着我们的资产明细，交易明细…，而我们信任银行，是因为银行的背后有国家或金融企业的信用做支撑。

同理，其他各行业，例如我们使用微信，QQ，支付宝，那么在腾讯，阿里也必定存在着中心服务器来记录和维护我们的各种行为和信息数据。

但是，

即便这样也同样无法确保万无一失。

假如村长、账房先生的人品都是杠杠的，千年难出一个的完人(几乎没这种可能性)。

万一钱庄着火了呢？

账本被小偷偷了呢？

村长家的傻儿子赌博输了钱，偷了钥匙跑到钱庄偷钱呢？

账房先生的老婆羡慕别人新买的项链，到账房把账本上自己家的钱后面加了个0呢？...

这些都是完全有可能存在的，又该怎么避免呢？？

现在村长发话，不再设立钱庄，也不设账房了。

接下来如何确认每个人手中有多少铜板，每个人产生的每一笔交易是否真实有效呢？

村长把账本复印了很多份，给了他自己认识的朋友。

村长的朋友又有很多想参与到记账活动中的朋友，于是村长的朋友们又把账本复印给他们各自的朋友，而他们各自的朋友又有自己的朋友...，最后形成一张联系网叫“全网”，这些有账本的村民就叫作“节点”。

往后，村里任何一个人改动了自己的账本，都必须通过村里的大喇叭把账本的修改内容广播给其他有账本的村民，其他人收到广播，就在自己的账本上同样地记上一笔。

全网上有任何一个节点对自己的账本进行了账目修改，都会自动广播给全网所有节点进行账本更新。

全网上的广播就叫“全网广播”，

这种通信方式就叫“网络路由”，

需要更新的账本内容会通过算法打包成一个“区块”，

每个区块产生的时间，会和账本内容一起打包进区块，也就是“时间戳”。

每个新产生的区块与第一个区块相隔的区块数，就叫这个区块的“区块高度”。

这些由时间戳进行唯一标识，串行相连的区块形成的数据链就叫“区块链”。

区块链形成了，但是关于区块链上节点的数据更新，新的问题又来了。

每个村民记账都是独立的，有可能有的村民这段时间外出了，没有记账，还有可能，有的村民比较懒，他不想收到每一条广播都去记账，那么等他下一次连到全网，更新自己账本的时候，以谁的账本为标准把账目抄到自己账本上呢？

在区块链中，每隔一个时间段，都会通过一种大家都认定的算法机制选出一个节点，其他需要更新账本的节点就以这个被选出来的节点的账本数据为标准进行更新。

这个算法机制就叫作“共识算法”。

这个节点在这一时间段内要负责验证，整理、打包和广播账本上的数据，以便大家更新账本。

这是很耗时耗力的一个活，于是一般的区块链系统都会设计一种奖励机制，被选中的这个负责打包和广播数据的节点可以获得一些奖励。

有的区块链系统会将这一权利，设置成让节点去竞争，谁抢到了这个权利，谁就可以有对数据进行打包和广播的权利，同时并得到一定的奖励，争夺这项权利的过程就叫“挖矿”。

最终争取到这一权利的节点又叫做“矿工节点”。

区块链上数据更新同步的问题解决了，

下面就是关于区块链最重要的核心问题了。

有人在自己的账本上更新假数据怎么办？区块链又是怎么保证数据的正确性的呢？

在区块链中，如果有节点将需要更新的账目与账本上之前的账目进行验证，发现不对，可以拒绝修改，直到全网有超过至少50%的节点进行核算并确认新的修改真实可靠后，才会对账本进行更新。

下面仍然举例说明。

例如，李四手中一共有100铜板，他找王麻子买了一只鸡，同时在自己的账本上记上了一笔真实账目。

村里的大喇叭随即将这条记录广播给全村。

其他所有有账本的村民就都往自己的账本上记上一笔：李四现在有100个铜板，今天他买了王麻子一只鸡，花了50个铜板，现在还剩50个铜板。

第二天李四又去找刘小二买牛，但是一头牛要500个铜板，而他却只有50个铜板了，他想在自己的账本上作假，所以他记上一笔假的账目：

李四有1000个铜板，今天他买了刘小二一头牛，花了500个铜板，现在还剩500个铜板。

他的账本一改动，消息通过网络路由广播到全网，所有有账本的村民收到消息后与自己账本上的记录先进行核对。

“什么？上一条账目明明记录着，李四就剩50个铜板了，他怎么可能有1000个铜板，还花500个买一头牛？假的，交易不成立，不予记账。”

因此，在这种情况下，
李四想做假是不可能的，除非他能够逐一说服超过50%的拥有账本的村民去更新自己手中的账本。

这在人数特别少的情况下可以实现，可一旦拥有账本的村民基数足够大，这种可能性基本上等于0.

这也是区块链相较于中心化技术的优势所在，它确实能够解决中心化所不能解决的信任问题。

这也是为什么比特币在没有中心化机构维护的情况下，运行了将近10年而没有出错的原因，同时也是区块链技术引起人们关注的原因。

但是，世上是没

有一项完美的技术或理论可以解
决所有的事情的，
区块链技术确实解决了中心化的信任问题，它却同样有着无法避免的弊端：

1.数据更新太慢，假如使用区块链进行一笔实时交易，等到账本核算、广播、更新完成，有可能需要2个小时，半天...，远远超过用银行卡或者微信支付，在中心化的情况下，瞬间数据就能更新完成。

2.消耗能源太大，区块链技术由于其复杂并且巨大的数据计算和同步，同样的一笔交易，区块链需要消耗的能源远远大于中心化的数据计算和同步。

3.人们对中心化的数据管理方式并不反感，中心化虽然有这样，那样的问题，相比于没有任何信用机构背书的区块链系统，实际生活中，人们更愿意相信有国家信用支撑的银行，有实体企业信用支撑的微信支付，支付宝等机构。

这也是区块链被捧上神坛，却并没有迅速普及和应用的原因。

尽管因此，区块链作为一种比较独特的技术实现，它也不是没有它自己的实用场景。

比如，在食品，药品，安全器件生产、流通等领域，可以使用区块链技术对每一个生产环节的负责人，机构，生产时间等进行记录。

这些场景对
数据记录的实时性要求不高，数据量不大，数据访问，存储也不是很频繁，但是对记录的数据的不可篡改性要求很高，这就完全可以应用区块链来完成。

也就是说，区块链这项技术如果好好开发和利用，也是可以解决一些社会问题，发挥它的价值的，远不仅仅只是炒虚拟币。

这就是区块链，它并没有太多神秘之处，只不过是相对于中心化的另外一种数据管理方式，它也并不是现在才出现，早在20多年前就已经有了区块链完备的理论基础，只不过是由比特币将其进行了落地和推广。

然而，
在比特币将区块链这一技术理论带到人们眼前之后，它一同带来的金钱游戏，让一批又一批的野心家们利用区块链的概念，使尽各种手段骗取钱财。

他们的骗术套路又是怎样的呢？

我们下一篇再讲。