比特币火了不止一年两年了，缔造了很多神话，但是真正懂比特币的人不多，很多人奇怪比特币有什么价值？凭什么可以达到上十万一个？本文从白皮书入手，告诉你答案。

比特币就是一个电子交易系统，就跟我们用手机银行转账一样，不同的是，比特币转账没有银行介入，只有交易双方。

那么，没有银行，如何保证整个交易系统的安全性呢？其实思路并不难，只要这个系统具有Y行系统的功能就可以了，你可以想想在我们平时Y行转账过程中Y行做了哪些事情？

比如我要转100块给小明，Y行是怎么完成的？

1、我和小明需要各有一张银行卡，然后我告诉Y行，要从我的卡里转100块给小明；

2、Y行验证我卡中是否有100元，如果有就从我卡中扣除100元，记账-100，在小明卡中增加100元，记账+100；

3、保存好我和小明的账本记录，并且保证没有人能更改这些记录。

那么，在这里面可以分解成几个问题，把这几个问题解决了，就可以保证系统安全性。

1、保证交易双方都有转账地址并且足够安全

2、发送币的一方发送一个币出去，自身就必须减少一个币（双花问题）

3、保证交易记录的正确性及不可随意篡改

4、保证有人愿意记录交易

第一个问题：如何保证交易双方都有转账地址并且足够安全？

解决办法：通过编程让系统利用密码学的非对称加密算法随机生成一对公钥和私钥，把公钥作为转账地址，私钥作为转账地址的密码，打个比方，把10通过加减法拆成7+3，其中7作为地址，3作为密码，只不过比特币的地址很长，包括字符和数字等；

第二个问题，如何解决双花问题（就是一个人的100块，同时发给另外2个人，这样100块就可以当200块用）？

解决办法：通过引入数字签名和时间戳服务器，把交易按时间排序成一条链来解决；打个比方，张三给小明交易100块，那就写一笔记录：转小明100元，然后签上张三的名字和签字的时间，如果张三要转大明100块，那就写另一笔记录：转大明100元，然后签上张三的名字和签字的时间，这两笔记录按时间先后连接起来，要么签名不一样，要么时间不一样，所以同一个人在同一时间就只有一笔转账记录，当然比特币系统中不可能签名字，它签的是上一个交易和本次交易公钥的哈希运算的结果，接收方通过哈希算法就可以验证签名的正确性。

第三个问题：如何保证交易记录的正确性及不可随意篡改？

解决办法：这个问题最难而且也是最核心的，我们把交易记录分为已经生成的交易记录和以后将要生成的交易记录，这里比特币系统引入了分布式节点和每个节点提交工作量证明的方法；

分布式节点，就是将交易记录分散到网络中的每个节点上，这样，已经生成的过去的记录你就很难更改，因为你需要同一时刻更改所有分散节点的记录，这在初期节点较少的情况下容易发生，在节点越多，发生概率越低，到现在全球上万节点的情况下基本不可能发生。

那么怎么保证即将生成的交易记录是正确且不可篡改呢？通过工作量证明来实现，简单来说，就是每记录若干笔交易（比如最近十分钟之内的交易）之前，需要进行一次随机的运算，类似一个高幂次的方程，这个方程没有运算解，只能用一个个的随机数代入运算，如果计算的方程式成立，则为正确答案，第一个得出正确答案的人所记录的交易为正确交易。这样，谁的计算能力越大，谁第一个算出来的概率就越大，如果有违法的节点想要篡改交易记录，那么从它开始作乱的那个时间开始，就在与其他所有不作乱的节点进行算力比拼，如果它的算力比其他节点大，那么它篡改记录的概率很大，如果它的算力比其他节点小，那么它篡改记录的概率很小，在白皮书里有一个计算公式，由于攻击者实施攻击是需要一个过程，因为它的算力不可能是一秒钟起来就超过其他节点，因此实际上攻击者的节点是落后正常诚实的节点的，那么它实际上是需要追赶正常节点，落后越多，篡改几率成指数级下降，概率有多低呢？白皮书里进行了分析：

大家好，这里是阿木说币，带你深入了解币圈、链圈、矿圈的那些事，欢迎关注！