## 通俗解释

**区块链**

去中心化的理念（类比电子商务），借助互联网信息技术实现。

解决的核心问题是：信任问题。

## 比特币

比特币是区块链去中心话理念的具体应用（类比淘宝网）。

2条核心规则：

1. 货币发行规则：一个方程式，有2100万条解， 每个人都很公平， 去解一个解，会有比特币回报。
2. 交易信息不记录在某一台机器上，记录在所有参与的节点上，理论上账本完全无法被篡改。

比特币并不是完全成功区块应用，有天生缺陷：

1. 客户端需要巨大的空间，保存交易记录。
2. 每笔交易的确认时间很长最少要10分钟， 等6个块以上就要1-2小时。
3. 总数有上线（2100w），人们不断增长的需求与币的总数不充分之间的矛盾。

区块链技术越成熟，比特币系统越被抛弃的快！

## 区块链是什么？

去中心化的分布式账本数据库。区块链就像是账本，构成区块链的每一块就是账本的每一页。交易细节被记录在一个网络里任何人都可以看到的空开账本上。最明显的应用是比特币。

去中心化？

所有的东西都通过预定的程序自动运行，每个人都有相同的账本，公开透明。

数据不可篡改？

区块链通过密码学的方式保证数据不被篡改。

非对称加密？（哈希加密）

一把公钥 一把私钥 ， 公钥加密的内容只能用私钥解密， 用私钥加密的内容只能用公钥解密。 公钥可以通 过私钥生成多把。

奖励机制

由于没有中心化机构，就没人发工资。没有奖励也就没有人会愿意记账了。

比特币系统中，每一个节点打包区块的时候都会给自己增加一定数量的比特币（具体数量根据实践在逐步递 减,nonce随机数控制计算难度），每记录一笔交易都会从中收取一定数额的比特币作为手续费 。

## 区块链是怎么产生的呢？

区块是记账的存储区域，可以类比为账本。算法设定每10分钟(10分钟可以调节)生成一个区块，区块之间相互连接，后一个区块会记录前一个区块的哈希值(即特定的加密生 成一串字符串)。从而连接在一起，称为区块链。

通俗点来讲，就是每个区块就是一个账本，每个账本都有一个编号，每10分钟会新生成一个新的账本，第二个账本会记录下来第一个账本的编号，从而连在一起。

**钱包(wallet)**

如果一个信息被公钥加密，只有配对的私钥才能解密读到信息。反之，如果你用你的私钥加密信息，只有配对的公钥可以解密。

所以当David想要转帐，他需要用他的私钥将转帐信息加密后，送到网络里，然后每个节点使用David的公钥将信息解开，以确认是由David发送的。

在加密完成时会产生一个电子签名（一般只对摘要进行签名），它会被节点们用来确认交易信息的发送来源和真伪。

在时间序列上，同个区块内的交易信息被认为是“同时发生”，还未被打包进区块的交易信息会被视为“未确认状态”。每个节点都可以将若干个交易信息打包成区块发送到网络上，并建议其为链上的最新候选区块。

因为任何节点都可以发送候选区块，系统如何决定谁才是可以放在链上的最新区块？

区块链系统使用加密哈希函数设计了一道复杂的数学题，候选区块只要有正确答案，就可以成为链上的最新区块。

数字钱包并不是用来保存数字资产的，而是用来保存“密钥和地址”的。

区块链里面没有账户余额的概念，你真正拥有的数字资产实际上是一段交易信息；通过简单的加减法运算获知你数字钱包里的余额。

冷钱包 （离线钱包，链上记录的是地址之间的交易，这个地址可以通过冷钱包生成，私钥生成）你可以在一台永远不上线的电脑上装一个比特币钱包软件，然后生成地址。这时候你的私钥是完全没有接触过互联网的。这个地址也可以用来接收比特币，而且你也可以在这台电脑上用私钥签名构造“交易”（此处比较牛逼），然后到另外连网的电脑钱包上去广播来发送比特币到别的地址。是最安全的存储比特币的方式。

真正必须存在比特币网络里的东西是“交易”，比如你的地址收到一笔比特币，这次“交易”是会被比特币网络记录的，这是不能离开网络的。但私钥和地址都可以和网络无关。

比特币其实就是一套特殊的复式记账本，你所买到的比特币本质上就是在这套复式记账本上买到了一笔可以登记在你的比特币地址上的“输入”。而你向他人支付比特币本质上就是你在你的比特币地址上将已经有的“输入”给其他人的地址登记一笔“输出”。

**对称加密 和 非对称加密**

1. 对称加密

对称加密指的就是加密和解密使用同一个秘钥，所以叫做对称加密。对称加密只有一个秘钥，作为私钥。

2. 非对称加密

非对称加密指的是：加密和解密使用不同的秘钥，一把作为公开的公钥，另一把作为私钥。私钥加密的信息，只有公钥才能解密。公钥加密的信息，只有私钥才能解密。

密钥：是成对出现的，由一个私钥和一个公钥组成。

私钥：就好像银行卡的密码，有了私钥就可以动用对应地址下的数字资产。

公钥：由私钥生成的，但是无法通过公钥倒推得到私钥。公钥的作用是跟签名配合用来证明我就是私钥的主人。

地址：就好像银行卡，收币的时候需要将地址（银行卡）给别人，让别人将数字资产转到自己的地址（银行卡）里。

数字签名：只能由私钥生成，和公钥配合就可以证明“私钥在我这！”

小A -> 小B （仅解释非对称加密，并非区块链工作方法）

第一步：小A会先用SHA256函数对自己的小纸条进行处理，得到一个固定长度的字符串，这个字符串就等价于这张小纸条。

第二步：小A使用只有自己知道的那一把私钥，对上面固定长度的字符串进行再加密，生成一份名叫数字签名的字符串，这份数字签名能够充分证明是基于这张小纸条的。

第三步：小A将「明文的小纸条」、刚刚加密成功的「数字签名」，以及自己那把可以公布于众的「公钥」打包一起发给小B。

第四步：当小B收这三样东西，首先会将明文的小纸条进行SHA256()处理，得到一个字符串，我们将其命名为“字符串2”。然后，小B使用小A公布的公钥，对发过来的数字签 名进行解密，得到另外一个“字符串1”。通过比对“字符串1”和“字符串2”的一致性，便可充分证明：小B接受到的小纸条就是小A发出来的小纸条，这张小纸条在中途没有被其他人所篡改；且这张小纸条确实是由小A所编辑。

非对称加密、数字签名

1.鲍勃有两把钥匙，一把是公钥，另一把是私钥。

2.鲍勃把公钥送给他的朋友们----帕蒂、道格、苏珊----每人一把。

3.苏珊要给鲍勃写一封保密的信。她写完后用鲍勃的公钥加密，就可以达到保密的效果。

4.鲍勃收信后，用私钥解密，就看到了信件内容。这里要强调的是，只要鲍勃的私钥不泄露，这封信就是安全的，即使落在别人手里，也无法解密。

5.鲍勃给苏珊回信，决定采用"数字签名"。他写完后先用Hash函数，生成信件的摘要（digest）。

6.然后，鲍勃使用私钥，对这个摘要加密，生成"数字签名"（signature）。

7.鲍勃将这个签名，附在信件下面，一起发给苏珊。

8.苏珊收信后，取下数字签名，用鲍勃的公钥解密，得到信件的摘要。由此证明，这封信确实是鲍勃发出的。

9.苏珊再对信件本身使用Hash函数，将得到的结果，与上一步得到的摘要进行对比。如果两者一致，就证明这封信未被修改过。

区块链加密算法

公钥加密，私钥解密，私钥签名，公钥解密。



**如何证明数字资产是你的？**

“地址+签名+密钥”

数字资产是没有人的概念的，只有地址的概念。一个人可以拥有多个地址，就好像一个人可以开多张银行卡一样。

区块链世界中，你不需要身份证这种东西来证明身份，只要拥有了“地址+签名+密钥”就能随意使用该地址下的数字资产。

由于私钥能生成公钥，公钥能生成地址，签名也是私钥生成的

所以只要拥有了私钥就相当于拥有了数字资产的所有权。这也是大家常说的：拿走你的私钥就可以拿走你的数字资产。

私钥->公钥->地址

私钥->签名

**共识机制**

分布式账本需要解决的一个核心问题，数据一致性。

节点都会认为最长链为唯一正确的链，并希望自己是基于最长链进行的打包区块工作。

怎么保证区块生成的频率为每十分钟一个，并且由谁来生成区块？

1. 工作量证明（POW） 比特币为例：（所以打包和认可还是2回事情）

区块链打包生成哈希值的时候规定升成的哈希值必须由多个0开头。那么打包过程中就需要引入一个被称为（nonce）的随机值，区块链中想要参与打包区块工作的节点就得不停更换nonce的数值重新打包，直到生成了规定的哈希值为止（就是猜）。那么第一个打包成功的区块就会被其他节点认可。而这个找到随机值的难度会根据整个比特币网络的计算能力调整，确保在十分钟左右，整个网络将会有节点找到这个随机值并打包成新的区块广播到网络中。（打包完了会获得比特币的奖励） 这个机制还算挺公平的，只要你自己努力，肯计算，就会获得相应的打包权利。

虽然本机制被实践证明是现在区块链世界中最可靠的共识机制，但是缺点显而易见，浪费了大量无谓的计算。现在很多人诟病比特币浪费电也是基于这个原因。中本聪规定，每笔交易的发起人，不但要将交易单给到收款人，还要同时复制若干份一模一样的交易单投递到每个矿工小组的收件箱里。矿工小组的人定期到自己的收件箱里把收集到的交易单一并取出来。打包成功（加上幸运数字后生成的哈希值前几位是000），就会有奖励。随着交易和矿工的活动 ，比特币的数量会不断增多。

确认账簿

当某挖矿小组幸运的生成了一张有意义的账簿，为了得到奖励，必须立刻请其它小组确认自己的工作。前面说过，当前村里有7个挖矿组，所以这个小组必须将有效 账簿纸誊抄6份快马加鞭送到其他6个小组请求确认。中本聪规定，当某个小组接到其他小组送来的账簿纸时，必须立即停下手里的挖矿工作进行账簿确认。

需要确认的信息有三个：

1.账簿的编号有效。这个确认比较简单。只要将送来的账簿纸放入编码生成器进行验证，如果验证通过，则编号有效。）

2.账簿的前一页账簿有效。第二部分需要将账簿页上的“上一页账簿纸编号”和这个小组目前保存的有效账簿最后一页编号比对，如果相同则确认，如果不同，需要顺着已有账簿向前比对，直到找到这个编号的页。如果没有找到指定的“上一页账簿纸编号”对应的页，这个小组会将此页丢掉。不予确认。

3.交易清单有效 （一直往前追溯）

如果完成了所有了上述验证并全部通过，这个小组就认可了上述账簿纸有效，然后将这张账簿纸并入小组的主账簿，舍弃目前正在进行的工作，后面的挖矿工作会基于这本更新后的主账本进行。

比特币会一直增加下去，岂不是会严重通货膨胀？

给矿工组织的操作细则手册会说明，刚开始我们协议每生成一页账簿，奖励小组50个比特币，后面，每当账簿增加21,000页，奖励就减半，依次类推，等账簿达到 6,930,000页后，新生成账簿页就没有奖励了。此时比特币全量约为21,00万个，这就是比特币的总量，所以不会无限增加下去。

没有奖励后，就没人做矿工了，岂不是没人帮忙确认交易了到时，矿工的收益会由挖矿所得变为收取手续费。例如，你在转账时可以指定其中1%作为手续费支付给生成账簿页的小组，各个小组会挑选手续费高的交易单优先确认。

较短分支上的区块会立即丢弃，而里面的小纸条也会随之释放出来，被重新标记上“未确认”。

矿工如果越来越多，比特币生成速度会变快吗？

不会。中本聪解释，虽然可以任意加入和退出矿工组织，导致矿工人数变化，每个矿工也会拿到一个编码生成器，不过我已经在编码生成器中加入了调控机制，当前工作的编码生成器越多，每个机器的效率就越低，保证新账簿页生成速率不变。

“双花”与“51%攻击”

拜占庭将军问题（这就是比特币网络最长链选择）

假设攻下一个城堡需要多次的进攻，每次进攻的提议必须基于之前最多次数的胜利进攻下提出的（只有这样敌方已有损失最大，我方进攻胜利的可能性就更大），这样约定之后，将军A在收到进攻提议时，就会检查一下这个提议是不是基于最多的胜利提出的，如果不是（基于最多的胜利）将军A就不会同意这样的提议，如果是的，将军A 就会把这次提议记下来。

2) 股权权益证明（POS）(注意 比特币 ！= 比特币权益)

看名字就很容易该机制的运行原理，谁拥有的股权更多，谁就有更多的机会打包区块。假设比特币不使用POW而使用POS机制了，那么有打包权利的节点不再是所有愿意努力计算的节点了，而是账户上拥有比特币的节点。我们设计一个算法，账户上的每一个比特币一天产生1点比特币权益。假如我拥有10个比特币100天，那么我的账户上就拥有了1000个比特币权益。每次打包都会将我的比特币权益清零，而每次清零365个比特币权益 将会收获一定的利息。而区块链在选择打包节点的概率与每个节点拥有的权益正相关。

3) DPoS （Delegated Proof of Stake）：授权股权证明机制