火币网 COO 朱嘉伟

【1】比特币的由来。
为什么成本只有几里钱的货币能买到价值上百的商品。想要理解这个问题，就得了解我们人类从实物货币到记账货币的转变。另外还要理解现在互联网信息传递和价值传递的本质，这样才能为理解比特币做准备。

之所以成本很低的纸币可以买到成百的商品，主要是因为这是国家信用在背后做背书，所以才让一文不值的纸币具有了价值。

现在，出门甚至不用带钱，直接刷二维码，这又怎么理解？整个过程不会见到纸币，这是我们在使用记账货币。比如发工资，是在对应的银行卡上做加法，买衣服，是做减法。这是谁来负责的？各家银行，以及各种第三方支付机构。

对我国来讲，央行有绝对的大账本记账权，这是一种中心化的记账模式。

中本聪发现，美国在 08 年经济危机年，由于美国最大银行有中心记账权，所以为了应对危机印发了大量货币，最终导致了超发。所以他想，有没有这样一种货币，没有中心记账这么一说，我们每个人都有记账权利，但是这个货币又不能超发，并且整个账本公开透明…这就是比特币产生的源泉。

问题#
记账货币必须有一个记账方。记账方（或叫记账中心）一般是银行（或者是第三方机构），这种传统的记账方式，是一种中心化的记账方式，账户是由记账方（大银行）的信用来担保的，如果有人黑了银行数据库，那银行的账户就危险了…
而且如果银行失信，那就很危险了。

而如果多个中心，且人人都可以记账，就安全多了。这就是比特币的发行，记账。比特币依赖的底层技术– 区块链。（去中心化）

在现在的网络世界里，世界任何两个地方，只要有互联网连接，两个人就可实现点对点的信息传递。其实互联网下信息传递的本质是复制（如用微信发给盆友一个照片，发送了副本过去，我本地还有一个图片）。

但是，互联网状态下，价值传递如：版权、货币等价值传递的时候也用这种方式的话可能会有问题，因为不可能我给别人转了 100 块之后，我账户上还有这 100 块。

价值的传递要求信息和价值信息同时传递。。

区块链就做到了这点：即在没有记账中心存在的情况下，可以实现全球化的信息和价值传递。并且每一笔账都可以追溯到源头，每一笔账都有据可查。（其实，现如今银行账户信息的更新，并不是同时实现了信息和价值一起传递，而是账户信息先更新，然后银行会在一天的固定时间对账结算，价值的结算严重滞后于信息的传递更新。）

对比特币人们看法不一：
第一，有人认为比特币是一种无主权的货币，超越了国家信用的货币。这种说法现在越来越少了。

第二，有人认为比特币是一种全球的现金，来解决跨中心的支付问题。

第三，有人认为比特币由于储量恒定，开采难度逐渐变大，稀缺，易分割等特点，能快速传递，将来有可能会成为未来全球化的数字资产，起到了价值存储的功能，类似于黄金。

第三种观点，就现在来看是主流观点。

就现在来看，比特币作为区块链最成功的应用，它市值占有高达几百亿美金，很多国家都开始纷纷为此立法。美国，日本，菲律宾等等。

问题：
到了 2140 年，比特币发行完毕了，那个时候人们有什么动力竞争记账？

【2】比特币的转账机制以及（区块链的）专有名词。

第一，如果我有比特币，怎么转给别人。
以现有的通过银行 app 转账到别人账户为例，比特币的转账方式其实和这差不多。
不同的是登录上比特币钱包之后，转账之前，我需要填写比特币地址：一串 30 个数字字母串，表示比特币地址（类似于需要从哪张卡转钱给对方）
另外，还要签上比特币签名，最好还要填写手续费，提交给比特币网络，然后等矿工打包处理。

和传统转账不同的是，我可以自己选择手续费，当然我也可以选择不交手续费，但是如果我不交，可能会比较晚的被矿工记账确认。

第二，以比特币为例，学习区块链，必须知道的七个专有名词。
矿工和 挖矿（获得记账权的过程行为）
我们在上面提交了一个转账比特币的申请，等待矿工确认，为什么会是这样的流程？怎么还要等矿工确认呢？

比特币世界中，因为竞争记账会获得新生的比特币奖励，这种竞相记账的人的行为很像挖矿一样，我们把这些为了获得挖矿权利的人叫做矿工。

算力：每秒能做多少次哈希碰撞，即算力。

工作量证明：结果可以证明付出了多少工作量
POW

权益证明：根据持有的币多少决定了记账权利
POS

区块：每十分钟比特币市场就会产生新的一页账本，这就叫做区块。

区块链：每一页账本打上时间戳严格按照先后顺序串起来，叫做区块链。
区块的身份信息，哈希值，大小是多少。
这段时间内，网络上产生的比特币账本交易信息。

【3】比特币转账运行的原理
中本聪在 2008 年提出建立一个没有中心化记账机构的去中心化的货币发行体系，币就不会被无限超发，记账公开，大家都很公平公正。

『中本聪在比特币发行之初规定』

比特币的发行
1 ）总共是 2100w 枚比特币。
2 ）每十分钟，会产生新的一页账单（即区块），每个比特币的产生，伴随着每个账单的产生。
3 ）每个区块比特币发行量是 50 枚，然后每 21w 个区块减半一次，直到 2140 年，所有的比特币发行完毕。

比特币的流通

比特币的记账
中本聪把竞争记账和比特币货币的发行绑定在了一起。记账的人每当首先记账一次，那么他会获得系统新发行的比特币权利（还包括这一页账单上所有的手续费大概 0.2 到 2 个比特币）。这种独特的记账方式导致矿工竞相记账。

【4】比特币的由来（技术由来）
比特币具有去中心化，不可篡改、不可伪造的特点，这是为啥。这一节讲清楚。

1 ）去中心化依靠啥实现？
中心化（记账机构）的存在，是确认每笔交易的，去中心化，即不需要中心记账机构来确认交易。

因为这个账本文档中的每一个节点都可以验证这笔交易的真伪，所以不需要中心记账机构来验证。
那这是靠什么验证的？是非对称加密技术。
公钥和私钥成对存在，可以互相验证。
以一次转账为例：
我的比特币转出地址可以看作是我的公钥，签名信息可以看作是我的私钥。对方的比特币地址是对方的公钥，他的签名信息是他的私钥。
（每个等待挖矿的矿工拿到这笔交易信息，首先会验证这笔交易是不是匹配的，匹配的，即合法）
这样在我转账的时候，只需要知道我自己的比特币地址（我的公钥）我的转账密码（私钥）和对方的比特币地址（对方公钥）即可。

当然，比特币的分布式存储也保证了比特币去中心化的特点。

2 ）为什么说比特币账本是无法篡改的。
这是靠比特币的工作量证明机制和最长连接机制保证的。
首先说工作量证明机制，如果对工作量进行验证，通常效率比较低，而通过工作量证明机制的话，就很快可以验证真伪。（比如）

如果想篡改区块链记录的信息，需要篡改

【5】

【6】

【7】