区块链具有分布式记账和不可篡改的特点，这也让区块链技术天然就契合供应链金融各类场景中要挖掘和传递信任的首要风控需求。

区块链有哪些关键技术？又是如何帮助供应链金融链条中的价值做可信传递的呢？

第一个关键技术：P2P动态组网技术。

为什么迅雷下载那么快而浏览器下载这么慢？因为浏览器属于单线程下载，它只会从一个服务器的网点读取数据。而迅雷用的是多线程下载，它会从周边最近或网速最快的节点里把数据读取过来，所以速度会很快。

主网技术意味着大家都是平等的，就像看电视剧一样。比如我看了琅琊榜的第一集，别人看的时候会从我这里把数据读过去。等我看到第二集的时候别人可能已经看了，所以我可以从别人那里把数据读取过来。所以这个网络是平等对等的，没有一个中心化的人来做连接。

这个就是网络主网技术P2P的点对点传播技术，这个技术其实一直都有。

第二个关键技术：账本结构—加密解密技术

账本结构是区块链特别重要的一点，在交易的过程中，你把交易写到了块（block）里面，然后每次记下来的时候一定要告知上一句话说到哪里，因为要有指向。

它是链式结构的，好比我们冬天穿的羽绒服都有拉链，如果拉链底下那一块没拉上

去，顶上的所有的链都拉不上去，但是一旦把最底下的拉上去了，所有链条都能追溯。

区块链就跟衣服的拉链一样，每个数据独立存储完之后就会形成一个链条。在这个过程中还需要去做签名，这是密码学决定的。签完名的信息只有私钥能解出来。

接下来给大家做的一个演示：

假设在机器上写了一行中文：区块链是价值传递机器，然后拿着利用私钥做了加密。 加密后的秘闻其实就是左图下方那段乱码。没有私钥就根本无法知道里面的内容是什么。

在没修改密文的情况下，点解密就能解出来。但是把那段绿色的码删掉之后再点解密，它就会提示数据结尾异常。这其实就是加密解密的方式。

再举个更直观的例子，比如银行账户在2017年12月8号收到2000万，最后加密存储完之后就变成乱码，想改也改不掉。

第三个关键技术：共识算法。

共识说简单点就是投票。只是有的人是通过工作量来证明，例如根据挖矿的难易程度来决定报酬的多少。在节点里有十个人或五个人，其中有人的服务器可能坏了，或者它觉得验证的数据不对，因为可能被人恶意修改了。

但是只要网络上有51%的人验证通过，就可以认为它是有效的记账。当然这个比例是可以调整的，如果应用在供应链金融里面可以调整为百分之百，当节点数足够多的时候就可以慢慢地把节点的比例降下来。

所以共识算法可以理解为投票，跟人大选举一样，选定某个人作为代表。

第四个核心技术：智能合约。

智能合约就类似你用手机定了一个早上7点的闹钟，到了早上七点钟闹钟一定会响，这其实就是你跟手机有了一个智能的约定。

为什么一定要叫智能合约？原来传统的合约都写在合同里面没办法执行，做到了计算机里面后，这个合约就变成了大家都能够看到的，你不执行我可以帮你执行。智能合约的执行也是通过参与节点之间的选举决定到底由谁来执行。

举个例子，购买航班延误险后，航班延误大于两小时就可以获得200块钱赔付。这个延误险原来都是由保险公司执行的，但是延误两小时的数据到底如何计算？时间指的是开舱门时间、关舱门时间还是到达时间？数据源从“航旅纵横”上来还是从“非常准”来？如果保险公司没有钱赔付怎么办？其实这些都可以在智能合约里通过一系列的判断条件确定下来。

这些就是区块链的分布式账本过程之中所需要的核心技术。