给区块链一个定义

2020-08-09

一直以来，区块链似乎都没有一个明确的定义，伴随区块链出现的词语经常是去中心化、溯源、不可篡改、以信用为基础、下一代价值互联网之类，这些都是区块链的特性，不是区块链的组成，这些词都在说区块链有什么，没有说区块链为什么会有那些，以及为什么要有那些。

感觉上很多东西都没有明确的定义，比如，计算机是什么？都知道是那么一个东西，可以打游戏上网，稍微专业点的会说是基于冯诺依曼体系结构的、有 5 个组成部分的什么什么机器。其实计算机可以认为是“做计算的机器”，就这么简单。冰箱是什么？“一个放东西的柜子，有一些冷冻的功能”，就可以了。设计模式是什么？一种软件程序设计的范式。微服务是什么？一种软件架构的模式。所以区块链是什么？奇怪的是，区块链（blockchain）这个词不知从何而起，从来没有人明确提出这个概念，比特币白皮书里也只是提到 “chain of block”。

我以前对区块链有过一些不成熟的认识，虽然好像也没什么错，但不够清晰，尤其是没搞清楚一个问题，区块链是什么？现在来看，区块链的定义应该是：

> 区块链是一种数据协同软件，或者说，区块链是一种用来同步数据的软件。

数据协同软件决定用什么样的数据结构通过什么样的通信机制同步哪些数据。区块链不是数据库，区块链不负责储存数据，储存数据的事情会交给真正的数据库来做，区块链并不关心数据是怎么存在磁盘上的，不关心储存结构是否合理，利用率高不高，处理速度快不快。区块链关心数据以什么样的方式同步到其他的机器上，如何及时同步，以及其他机器同步过来的数据有没有问题。可以说，区块链是对数据协同软件的一种实现。

因为是数据协同软件，所以区块链多节点、去中心化，这显而易见。

溯源是指交易可溯源，只要数据之间有关联关系就可以，这是数据模型决定的，比如 UTXO。

链式的数据结构，是为了方便数据协同软件校验数据的完整性，类似用 md5 判断文件是否完整。这种数据结构并不是必要的，数据的全量对比也可以实现目的，只是效率非常低下。所以采用加密算法做摘要然后放到下一部分数据里的做法，相当于保证了一大块数据是完整的，仅此而已。

至于不可篡改，其实是数据协同软件带来的特性。区块链的不可篡改，并不是数据不能修改，而是改了之后其他节点不认可。这是不一样的，数据不能更改是技术问题，比如不提供更新数据的接口，用户就没有修改数据的渠道，通过技术手段可以控制。改了之后其他节点不接受，是一种机制，这种机制问题已经脱离技术领域。

区块链目前的发展受技术限制吗？计算机的计算理论包含两个主要部分，可计算性理论和复杂度理论。可计算性理论判断一个问题能不能用算法解决，复杂度理论意在提高算法的效率。和区块链有关系吗？退一步说，区块链需要计算吗？不需要，没有关系，不受限制。有个有趣的脑洞问题，如果把全世界的人都拉到一个微信群里，会发生什么？起码屏幕上的消息肯定刷不过来了。如果全世界的数据共用一条区块链，会发生什么？所以区块链最终还是机制的问题，不是技术问题。

比特币和区块链是两个概念，比特币是一种使用了区块链做数据同步的交易系统，比特币首先是一个交易系统，其次才需要的数据同步。这也是我以前犯的概念上的错误，把区块链等同于比特币了。很多对区块链概念比较模糊的人，提到区块链也都会往比特币之类的数字货币上想。记得去年参加过一个分享会，主讲人是某知名交易所总监，分享标题是区块链和国家政策什么的，整个会议下来，讲的却全是比特币的趣闻轶事。

区块链是比特币的组成部分。比特币的作者看到了比特币的价值，把软件和白皮书发布出来了。为什么比特币的作者没有把区块链的概念抽离出来，发个通用软件和说明书？是水平不够没有意识到区块链潜在的巨大价值吗？不是。区块链的提出，是因为人们看到了比特币的价值，想要复制比特币的成功，所以把比特币的技术组成提取出来，叫做区块链。可惜比特币是一个设计巧妙

的系统，单独把某些技术特点拿出来难以产生预期的价值，这也是区块链的现状。这是现代版技术圈的东施效颦。

智能合约（Smart Contract）早在 1997 年由一位金融、法律从业者提出，“智能”是指和纸质合同相比，智能合约达到某一条件时就会自动执行某些操作，确实比纸质合同智能了一点，尤其在那个年代，数字化还没有普及，描述这是一种智能并不为过。而且，作者明确说，智能合约没有用到人工智能。

智能合约抽象一下，达到某一条件自动执行一些动作，不就类似编程语言的条件语句吗，事实上现在的智能合约大多是用图灵完备的编程语言实现的。用编程语言来描述合约的致命问题在于，编程语言的表达能力比自然语言弱太多了，如果试图用编程语言来重写保险说明书里的所有条文，“发生什么，就赔偿多少……”，这种改写的成本太高了，而且很多时候法律条文需要专业律师、法官解释和判断，现实世界的逻辑远比程序逻辑复杂，编程语言是搞不定的。

一种数据同步软件不应该被推崇，区块链被神化、妖魔化了。也因此，不能说区块链没有价值，因为区块链是且只是一种工具软件。