## 区块链概念的学习路径

目前整个业界还处于区块链发展的萌芽时期，其概念也还在不断发展和完善中，这就给一些初学者带来了很大的困惑。

从区块链基础概念的发展路径循序渐进地去理解它，是一个非常好的模式——这就像我们学习生物必须顺着生物发展的轨迹，也就是从低等生物到高等生物；学习化学必须先从元素周期表的某些元素开始。

譬如因为区块链源于比特币，我们首先就应该仔细阅读中本聪的论文《比特币：一种点对点的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）。经过简单梳理之后，我们会发现这篇论文的一些关键信息点：

* 采用带有时间戳（timestamp）标记的分布式数据库记录数据；
* 数据库本身即是由不断有序增加的区块链条构成，或者说数据被记录在一种链状的时态数据库里；
* 区块则按时间顺序前后相连而形成区块链条，并且每个区块都通过密码学方法使之与其前后区块唯一关联，做到所有的历史数据井然有序地保存下来。
* 具备可靠且适合于自身需求的共识机制，来保障去中心化数据记录和数据验证机制的可靠性，从而做到数据能够去信用（trustless）和抗审查（anti-censorship）；
* 数据公开透明；
* 通过点对点（peer-to-peer）技术，保障数据能够及时分发。

通过百度百科等工具的辅助，你完全可以自己顺着这些信息点很快搞清楚以下区块链技术的重点概念：

1. **采用****带有时间戳（timestamp）标记的分布式数据库记录数据**

**时间戳**是指格林威治时间1970年01月01日00时00分00秒(北京时间1970年01月01日08时00分00秒)起至现在的总秒数。通俗的讲，时间戳是一份能够表示一份数据在一个特定时间点已经存在的完整的可验证的数据。它的提出主要是为用户提供一份电子证据，以证明用户的某些数据的产生时间。在实际应用上，它可以使用在包括电子商务、 金融活动的各个方面，尤其可以用来支撑公开密钥基础设施的 “不可否认” 服务[3]。

时间戳的获取，一般是通过时间接收设备（如GPS，CDMA，北斗卫星）来获取时间到时间戳服务器上，并通过时间戳服务器签发时间戳证书。

带有时间戳（timestamp）标记的分布式数据库，技术也属于时态数据库（Temporal database）的一种，是内建时间特性的数据库。

每个区块有了时间戳（timestamp），比特币账本才能根据时间顺序前后相连，而形成区块链。



图1：时态数据库

1. **数据库由不断有序增加的区块构成，或者说数据被记录在一种时态数据库的每个区块（block）中。**

比特币在数据记录方面采用了十分轻量级的文本数据格式JSON来构建自己的**时态数据库（**Temporal Database）。每一个区块，就是一个独立的数据表。比特币每十分钟新增一个区块，也就意味着它每十分钟新增一张数据表。

右边的二维码是百度百科对“时态数据库”的详细解释。

1. **区块则按时间顺序前后相连而形成区块链条，且每个区块都通过密码学方法使之与其前后区块唯一关联。**

因为每个区块都带有时间戳（timestamp）标记，因此所有区块就能按照时间顺序前后相连，而形成一条区块长链。加上每个区块都通过密码学方法使之与其前后区块唯一关联，那么这个链条的区块排序不光确定无疑，在关联过程中，由于采用的是与整个区块数据直接相关的**hash**值，亦即任何数据的变化必然造成hash值的不同，就能保障一个区块里的数据无法在任何时候被偷天换日。

近年来**有向无环图（Directed Acyclic Graph, DAG）**技术被引入到区块链领域，并且一度成为热点。简单地说它是通过父交易证明子交易，来保证交易数据的真实可靠。因为它突破了区块链的区块概念。有的人认为它将会成为下一代区块链的技术基础。鲜有人知道，高手已经证明以太坊底层就是最简版的有向无环图——有人不知道，有人装着不知道，有人一心要钻牛角尖，这就是区块链现在复杂之所在。

1. **具备可靠且适合于自身需求的共识机制，来保障****去中心化****数据记录和数据验证机制的极端可靠性，最终达到数据能够抗审查（anti-censorship）的目的。**

所谓**抗审查（anti-censorship）**，就是区块链里面的数据不可被伪造、篡改或删除。区块链抗审查的特性，需要通过适当的共识机制，保障通过去中心化的模式记录数据和验证数据才能得以实现。

比特币的共识机制是基于随机散列的工作量证明（proof-of-work）。这个机制归功于已经过世的科学家Hal Finney。是的，你在百度百科找不到他的词条。

1. **数据公开透明。**

抗审查（anti-censorship）实现了数据永存，但如果数据非公开透明，那么数据的完整性连同数据不可被伪造、被篡改等等，就都是一句空话。

1. **通过点对点（peer-to-peer）技术，保障数据能够即时分发。**

**点对点技术（peer-to-peer，简称P2P）**又称对等互联网络技术，它只有对等协议，没有服务器和客户端的概念。这也就是说每个比特币全节点钱包都可以既是客户端，同时也是服务器！除非互联网上无人使用全节点钱包，否则比特币就永远在线。这就是比特币玩家、自由音乐人张张创作《杀不死的比特币》的灵感源泉。

点对点技术在电驴（eDonkey）、BT分享和下载方面得到了很广泛的应用，但因为它们的种子仍然需要通过中心化的网站传播，因此难逃中心化模式的厄运，近年来迅速衰落——这也从侧面告诉我们：区块链项目如果不坚持彻彻底底的去中心化，一切都将会是过眼云烟！

不知不觉，我们已经学习和重温了一些基础概念，对吧？

而且，大家会突然发现作为年轻一代的我们自身的很多学习与发展的天然优势，也突然发现了时代赋予我们的责任感，以及无数前辈们呕心沥血、穷极一生之智慧和殷切之希望为我们铺垫的美好未来！

**必须要声明下了：**

百度百科并非自由的百科全书，无法和“维基百科”（www.wikipedia.org）相提并论。维基百科遵照Creative Commons Attribution-ShareAlike 3.0开源协议完全开放，百度百科则完完全全属于百度所私有。并且，百度百科确实有毒！

但因为网络封锁的原因，为照顾不会使用VPN的学生，有的地方，我们仍引用百度百科可用的词条解释。