第07课：区块链...

大家好，我是丹华。今天介绍区块链技术的第三个支柱分布式账本技术，另外会介绍区块链的主要分类。

7.1 分布式账本技术

分布式账本技术（distributed ledger technology，简称 DLT，也称为 shared ledger），是一种在网络成员之间共享、验证和同步的、记录成员之间的交易的分布式数据库，需要匹配一个点对点网络和共识算法，节点成员一般是地理上分开的，每个节点都存储一套账本的副本，没有中央管理者和中心化的数据存储。

如图7.1所示，中心化账本和分布式账本的区别非常明显。

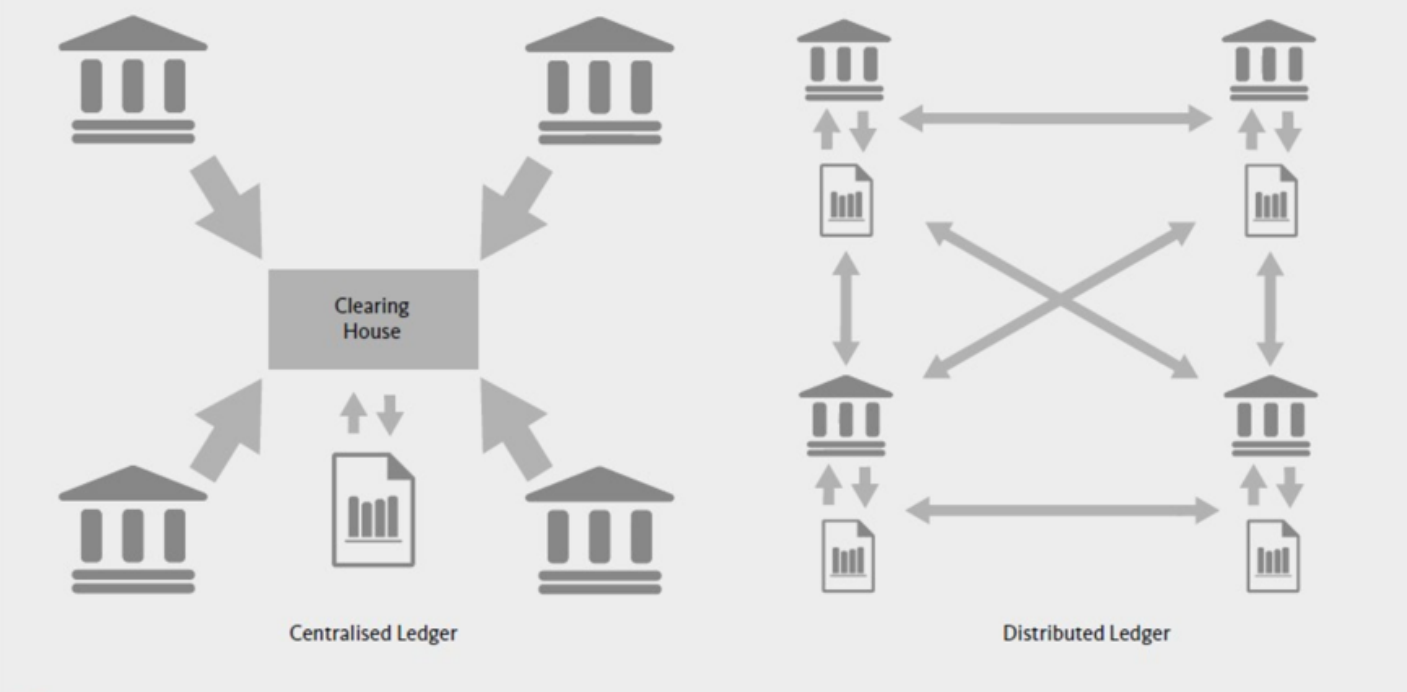

图7.1 中心化账本和分布式账本

网络中的参与者根据共识原则来制约和协商对账本中的记录的更新，没有中间的第三方权威中介机构的参与。每个节点都可以参与验证和监督交易的合法性，同时也可以共同为其作证。分布式账本中的每条记录都有一个时间戳和唯一的密码签名，这使得账本成为网络中所有交易的可审计历史记录。

分布式账本可能是区块链行业里，最具有争议性的概念了。有些人认为它跟区块链是同义词，没什么区别。有些人则争辩说，区块链是线性的、链式数据结构，而分布式账本则不一定是链式，如 IOTA 的 Tangle，即，分布式账本不一定用区块链技术实现。从字面上来看，分布式账本强调了“分布式”和“账本”两个侧面。也有人因为分布式账本不强调“币”的属性，认为分布式账本适合于面向企业的联盟链模式。

鉴于区块链和分布式账本都处于发展初期，概念没有定论是正常的，我们建议读者根据具体的文本环境灵活理解。本文中，我们取分布式账本的狭义含义，即字面意义，并认为分布式账本是广义区块链技术的一个重要组成部分。

分布式账本与传统“分布式存储”的区别

传统分布式存储一般是将数据按照一定规则分割成许多份进行存储，而且一般是通过中心节点往其他备份节点同步数据，中心节点负责数据管理。传统存储模式是跟日益中心化的互联网发展密切相关的。大公司自然对应着大规模的数据中心，而这有必然对应着可能的单点故障、信息泄露、信息滥用等中心化信任问题。普通用户只能选择相信大公司的“好意”，而不是在技术上保证信息安全。

分布式账本技术可以从根本上改善这一点。由于各个节点均各自维护了一套完整的数据副本，任意单一节点或少数集群对数据的修改，均无法对全局大多数副本造成影响。换句话说，无论是服务提供商在无授权情况下的蓄意修改，还是网络黑客的恶意攻击，均需要同时影响到分布式账本集群中的大部分节点，才能实现对已有数据的篡改，否则系统中的大多数诚实节点将很快识别并追溯到恶意行为。这显然会大大提升系统的可信度和安全性。

7.2 区块链的分类

按照区块链网络节点的公开程度，可以将区块链分为三类：公有链（public blockchain）、联盟链（consortium blockchain）和私有链（private blockchain）。

公有链（Public Blockchain）

公有区块链开放程度最高、去中心化程度最高、节点信任要求最低的区块链：任何个体都可以发送交易、成为节点、参与共识过程，且交易能够获得网络的有效确认。参与节点按照系统规则自由接入网络、不受控制，节点间基于共识机制开展工作。公有链向任何人开放，任何人都可以下载获得完整区块链数据，即全部账本。公有区块链是最早的区块链形态，也是目前应用最广泛的区块链。典型的数字货币如比特币、以太坊、莱特币等都是公有链。

联盟链（consortium blockchain）

联盟链是部分去中心化的区块链，由若干机构联合发起，介于公有链和私有链之间，只对有限的参与者开放。节点之间有一定的相互信任，节点类型可能有两类或更多类，各节点在不需要完全互信的情况下实现数据的可信交换，节点对应有权利和义务的分配，并对共享数据的访问做一定的访问控制。联盟链节点通常有对应的实体机构，适用于多个实体构成的组织或联盟，通过授权后才能加入或退出网络。

联盟链是一种公司与公司、组织与组织之间达成联盟的模式。比如几十家商业银行可以组成一个银行间的联盟链。联盟链的实质是产业联盟的区块链化，由某个群体（产业）内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不参与记账过程。因此对联盟链来说，预选节点的多少，如何决定每个块的记账者成为主要风险点。

跟公有链中每个节点地位等同不同，联盟链的节点是分层的、不对等的，有些节点权力比较大，如控制节点。

联盟链的特点是，节点之间互相熟悉，信任程度较高；节点、账本的可控制，满足监管和准入需求；通过分布式账本实现不可篡改的加密交易数据，交易可追溯不可抵赖，实现了较高程度的隐私保护（牺牲了去中心化程度）：交易匿名，交易不可关联；可监管和审计。

典型的联盟链项目有超级账本 HyperLedger 和 R3 等。我们将在第三篇中介绍这些主流的联盟链项目。

私有链（Private Blockchain）

私有链是只对一个参与者开放、完全中心化的区块链，其写入权限由中心机构控制，读取权限可视需求有选择性地对外开放，只有被许可的节点才可以参与并且查看数据。比如一个企业内部的区块链。私有链一般适用于特定机构将自己的业务流程实现区块链化改造。

关于区块链的分类，还可以分为两类：许可区块链和无许可区块链。

许可区块链（permissioned blockchain）

如果区块链的节点需要许可和授权可能加入网络，则称为许可区块链。许可区块链可以进一步细分为私有链、联盟链。

无许可区块链（permissionless blockchain）

如果区块链对所有人开放，节点加入网络不需要许可，可以自由加入或推出网络，节点之间不需要信任（即允许恶意节点的存在），则称为无许可区块链，等同于公有区块链。

区块链分类小结

从目前的行业实践来看，联盟链的处理性能和效率更高，更易标准化，因此一般大企业更重视联盟链的开发。但是联盟链内是没有代币发行，因此对节点的激励机制上可能存在问题。

现在越来越多的人们开始意识到，没有代币的区块链，无法发挥出区块链模式的所有潜力，实际上是将区块链降格为一个普通的 IT 技术实施。虽然公有链在处理性能和效率有一定的瓶颈，但借助于开放式的社区和创新，系统价值直接反应在代币价格上，激励机制充分，因此大多数创业企业和开发者们更重视公有链的开发。

展望未来，有可能联盟链和公有链两分天下，互相融合。也有激进者认为，公有链开放程度更高、信任要求更低，因而变革更彻底，而联盟链很难解决代币发行和节点激励的问题，容易变成形式上的区块链而失去活跃度和创新性，最终可能会发生公有链一统天下的局面。