第3章 区块链点对点通信

【本章导学】

区块链系统与传统中心化系统在数据通信方面存在较大区别，传统中心化节点的数据通信大多是以客户端/服务器(Client/Server，C/S)架构实现；在区块链系统中，由于节点地位相同，所以通信以去中心化的方式实现，与传统技术相比在网络拓扑方面有较大不同。另外，由于区块链具有不同分类，每个分类基于的应用场景不同，所采用的网络拓扑通信方式也会不同。本章将围绕区块链点对点通信方式展开讲述。

【学习目标】

- 点对点网络的基本概念和特性；
- 点对点网络在区块链的应用场景。

3.1 点对点网络

区块链为一种“分布式记账”的技术，记录了一系列有顺序的交易。以传统的交易系统为例，比如银行系统均采用中心服务器架构，以银行服务器为中心节点，每个网点、ATM机、手机App为客户端。当发起转账时，首先提供银行卡账号、密码等信息证明身份，然后生产一笔转账交易，发送到中心服务器后，中心服务器校验余额是否充足等信息，然后记录到中心服务器，即可完成一笔转账交易。

传统的网络服务架构大部分采用C/S架构或者都是浏览器/服务器(Browser/Server，B/S)架构，都是通过中心化的服务端节点，对需要申请服务的客户端或者是浏览器端进行应答和服务，客户端之间的通信需要依赖服务器的协作。

举个例子，即时通信客户端(例如微信等)进行消息收发的时候，手机客户端都会先把消息发给中心服务器，再由中心服务器转发给接收方客户端；而当通过银行转账时，则是会由银行先查看转账方的账户是否有足够余额，确认足够后，银行将这部分账

款划给收款方账户。

C/S模式和B/S模式都属于中心化的服务器架构，这种架构的优点是便于对服务进行维护和升级，同时便于管理。但这种架构也有缺点：首先由于中心化服务器架构只有单一的服务端，因此当服务端节点出现故障时，整个服务都会陷入瘫痪，也就是“单点故障”；其次，中心化服务器节点的处理能力是有限的，因此中心服务节点往往成为整个网络的瓶颈。

在区块链网络中，并不存在一个中心节点来校验并记录交易信息，校验和记录工作由网络中的所有节点共同完成。当一个节点需要发起转账交易时，需要指明转账目的地址、转账金额，还需要对该交易进行签名。

由于不存在中心服务器，所以该交易会随机发送到网络中的邻近节点，邻近节点收到交易信息后，对交易的签名进行校验，确认身份合法性后，再校验余额是否充足等信息。验证完成后，它将该信息转发至自己的邻近节点。如此反复，直至网络中所有节点都收到该交易。最后矿工获得记账权后，则将该交易打包至区块，然后广播到整个网络。广播的过程同交易的广播过程，依然采用一传十、十传百的方式完成。收到区块的节点完成区块内容的校验后，将区块保存到本地，即交易生效。如图3-1所示为数据传输点对点比较。

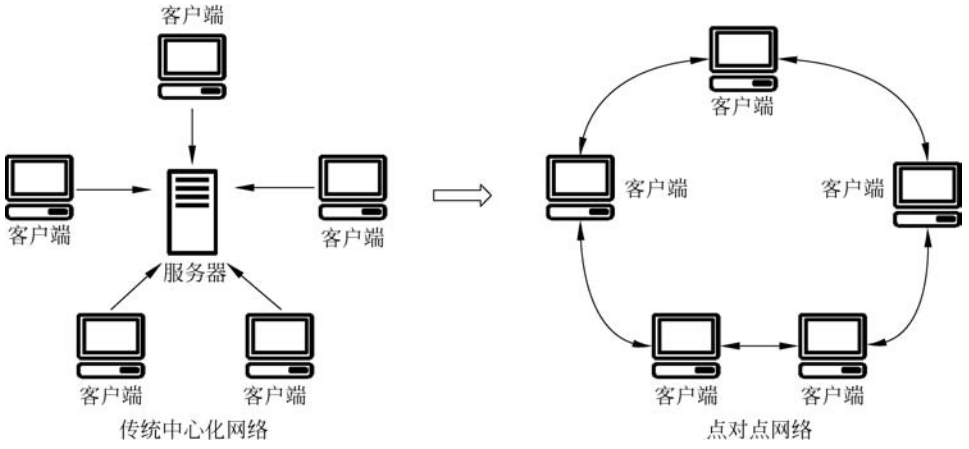

图3-1　中心化与去中心化数据传输网络比较

3.1.1　点对点网络的基本概念

不同于有中心服务器的中心化网络系统，点对点(Peer-to-Peer，P2P)网络消除了中心化服务节点，将所有的网络参与者视为对等节点(Peer)，并在它们之间进行任务和工作负载分配。P2P网络结构打破了传统的中心服务器架构，去除了中心服务器，

是一种依靠用户群共同维护的网络结构。

3.1.2 点对点网络的特点

由于节点间的数据传输不再依赖于中心服务节点，因此 P2P 网络具有以下特点。

(1) 非中心化：P2P 网络的优势是它是非中心化的，网络中的资源和服务分散在所有节点上，信息的传输和服务的实现都直接在节点之间进行，可以无须中间环节和服务器的介入。

(2) 可扩展性：P2P 网络通常都是以自组织的方式建立起来的，并允许节点自由地加入和离开。在 P2P 网络中，理论上其可扩展性几乎可以认为是无限的。例如，在传统的通过中心化服务器下载方式中，当下载用户增加之后，下载速度会变得越来越慢，然而 P2P 网络正好相反，加入的用户越多，P2P 网络中提供的资源就越多，下载的速度反而越快。

(3) 健壮性：P2P 网络服务是分散在各个节点之间进行的，部分节点或网络遭到破坏对其他部分的影响很小。P2P 网络一般在部分节点失效时能够自动调整，保持其他节点的连通性。

3.2 点对点网络在区块链中的应用

总体来说，虽然客户端/服务器和浏览器/服务器等中心化的服务器架构应用非常成熟，但是这种存在中心服务节点的模式，显然不符合区块链网络的需求。

在区块链系统中，要求所有节点共同维护账本数据，即每笔交易都需要发送给网络中的所有节点。如果按照传统的中心化的服务器架构，中心节点要将大量交易信息转发给所有节点，这也是非常低效率的。

P2P 网络的这些设计思想和区块链的理念完全契合。在区块链中，所有交易及区块的传播不需要发送者将消息发给所有节点。节点只需要将消息发送给一定数量的相邻节点即可，其他节点收到消息后，会按一定的规则发给自己的相邻节点，通过指定的数据通信方式，实现节点间的数据传输，最终将消息发给所有节点。

3.2.1 点对点网络在公有链中的应用

公有链是区块链点对点网络的最典型的应用，在公有链中所有节点的联络度均相

等，从理论上说所有节点都会有与其他节点通信的可能，这样构建出的区块链网络如图 3-2 所示。

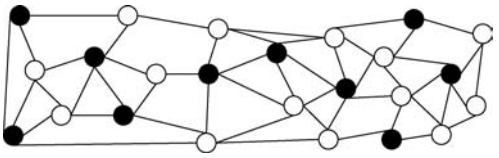

图 3-2　点对点应网络在公有链的应用

由于公有链的区块链节点有可能分布在世界各个地方，为了保证网络中所有的节点都能成为网络成员，如何设计点对点网络架构是区块链应用的一个研究方向。在区块链网络中发现周围节点并与周围节点通信的处理流程如下所述。

（1）节点会记住它最近成功连接的网络节点，当重新启动后它可以迅速与先前的对等节点网络重新建立连接。

（2）节点会在失去已有连接时尝试发现新节点。

（3）当建立一个或多个连接后，节点将一条包含自身 IP 地址的消息发送给其相邻节点。相邻节点再将此消息依次转发给它们各自的相邻节点，从而保证节点信息被多个节点所接收，保证连接更稳定。

（4）新接入的节点可以向它的相邻节点发送获取地址消息，要求它们返回其已知对等节点的 IP 地址列表。任何节点都可以找到需连接到的对等节点。

（5）在节点启动时，可以给节点指定一个正活跃节点 IP，如果没有，客户端也维持一个列表，列出了那些长期稳定运行的节点。这样的节点也被称为种子节点（其实和 BT 下载的种子文件道理是一样的），就可以通过种子节点来快速发现网络中的其他节点。

比特币节点通常采用 TCP 协议、使用 8333 端口与相邻节点建立连接，建立连接时也会有认证“握手”的通信过程，用来确定协议版本、软件版本、节点 IP、区块高度等。当节点连接到相邻节点后，接着就开始跟相邻节点同步区块链数据（轻量级钱包应用其实不会同步所有区块数据），节点间会交换一个 getblocks 消息，它包含本地区块链最顶端的哈希值。如果某个节点识别出它接收到的哈希值并不属于顶端区块，而是属于一个非顶端区块的旧区块，则说明其自身的本地区块链比其他节点的区块链更长，并告诉其他节点需要补充区块，其他节点发送 getdata 消息来请求区块，验证后更新到本地区块链中。

3.2.2　点对点网络在联盟链中的应用

联盟链也是点对点网络通信的应用场景之一。与公有链不同，在联盟链中的不同

节点具有不同的角色与权限。以超级账本 Fabric 网络系统为例，系统网络包括诸多类型的节点，如 Orderer 节点、验证节点、提交节点等，在网络中数据的流向也不同。整体上具体的流通方式如图 3-3 所示。

由于在联盟链中节点的权限不同，数据传输往往会流向局部的数据中心，再从数据中心将数据分发给其他的节点，所以在点对点网络在联盟链中并不是完全的去中心化，我们可以理解为“弱中心化”或者“多中心化”网络。

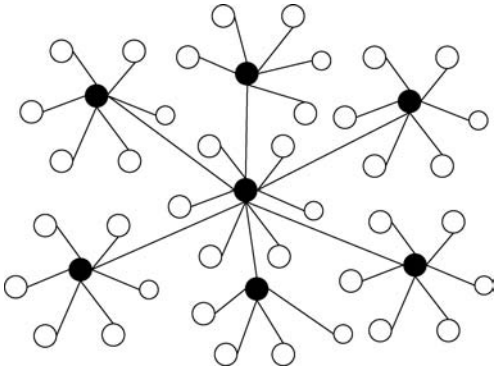

图 3-3　点对点网络在联盟链的应用

第4章 区块链的分布式共识

【本章导学】

在区块链系统这样的非中心化系统中，并不存在中心权威节点，由于参与的各个节点的自身状态和所处的网络环境不尽相同，而交易信息的传递又需要时间，并且消息传递本身并不可靠，所以每个节点收到的需要记录的交易内容和顺序也很难保持一致。此外，由于区块链中参与的节点身份难以控制，还可能出现恶意节点故意阻碍信息传递或者发送不一致的信息给不同节点，从而扰乱整个区块链系统的记账一致性。因此，区块链系统的记账一致性问题，是一个非常关键的问题，关系到整个区块链系统的正确性和安全性。

【学习目标】

- 熟悉分布式共识的基础知识以及分布式共识的历史；
- 熟悉分布式共识的定理以及分布式算法的分类；
- 掌握常用分布式共识算法的原理、实现过程以及应用场景；
- 熟悉共识算法的实训案例。

4.1 分布式共识的基础

4.1.1 “分布式”与“共识”

可以把分布式共识分为“分布式”和“共识”两方面进行理解。

1. 分布式

分布式的字面含义是分散的，与其相对的概念是中心化。在区块链领域中，分布式的概念应用很广，但主要可以概括为每个节点有自主管理权(Self-Governance)，且成员之间可以点对点地完成信息的交换或资产的交易。能实现以上功能的系统称为