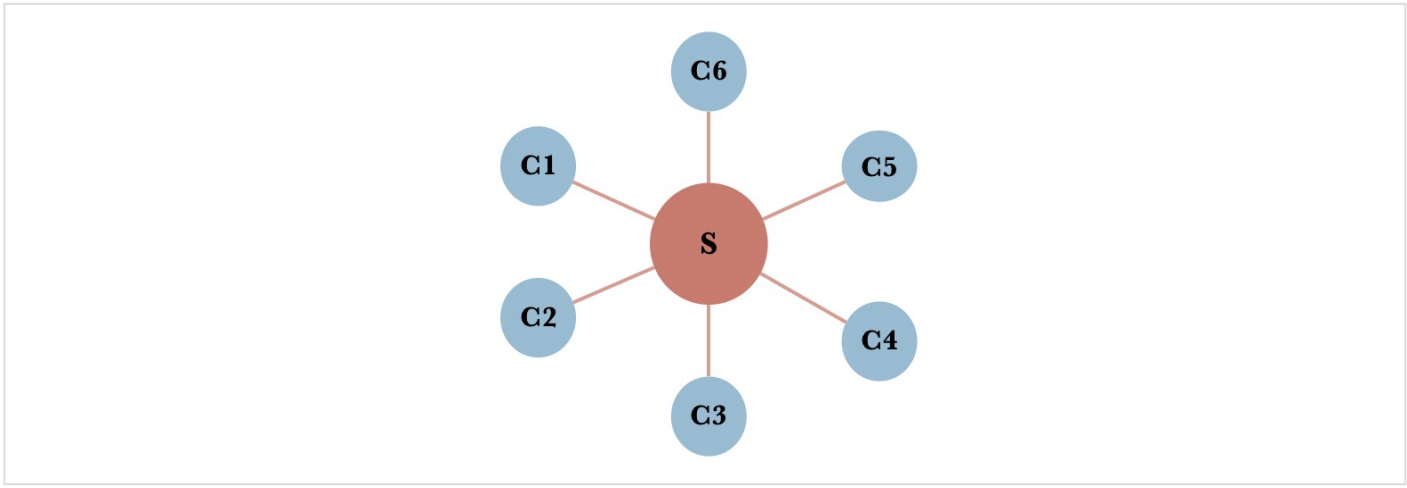
分析比特币网络：一种去中心化、点对点的网络架构

2017-11-07 | 2018-07-31 | 比特币

比特币采用了基于互联网的点对点（P2P：peer-to-peer）分布式网络架构。
比特币网络可以认为是按照比特币P2P协议运行的一系列节点的集合。
本文来分析下比特币网络，了解它跟传统中心化网络的区别，以及比特币网络是如何发现相邻节点的。

中心化网络

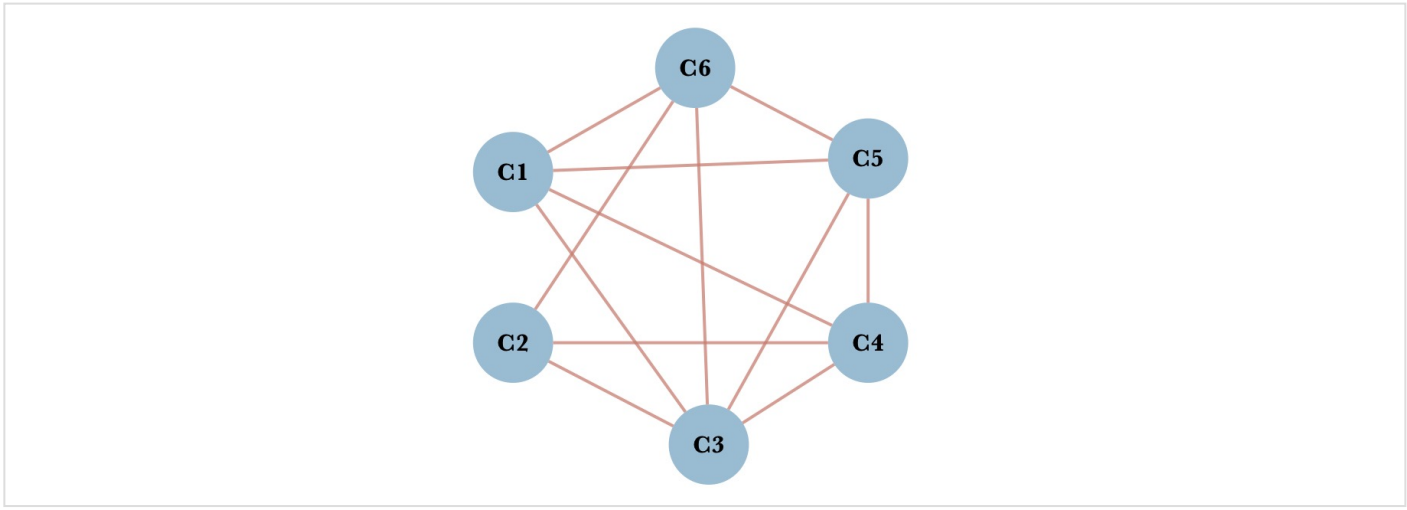
为了更好的理解P2P网络，我们先来看看传统的中心化模型：



这是一种典型的星型（“中心化”）结构，我们常见B/S及C/S网络架构就是这种模型，C1 、C2 、C3等之间没法直接的连接，C节点如果要连接必须要通过中心化S节点做为桥梁。
中心化节点充当服务者、中介作用，比如我们没有办法把资金直接从一个人转移给另一个人，必须通过银行这个中介。

P2P网络

P2P网络是指位于同一网络中的每台计算机都彼此对等，各个节点共同提供网络服务，不存在任何“特殊”节点，每个网络节点以扁平（flat）的拓扑结构相互连通。



对比中心化网络，在P2P网络中不存在任何服务端（server）、中央化的服务。
P2P网络的节点之间交互连接、协同，每个节点在对外提供服务的同时也使用网络中其他节点所提供的服务，每个

节点即是服务端又是客户端。
P2P网络模型除应用于比特币网络，使用广泛的BT下载就是基于P2P网络。

P2P网络不仅仅去除了中心化带来的风险（中心化可能作恶），还可以提高传输的效率。（中心化网络当能也有优点）

如何发现节点

既然每个网络节点都是平等的（是指在网络层面上节点是平等的，但各节点在功能上可以有不同的分工, 如钱包节点、挖矿节点等），不存在任何“特殊”中心节点，那么当新的网络节点启动后，它是如何跟其他的节点建立连接，从而加入到比特币网络呢?

> 在中心化网络中，新加入的节点只要连接“特殊”的中心节点就可以加入网络。

为了能够加入到比特币网络，比特币客户端会做一下几件事情:

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getaddr消息，要求它们返回其已知对等节点的IP地址列表。节点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。

节点通信简述

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），节点们会交换一个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，就说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。