VICTORLAMP

区块链技术基础篇
之三：白话P2P (Peer-to-Peer)网络

e休，爱编程的葫芦娃：exiu@victorlamp.com

煤油灯科技公司 http://www.victorlamp.com

多媒体课程：《深入浅出区块链技术基础篇》

深入浅出区块链技术

课程目录

《区块链技术基础篇之一：白话非对称加解密》
《区块链技术基础篇之二：白话哈希算法》
《区块链技术基础篇之三：白话P2P网络》
《区块链技术基础篇之四：白话拜占庭将军问题》
《区块链技术核心篇之一：比特币区块链起源及原理》
《区块链技术核心篇之二：比特币区块链密钥与地址》
《区块链技术核心篇之三：比特币区块链交易共识》
《区块链技术核心篇之四：比特币区块链核心架构》

讲师介绍

网名：一休

2015 年开始，从事区块链技术开发，先后成功的研发出：区块链技术的数字版权管理（DRM）系统、基于区块链IPFS的CDN产品开发。

是多项区块链技术专利发明人。

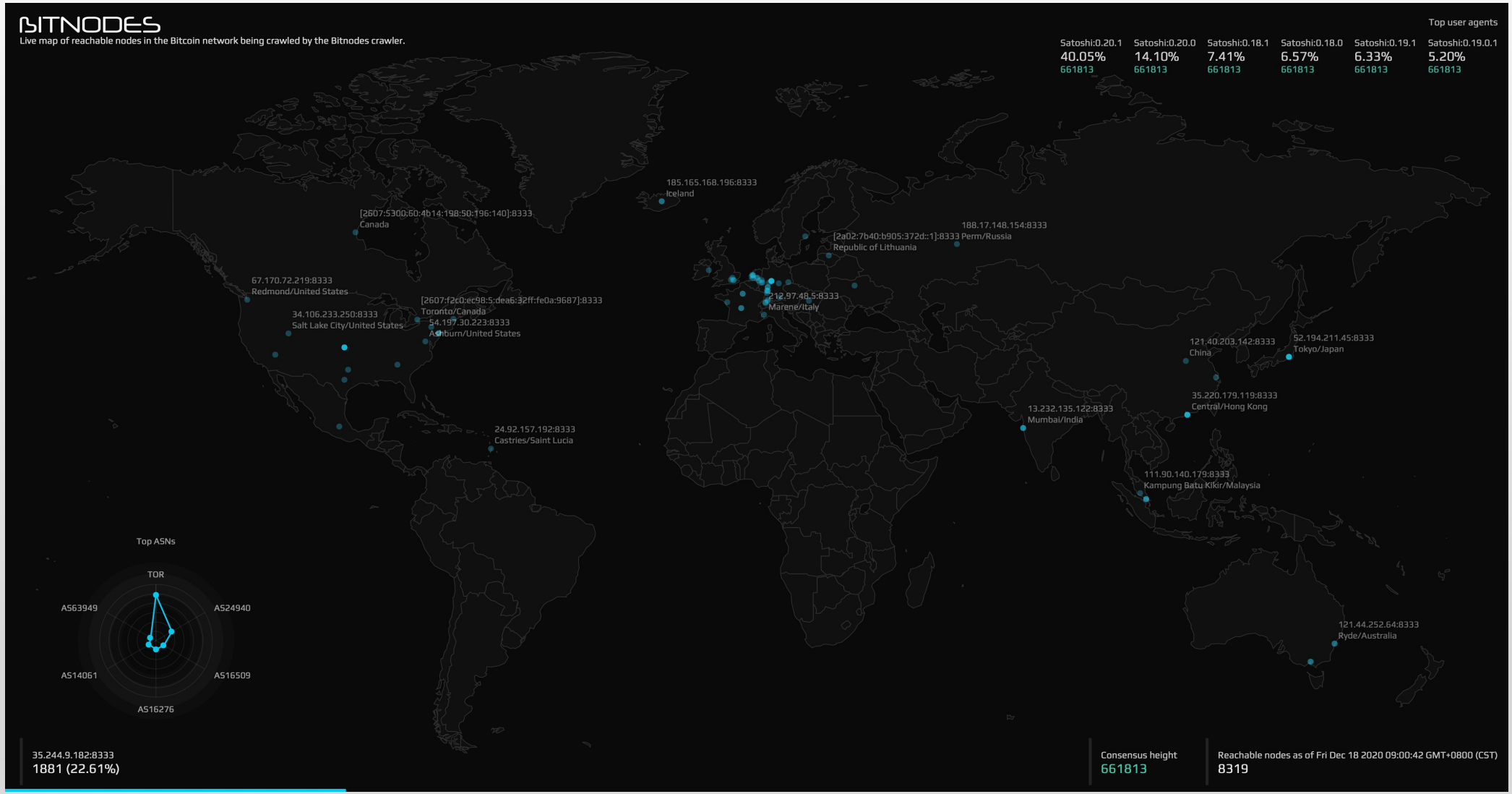
对于比特币区块链、IPFS项目源码非常熟悉。

本人负责的基于区块链的创新技术方案，获得了当年华为公司年度十大发明奖。

区块链技术大量依赖于P2P网络，可以说没有P2P就没有区块链现在的发展。而区块链拥有去中心化的应用理论，所以对P2P的过程有着近似严苛的安全要求。

本课程带领读懂区块链技术之核心—P2P （peer-to-peer）网络。

比特币网络是一个全球化的无国界的网络，是一个没有中心的P2P对等网络



比特币区块链的实时网络地图：https://bitnodes.io/nodes/live-map/

VICTORLAMP 煤油灯科技

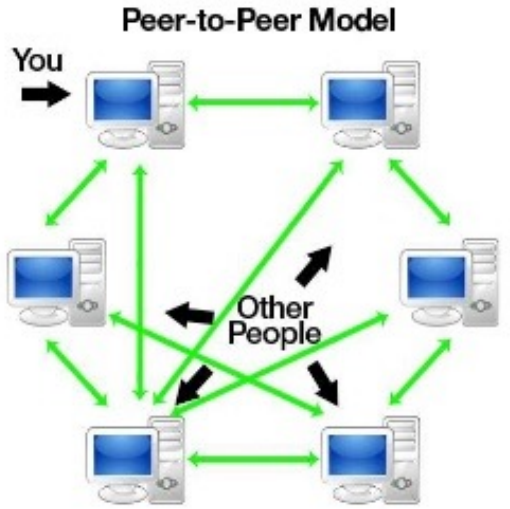
什么是P2P （peer-to-peer）网络

去中心化P2P网络又称为对等式网络，或者叫点对点网络。这是一种无中心的服务器、完全由用户群进行交换信息的互联网体系，P2P网络的每一个用户即是一个客户端，同时也具备服务器的功能。采用P2P技术实现的每台计算机既是客户端，也是服务器，他们的功能都是对等的。

传统互联网业务网络是中心化的：在P2P技术之前，我们所有的网络应用都采用C/S或者B/S架构来实现的，然而在之前C/S架构的应用程序中，客户端软件向服务器发出请求，服务器然后对客户端请求做出响应，在这种情况下，如果客户端越多，此时服务器的压力就越大。

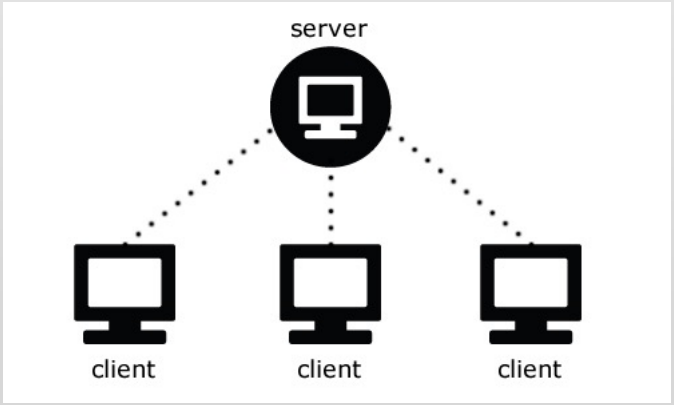
WHAT IS P2P?

- A peer-to-peer network, P2P, is considered to be a type of network architecture composed of contributors that make their resources available to other contributors on the same network without the need for a server to oversee the transfer of information.



比如：比特币网络、BitTorrent下载

传统业务中心化网络

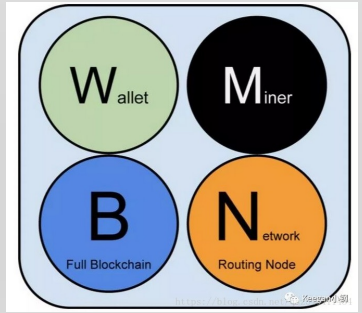


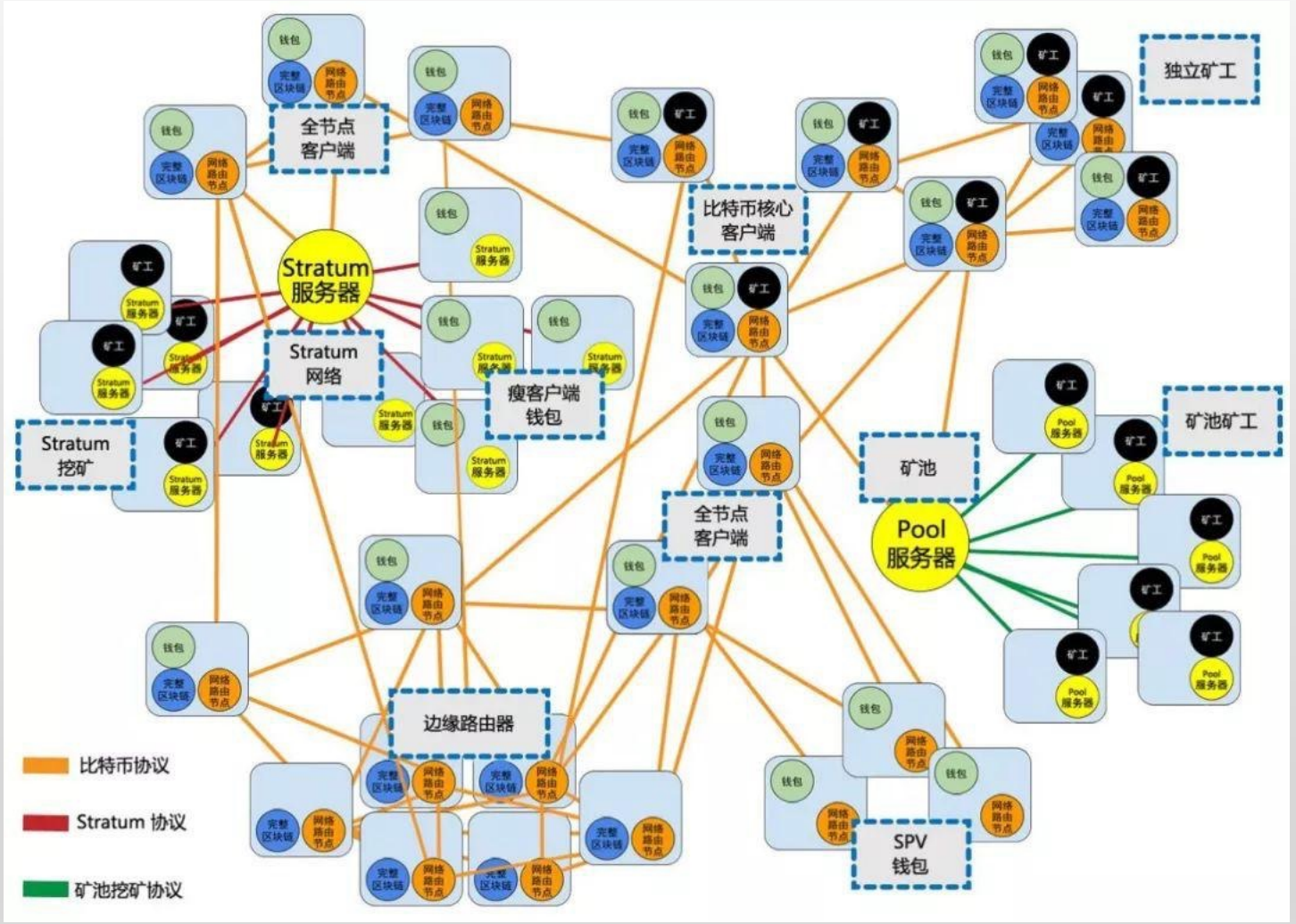
比如：新浪新闻网站、淘宝、京东

比特币区块链P2P网络

比特币网络中的节点主要有四大功能：钱包、挖矿、区块链数据库、网络路由。

每个节点都会具备路由功能，但其他功能不一定都具备，不同类型的节点可能只包含部分功能，一般只有比特币核心(bitcoin core)节点才会包含所有四大功能.





煤油灯科技
VICTORLAMP

P2P网络面临的问题

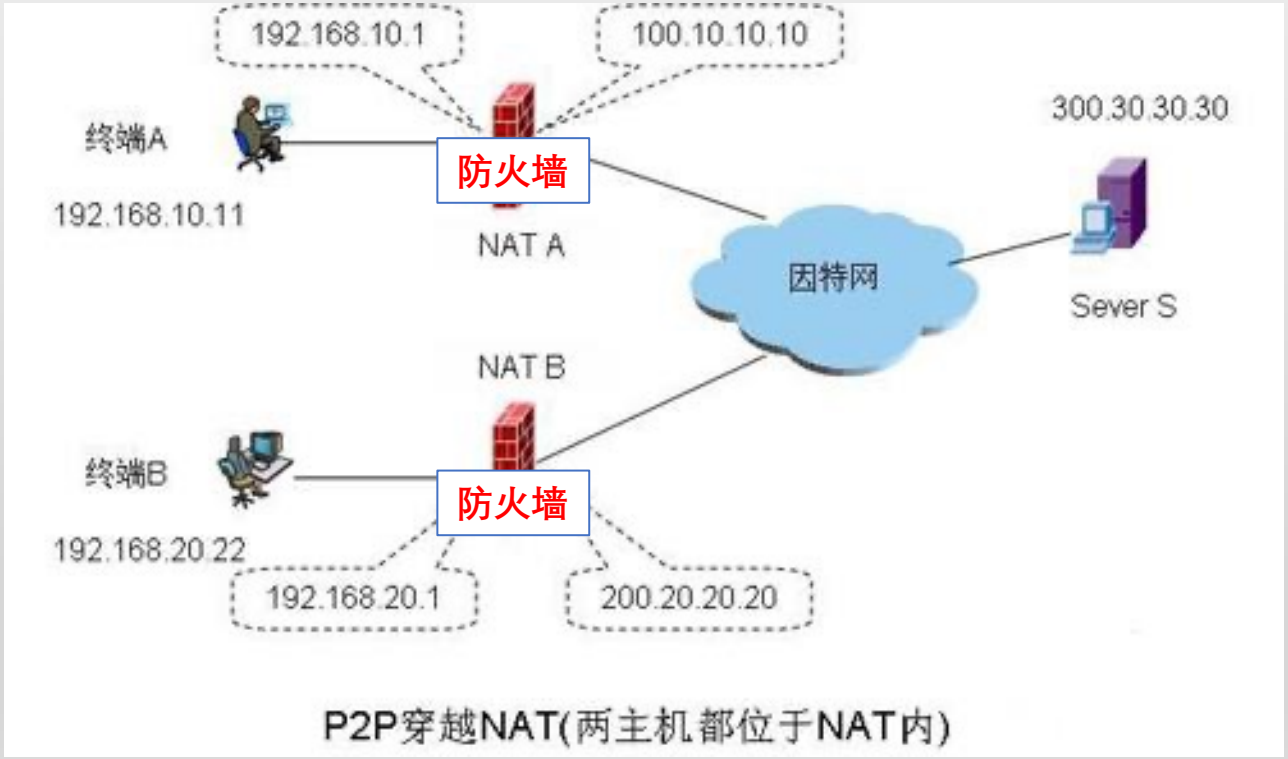
通常情况下，通过外部互联网是找不到我们在家里或者办公室的电脑的。

比如说你要在办公室访问你家里的电脑是不行的，或者你要在外面用手访问你家里的电脑是不行的。

为什么？

因为，我们的电脑通常都是被各种各样的“防火墙”给挡在互联网外面。

“墙里”和“墙外”的互通是需要通过各种限制和代理的。



P2P穿越NAT(两主机都位于NAT内)

NAT 产生背景

互联网中主要依靠IP进行寻址，IPv4地址使用32个比特位进行标记，一般使用点分十进制形式书写。IP地址分类如表所示：

网络类型	特征地址位	起始地址	结束地址	默认子网掩码
A	0	1.0.0.0	126.255.255.255	255.0.0.0
B	10	128.0.0.0	191.255.255.255	255.255.0.0
C	110	192.0.0.0	233.255.255.255	255.255.255.0
D	1110	224.0.0.0	239.255.255.255	----
E	1111	240.0.0.0	255.255.255.255	----

注：a 由于历史原因0.0.0.0被保留；b 127.0.0.0 - 127.255.255.255 被用作特殊用途，如127.0.0.1 用于本地回环地址lo

互联网中的IP地址分配以及TCP/UDP公共服务端口号有专门的机构进行统筹和分配——IANA（Internet Assigned Numbers Authority）。

在互联网初期，IP地址分配策略使得IP地址浪费严重，因此当互联网以超乎想象的速度发展，终端接入网络的速度爆炸式增长时，IPv4地址资源很快便被耗尽。

2011年2月3日，IANA对外宣布，IPv4地址空间最后5个地址块被分配完；

同年4月15日，亚太区委员会宣布，除了个别保留地址外，本区域所有的IPv4地址基本被耗尽。

NAT 产生背景

早期网络通信协议和标准的组织已经意识到了IPv4地址马上被耗尽的危机，因此制定了长期措施和短期措施。

- 长期措施：制定下一代互联网协议IPv6(Internet Protocol Version 6)；
- 短期措施：NAT(Network Address Translation, 网络地址转换)和CIDR(Classless Inter-Domain Routing, 无类别域间路由)。

NAT的功能是：

将一个IP地址转换为另一个IP地址。通常一个局域网由于申请不到足够的IP地址，或者为了编址方便，在局域网内部采用私有IP地址为设备编址，当设备访问外部网络时，再通过NAT将私有地址翻译成合法的共有地址。

公网IP地址可以在Internet上使用，且全球唯一，而私有IP地址则是用来在局域网中使用。私有地址范围如表所示。

IP地址范围	网络类型	网络个数
10.0.0.0 ~ 10.255.255.255	A	1
172.16.0.0 ~ 172.31.255.255	B	16
192.168.0.0 ~ 192.168.255.255	C	256

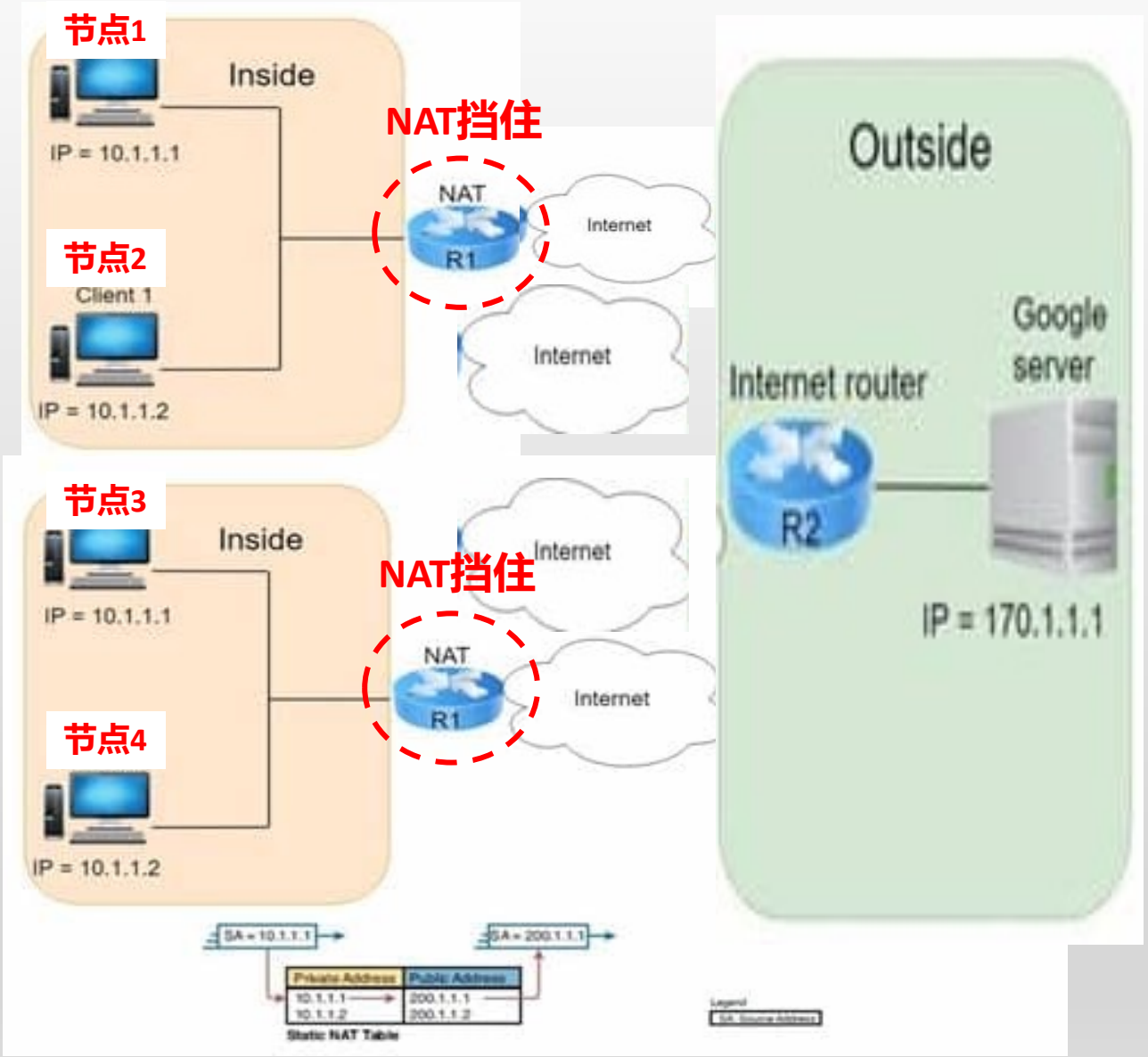
P2P网络最大的挑战：如何穿越NAT（Network Address Translation）墙?

关注点：

(1) 有了NAT以后，内网的主机不再需要申请公网IP地址，只需要将内网主机地址和端口通过NAT映射到网络出口的公网IP即可，然后通信的两端在无感知的情况下进行通信。

这也是说NAT挽救了IPV4，因为大量的内网主机有了NAT，只需要很少的公网地址做映射就可以了，可以节约出很多的IPV4地址空间，也带来了内网的安全性。

(2) 当在私网网络出口处部署了NAT网关以后，只能由内网主机发起到外网主机的连接，外网主机无法主动发起连接到内网。这样虽然对外隔离了内网主机，但同时又限制了P2P的通信，这也是NAT带来的一大弊端。



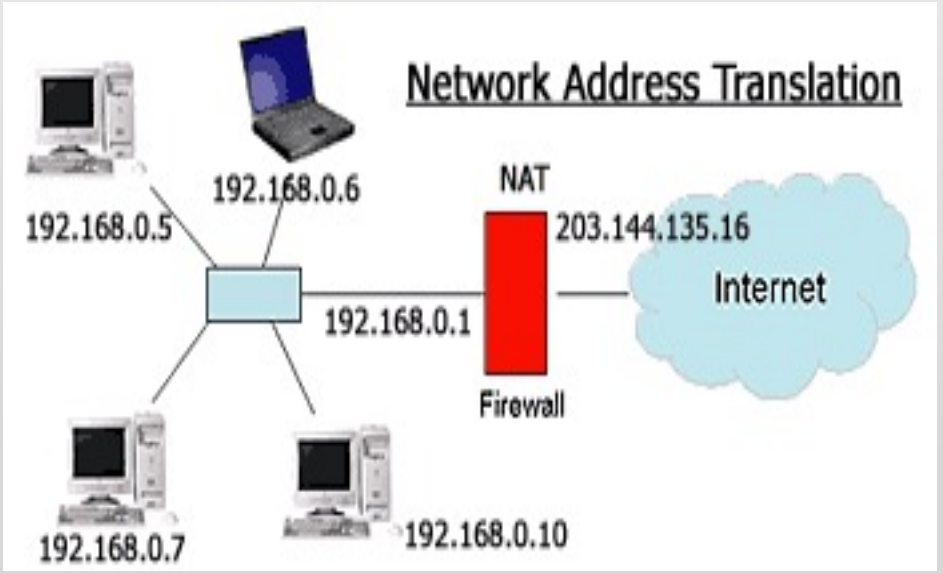
煤油灯科技

P2P网络带来的最大挑战，NAT（ Network Address Translation)

NAT英文全称是“Network Address Translation”，中文意思是“网络地址转换”，允许一个整体机构以一个公用IP（Internet Protocol）地址出现在Internet上。顾名思义，它是一种把内部私有网络地址（IP地址）翻译成合法网络IP地址的技术。NAT 可以让那些使用私有地址的内部网络连接到Internet或其它IP网络上，这个过程对用户来说是透明的。NAT路由器在将内部网络的数据包发送到公用网络时，在IP包的报头把私有地址转换成合法的IP地址。因此我们可以认为，NAT在一定程度上能够有效的解决公网地址不足的问题。

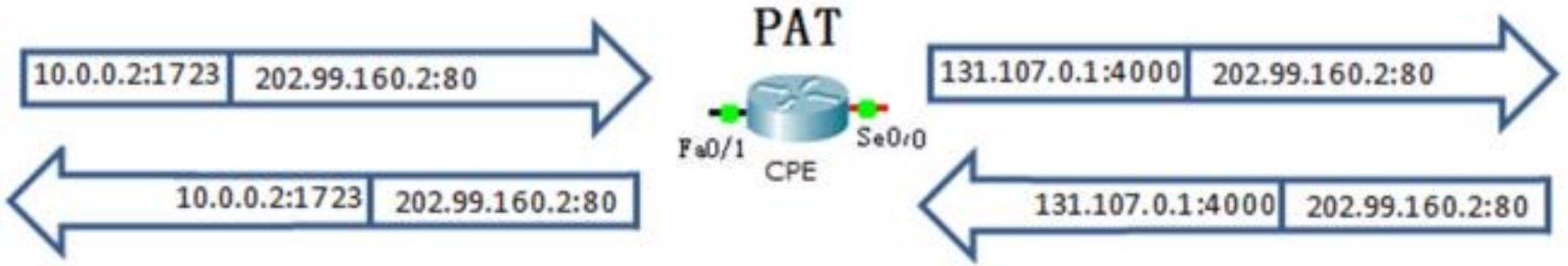
穿越NAT的意义：
NAT是为了节省IP地址而设计的，但它隐藏了内网机器的地址，“意外”起到了安全的作用。
对外不可见，不透明的内部网络也与互联网的“公平”应用，“相互共享”的思想所不容，尤其是P2P网络中“相互服务”的宗旨，所以穿越NAT，让众多内部网络的机器也参与到P2P网络中的大集体中来，一直是P2P开发者的所希望的。

穿越NAT需要借助外部的支持，说白了就是“内外勾结”，骗过NAT。很多P2P网络成功地实现了这一目标，但还是有一些“遗憾”---并非所有的情况下都可以。
由于客户端是主动登录P2P网络才可穿越，所以P2P的方式也没有违背企业的内部管理原则，毕竟“自由世界”的加入都是自觉自愿的。



NAT地址映射举例

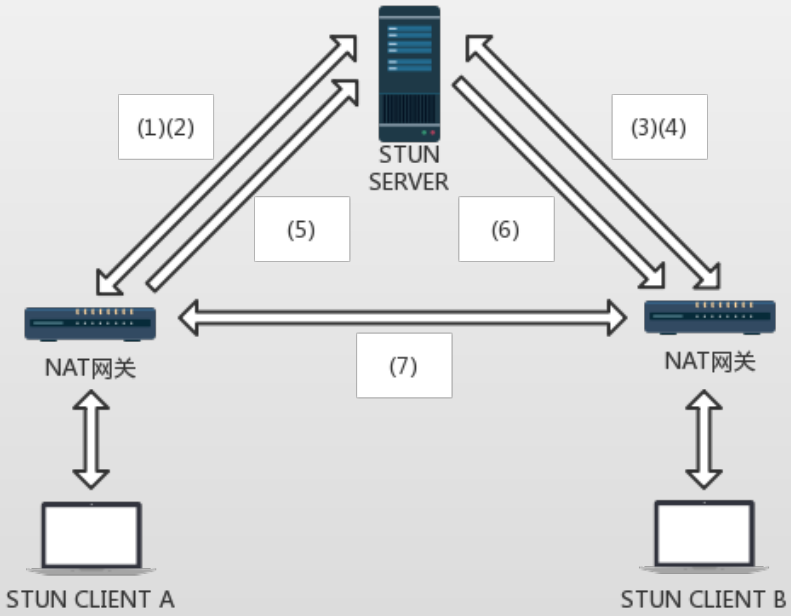
	协议	内网地址和端口	外网地址和端口	Server地址和端口
PC0 访问 Server	TCP	10.0.0.2:1723	131.107.0.1:4000	202.99.160.2:80
PC1 访问 Server	TCP	10.0.0.3:1723	131.107.0.1:4001	202.99.160.2:80
PC2访问 Server	TCP	10.0.0.4:1723	131.107.0.1:4002	202.99.160.2:80
PC3 访问 Server	TCP	10.0.0.5:1723	131.107.0.1:4003	202.99.160.2:80



局域网可使用的网段（私网地址段）有三大段：

A类: 10.0.0.0~10.255.255.255； B类: 172.16.0.0~172.31.255.255 ； C类:192.168.0.0~192.168.255.255 。

P2P网络穿越NAT的方案1： STUN全称为Simple Tranversal of UDP through NAT



(1) CLIENT A通过NAT网关向STUN SERVER发送STUN请求消息(UDP)，查询并注册自己经过NAT映射后的公网地址；

(2) STUN SERVER响应，并将CLIENT A经过转换后的公网IP地址和端口填在响应报文中；

(3) CLIENT B通过NAT网关向STUN SERVER发送STUN请求消息(UDP)，查询并注册自己经过NAT映射后的公网地址；

(4) STUN SERVER响应，并将CLIENT B经过转换后的公网IP地址和端口填在响应报文中；

(5) 此时CLIENT A已经知道了自己映射后对应的公网IP地址和端口号，它把这些信息打包在请求中发送给STUN SERVER，请求和B进行通信；

(6) STUN SERVER查询到B注册的公网地址和端口，然后将请求通过NAT网关转发给B；

(7) B从消息中知道A的公网地址和端口，于是通过此地址和端口，向A发送消息，消息中包含B映射后的公网地址和端口号，A收到消息后就知道了B的公网地址及端口，这样在A和B之间建立起了通信通道。

需要在互联网上部署专门的 STUN SERVER服务器，对于比特币区块链来说不适合。穿透技术的缺点在于无法穿透对称型NAT 。

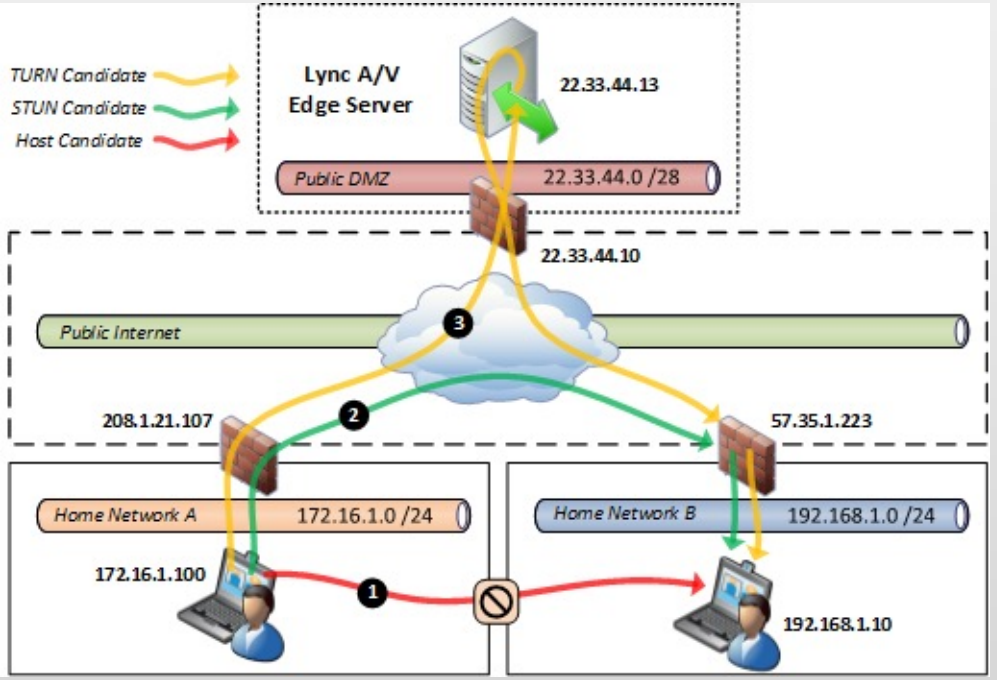
P2P网络穿越NAT的方案2：TURN（Traversal Using Relays around NAT）

TURN的工作过程和STUN非常相似，区别在于在TURN中，公网地址和端口不由NAT网关分配，而是由TURN服务器分配。TURN可以解决STUN无法穿透对称NAT的问题，但是由于所有的请求都需要经过TURN服务器，所以网络延迟和丢包的可能性较大，实际当中通常将STUN和TURN混合使用。

TURN Server也主要做了两件事：

•为NAT打洞：
如果A和B要互相通信，那么TURN Server，会命令A和B互相发一条信息，这样各自的NAT就留下了对方的洞，下次他们就可以之间进行通信了。

•为对称NAT提供消息转发：
当A或者B其中一方是对称NAT时，那么给这一方发信息，就只能通过TURN Server来转发了。



需要在互联网上部署专门的 TURN SERVER服务器，对于比特币区块链来说不适合。

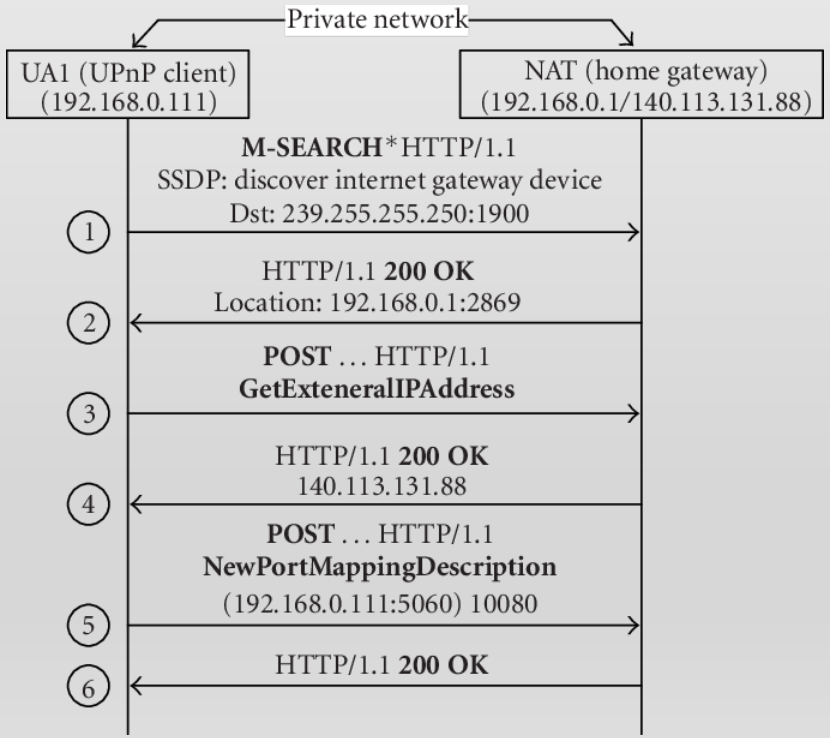
P2P网络穿越NAT的方案3： UPNP （ Universal Plug and Play ）， 比特币区块链就是用UPNP模式穿越NAT的

UPNP意为通用即插即用协议，是由微软提出的一种NAT穿透技术。使用UPNP需要内网主机、网关和应用程序都支持UPNP技术。

UPNP通过网关映射请求可以动态的为客户分配映射表项，而NAT网关只需要执行地址和端口的转换。UPNP客户端发送到公网侧的信令或者控制消息中，会包含映射之后公网IP和端口，接收端根据这些信息就可以建立起P2P连接。

直白说：
UPNP就是通过一套协议，应用程序（如：比特币钱包）自动在NAT网关创建内外网IP和端口映射。

UPNP初始化流程



UPNP主要的命令

actionName	描述
GetStatusInfo	查看UPNP设备状态
AddPortMapping	添加一个端口映射
DeletePortMapping	删除一个端口映射
GetExternalIPAddress	查看映射的外网地址
GetConnectionTypeInfo	查看连接状态
GetSpecificPortMappingEntry	查询指定的端口映射
GetGenericPortMappingEntry	查询端口映射表

UPNP在比特币P2P网络中的应用实现

区块链是建立在P2P网络基础上的。在比特币系统中，穿透NAT建立节点之间点对点的P2P网络，采用的是UPNP技术。比特币使用的是miniupnp开源软件。

比特币系统的初始化大部分都是在init.cpp中的AppInitMain中进行的。

端口映射部分：

(1) 首先第一行拿到比特币系统所使用的端口号，默认为8333，之后将要映射此端口到公网ip上；

(2) 调用upnpDiscover查找当前局域网中的所有upnp设备；

(3) 调用UPNP_GetValidIGD，从（2）中找到的upnp设备列表中找到有效的IGD设备；

(4) 如果UPNP_GetValidIGD返回1，表示有一个连接，此时调用UPNP_GetExternalIPAddress获取公网地址，然后对此公网地址进行DNS查询，将解析到的地址记录到内存中，这些公网地址之后将会被广播给P2P网络中的其他节点，一传十，十传百。

(5) 通过UPNP_AddPortMapping进行端口映射，假设内网获取的有效IGD设备的IP地址为192.168.0.1，网关出口的外网地址为192.169.1.1，采用比特币的默认端口8333，则端口映射后就是将内网中192.168.0.1：8333映射到网关出口的公有IP地址和端口：192.169.1.1:8333，之后外部节点通过此公网IP和端口，就可以与内网节点进行通信了。

UPNP在比特币P2P网络中的应用实现

在init.cpp中的AppInitMain中。

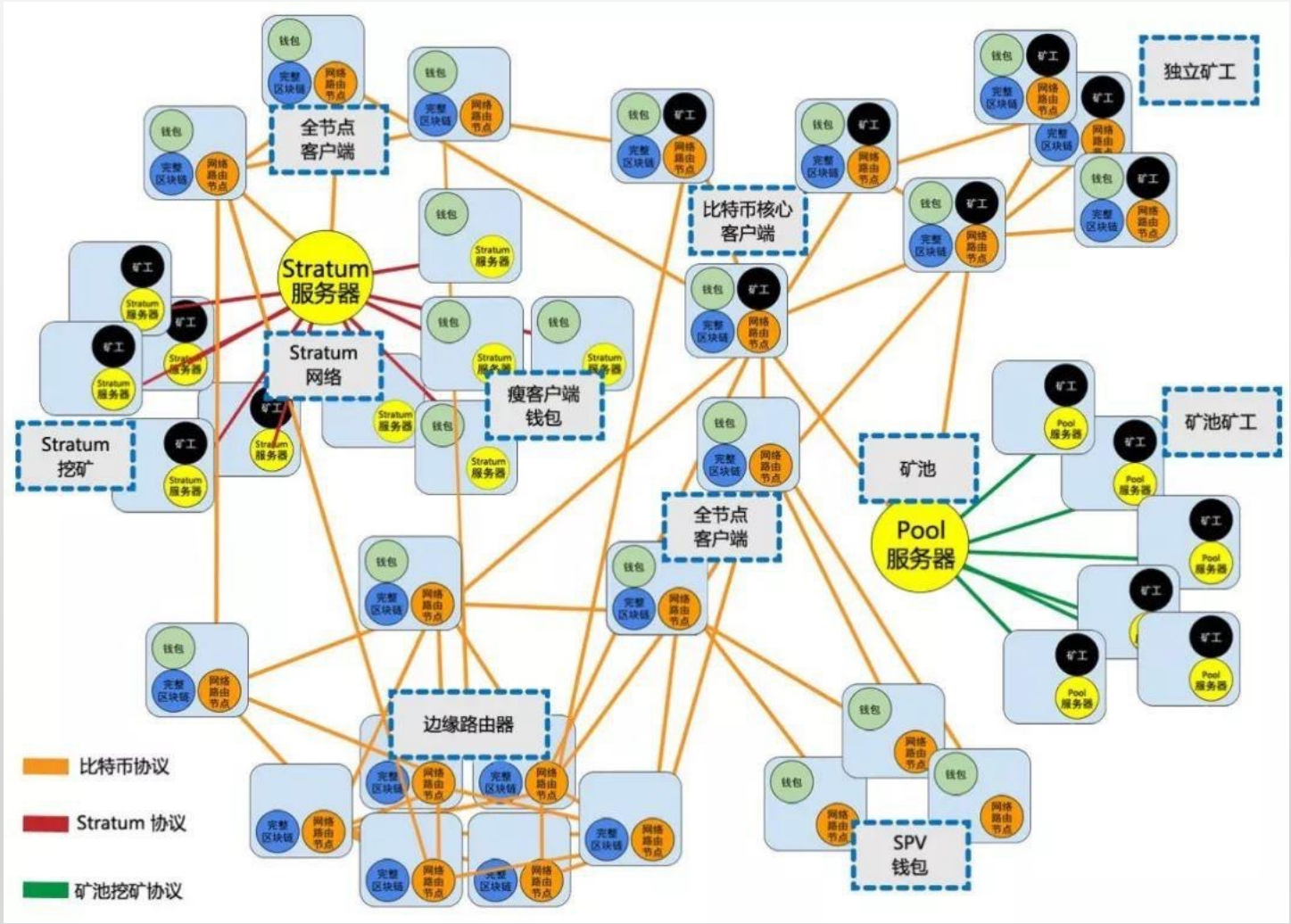
```
    // init.cpp line1901  Map ports with UPnP
    if (args.GetBoolArg("-upnp", DEFAULT_UPNP)) {
        StartMapPort();
    }
```

源代码：
https://codechina.csdn.net/mirrors/bitcoin/bitcoin?utm_source=csdn_github_accelerator

```
// net.cpp
#ifdef USE_UPNP
#include <miniupnpc/miniupnpc.h>
#include <miniupnpc/upnpcommands.h>
#include <miniupnpc/upnperrors.h>
// The minimum supported miniUPnPc API version is set to 10. This keeps compatibility
// with Ubuntu 16.04 LTS and Debian 8 libminiupnpc-dev packages.
static_assert(MINIUPNPC_API_VERSION >= 10, "miniUPnPc API version >= 10 assumed");
#endif
```

```
// net.cpp line1628
void StartMapPort()
{
   if (!g_upnp_thread.joinable()) {
      assert(!g_upnp_interrupt);
      g_upnp_thread = std::thread((std::bind(&TraceThread<void (*)()>, "upnp", &ThreadMapPort)));
   }
}
```

回顾：比特币区块链盘P2P网络



煤油灯科技
VICTORLAMP

谢 谢!

VICTORLAMP

Shenzhen VictorLamp Technologies CO. Ltd.
http://www.victorlamp.com

多媒体课程：《深入浅出区块链技术基础篇》

深入浅出区块链技术