**区块链：比特币中的P2P网络**

**小组成员：黄刚、谈玉胜、龙祖涛**

**摘要：**P2P网络优势在于:去中心化, 可基于全部节点, 实现区块链资源及服务的均衡分布, 并利用共识机制, 为区块链一致性提供保障;可拓展性, 区块链节点可以自由增加并减少, 实现网络系统的拓展;健壮性, 缺乏中心节点的情况下, 对区块链的攻击对象不明确, 即使某些节点被破坏, 区块链的安全性也不会受到太大的影响, 因而可加强区块链与P2P网络的相互结合。

**关键词：**区块链; P2P网络; 比特币;

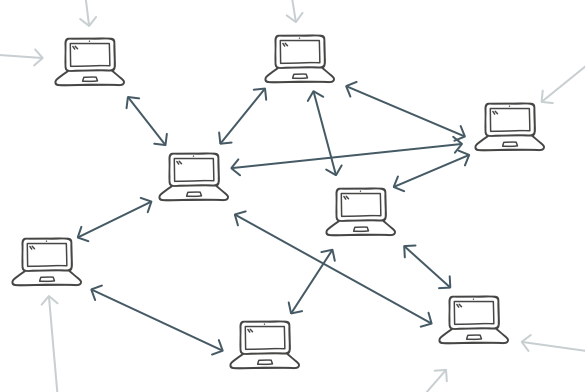
1. **引言**

在传统客户机/服务器网络中，服务器是网络的核心，而客户机是网络的基础，客户机依靠服务器获得所需要的网络资源，而服务器为客户机提供网络必须的资源。客户服务器模式，需要专人维护、管理服务器，增加费用。P2P 网络中的每个节点都可以既是客户端也是服务端，在区块链的应用中，区块链的资源和服务分布在所有参与节点上,利用P2P网络去中心化特点，通过共识机制维护区块链网络的一致性,无须中心系统的存在。

**2.项目技术背景分析**

区块链网络是去中心化的，这意味着没有服务器，客户端也不需要依赖服务器来获取或处理数据。在区块链网络中，有的是节点，每个节点是网络的一个完全（full-fledged）成员。节点就是一切：它既是一个客户端，也是一个服务器。这一点需要牢记于心，因为这与传统的网页应用非常不同。

区块链网络是一个 P2P（Peer-to-Peer，端到端）的网络，即节点直接连接到其他节点。它的拓扑是扁平的，因为在节点的世界中没有层级之分。下面是它的示意图：



要实现这样一个网络节点更加困难，因为它们必须执行很多操作。每个节点必须与很多其他节点进行交互，它必须请求其他节点的状态，与自己的状态进行比较，当状态过时时进行更新。

**2.1 P2P在区块链的应用**

P2P网络自身有多方面优点,在区块链的应用如下:a)去中心化,区块链的资源和服务分布在所有参与节点上,通过共识机制维护区块链网络的一致性,无须中心系统的存在;b)可扩展性;c)健壮性,区块链网络没有中心节点,也就没有了攻击对象,参与节点分布在网络中,部分节点遭到破坏对区块链系统无影响;d)高性价比,不需要昂贵的专业设备搭建中央服务器、不需要支付昂贵的宽带费用,普通用户也可以参与区块链;e)隐私保护,区块信息采用广播机制,无法定位广播初始节点,防止用户通信被监听,保护用户隐私;f)负载均衡,区块链通过限制节点连接数等配置,来避免资源负载、网络阻塞。

**2.2 P2P网络类型**

**2.2.1集中式P2P网络**

中心化P2P网络十分依赖中心服务器, 并将接入节点地址数据作为网络核心。区块链技术环境下, 普通网络节点与中心服务器相连, 掌握节点地址, 以便于进行节点通讯。Napster作为世界知名MP3共享软件, 所采用的网络结构就是中心化P2P网络, 通过该网络, 实现音乐文件与保存文件的相互关联, 用户可通过在对某文件进行查找时了解到的节点存储位置,实现点对点的连接, 获取该MP3文件的共享。中心服务器的应用, 可对网络稳定性造成决定性影响, 若中心服务器存在问题, 则P2P网络会瘫痪, P2P网络中心向用户提供索引与节点通信。

**2.2.2 全分布、非结构P2P网络**

该网络结构下, P2P网络节点具备较大自由性, 不存在中心节点的限制, 以及同一的结构化标准, 以随机图的形式提供网络服务。该网络结构中, Gnutella协议较为知名, 该协议是一种点对点的搜索系统, 通过洪泛技术发现节点并转发节点, 通过TTL减值以有效控制传播次数。但同时, 过于自由的网络机制, 会导致P2P网络信息难以被新的入网节点所掌握, 影响节点入网, 同时导致网络结构的稳定性受到影响, 资源大量被无端消耗, 并造成网络阻塞。

**2.2.3 全分布、结构化P2P网络**

该结构的应用中, 节点地址管理是其中较为严重的问题, 节点之间缺少规则限制的情况下, 节点信息难以精准定位, 需要进行查找, 造成网络消耗。而全分布、结构化P2P网络, 采用哈希表, 以加密散列函数, 对节点地址数据加以规范, 该方式应用并不存在固定的网络结构, 但需要基于固定的结构图进行网络节点管理。为此, 以太坊采用节点椭圆加密转换的方式实现节点区分, 精准定位节点地址。

**2.2.4 半分布式P2P网络**

该网络结构兼具中心化及分布式两种结构的优势, 划分网络节点, 打造半分布式网络结构, 由超级节点对网络节点地址加以维护, 以保证中心服务器的功能性得以凸显。超级节点为分布式节点, 具备入网及退出的自由性。其中具有代表性的应用为Kazza。半分布式结构将节点划分为普通节点及超级节点, 超级节点的确定可基于普通节点, 或可自行单独配置。

**2.3 比特币及P2P网络**

比特币开启了区块链时代,任何节点开启客户端后即可实现去中心化可信任的比特币交易。然而当一个全新的节点加入比特币网络时,首先要做的是接入网络。由于比特币完全去中心化,节点自由加入、退出导致新加入的节点无从获取网络中节点地址从而接入网络。为此,比特币设计三种节点发现方式:

**种子节点。**种子节点为具备长期稳定性的网络节点, 将其编写至代码中, 初步启动种子节点, 即可向入网节点提供节点地址。从而保证新节点与其他节点的相互连接, 并获取相依的地址列表。

**地址广播。**该技术的应用, 是以某网络节点作为中介与桥梁, 通过该节点获取其他节点地址, 该技术的具体应用, 包括主动广播及主动获取两种方式。

**建立地址数据库。**该技术的应用, 是出于避免种子节点连接站及带宽限制, 对地址广播中的节点地址信息加以保存, 形成数据库,若两个已建立连接的节点之间, 一段时间内未有数据通信, 则一个节点向另一节点发送信息, 接收信息的节点回复响应报文, 以维持连接。

比特币通过以上三种方式保持稳定的网络接入,实现对频繁进出节点的地址列表维护,不需要中心机构的存在即可保持节点可以自由加入网络,从而保障比特币P2P网络稳定。

**3.实现比特币P2P网络**

**3.1比特币节点**

尽管节点具有完备成熟的属性，但是它们也可以在网络中扮演不同角色。比如：

3.1.1 **矿工，**这样的节点运行于强大或专用的硬件（比如 ASIC）之上，它们唯一的目标是，尽可能快地挖出新块。矿工是区块链中唯一可能会用到工作量证明的角色，因为挖矿实际上意味着解决 PoW 难题。在权益证明 PoS 的区块链中，没有挖矿。

3.1.2 **全节点，**这些节点验证矿工挖出来的块的有效性，并对交易进行确认。为此，他们必须拥有区块链的完整拷贝。同时，全节点执行路由操作，帮助其他节点发现彼此。对于网络来说，非常重要的一段就是要有足够多的全节点。因为正是这些节点执行了决策功能：他们决定了一个块或一笔交易的有效性。

3.1.3 **SPV，**SPV表示Simplified Payment Verification，简单支付验证。这些节点并不存储整个区块链副本，但是仍然能够对交易进行验证（不过不是验证全部交易，而是一个交易子集，比如，发送到某个指定地址的交易）。一个 SPV 节点依赖一个全节点来获取数据，可能有多个 SPV 节点连接到一个全节点。SPV 使得钱包应用成为可能：一个人不需要下载整个区块链，但是仍能够验证他的交易。

**3.2比特币网络**

为了在目前的区块链原型中实现网络，我们不得不简化一些事情。因为我们没有那么多的计算机来模拟一个多节点的网络。当然，我们可以使用虚拟机或是 Docker 来解决这个问题，但是这会使一切都变得更复杂：你将不得不先解决可能出现的虚拟机或 Docker 问题，而我的目标是将全部精力都放在区块链实现上。所以，我们想要在一台机器上运行多个区块链节点，同时希望它们有不同的地址。为了实现这一点，我们将使用端口号作为节点标识符，而不是使用 IP 地址，比如将会有这样地址的节点：127.0.0.1:3000，127.0.0.1:3001，127.0.0.1:3002 等等。我们叫它端口节点（port node） ID，并使用环境变量 NODE\_ID 对它们进行设置。故而，你可以打开多个终端窗口，设置不同的 NODE\_ID 运行不同的节点。

这个方法也需要有不同的区块链和钱包文件。它们现在必须依赖于节点 ID 进行命名，比如 blockchain\_3000.db, blockchain\_3001.db , wallet\_3000.db, wallet\_30001.db 等等。

在 Bitcoin Core 中硬编码一个地址，已经被证实是一个错误：因为节点可能会被攻击或关机，这会导致新的节点无法加入到网络中。在 Bitcoin Core 中，硬编码了 [DNS seeds](https://bitcoin.org/en/glossary/dns-seed)。虽然这些并不是节点，但是 DNS 服务器知道一些节点的地址。当你启动一个全新的 Bitcoin Core 时，它会连接到一个种子节点，获取全节点列表，随后从这些节点中下载区块链。

不过在我们目前的实现中，无法做到完全的去中心化，因为会出现中心化的特点。我们会有三个节点：

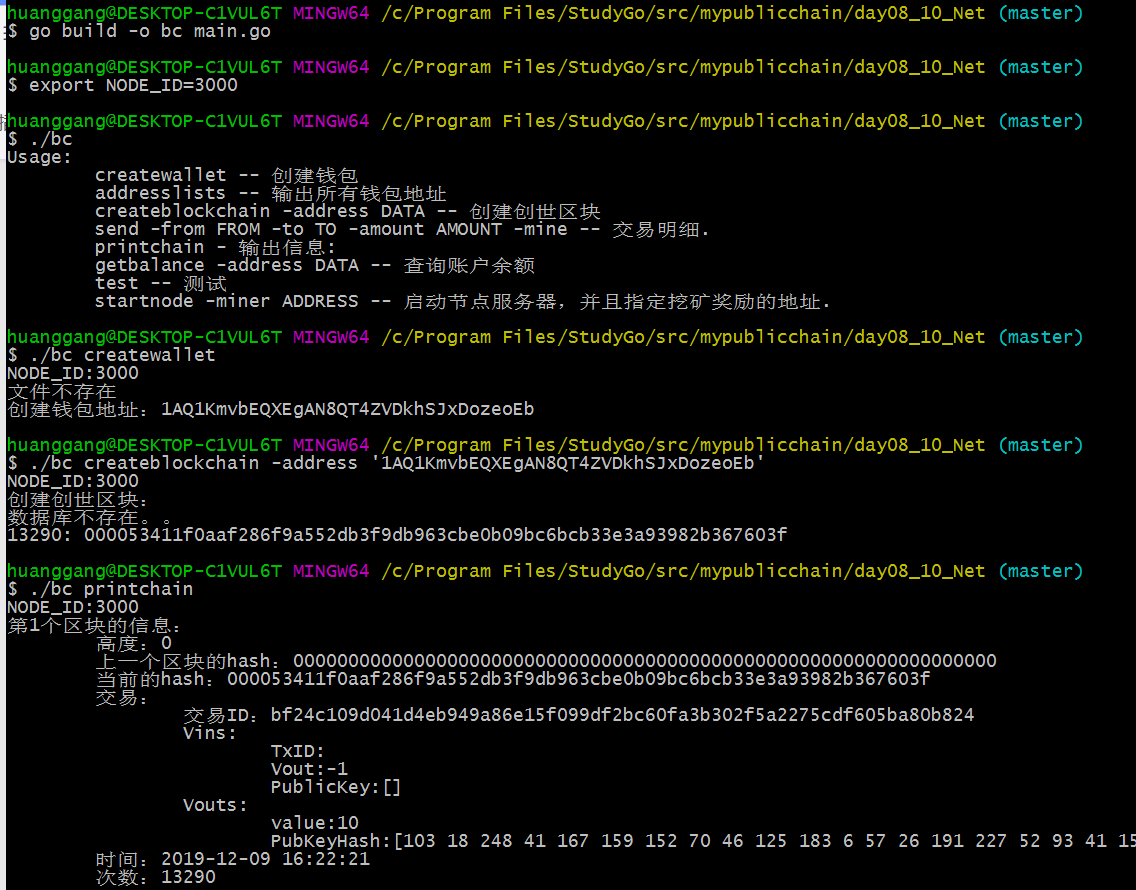
一个中心节点。所有其他节点都会连接到这个节点，这个节点会在其他节点之间发送数据。

一个矿工节点。这个节点会在内存池中存储新的交易，当有足够的交易时，它就会打包挖出一个新块。

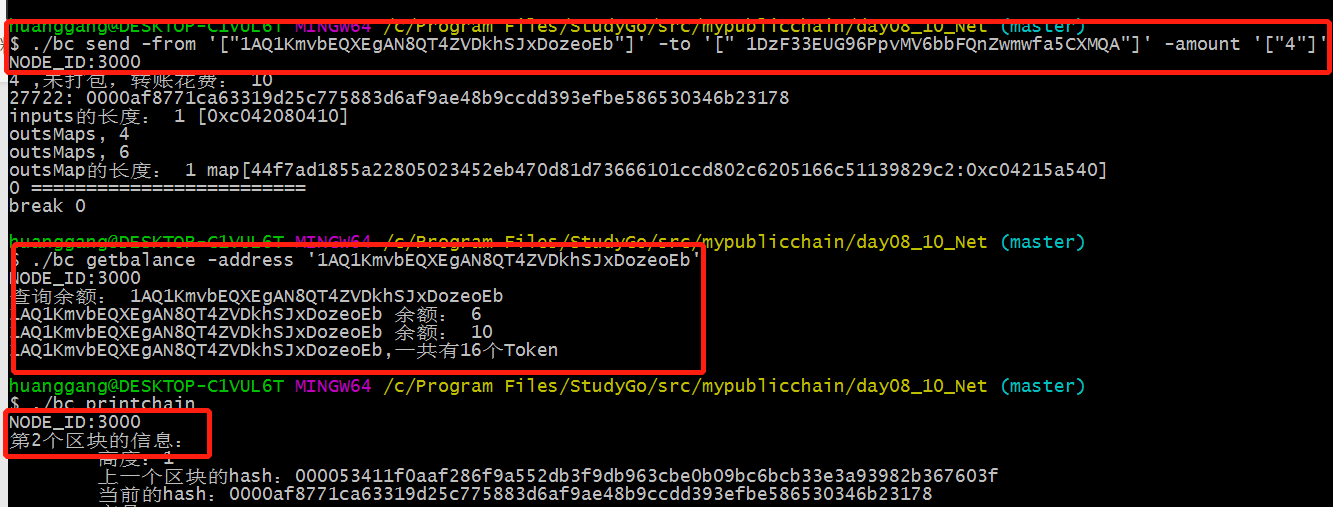
一个钱包节点。这个节点会被用作在钱包之间发送币。但是与 SPV 节点不同，它存储了区块链的一个完整副本。

**3.3 p2p网络的实现**

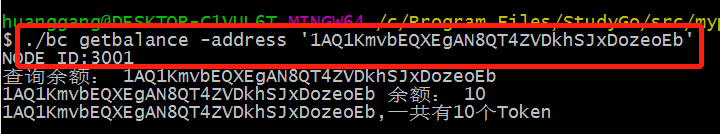
（1）中心节点创建一个区块链。设置NODE\_ID:3000为中心节点，并创建第一个创世区块。会生成一个仅包含创世块的区块链。我们需要保存块，并在其他节点使用。创世块承担了一条链标识符的角色（在 Bitcoin Core 中，创世块是硬编码的），所以我们备份了创世区块。



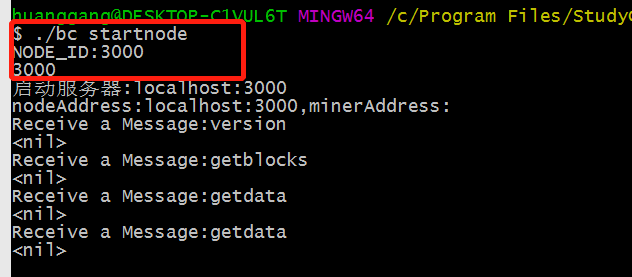
（2）一个其他（钱包）节点连接到中心节点并下载区块链。创建节点NODE\_ID=3001，主节点3000向钱包地址发送一些币，并查询钱包地址余额，打印区块。



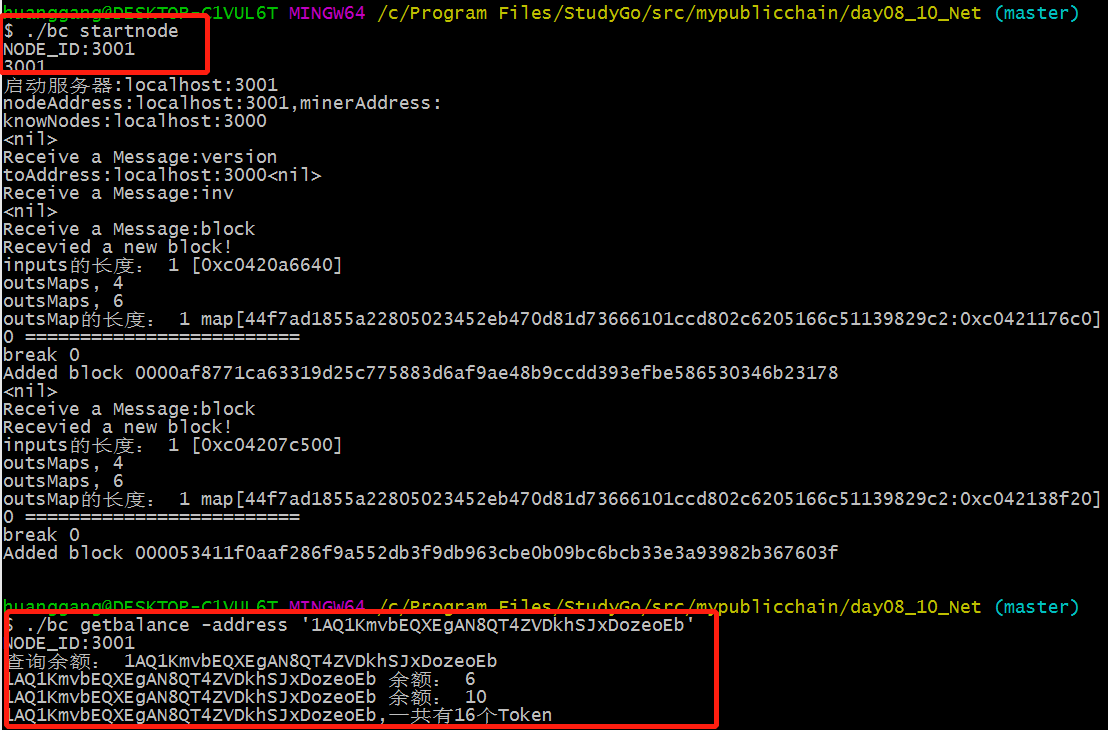
切换节点3001，查询主节点钱包的余额。



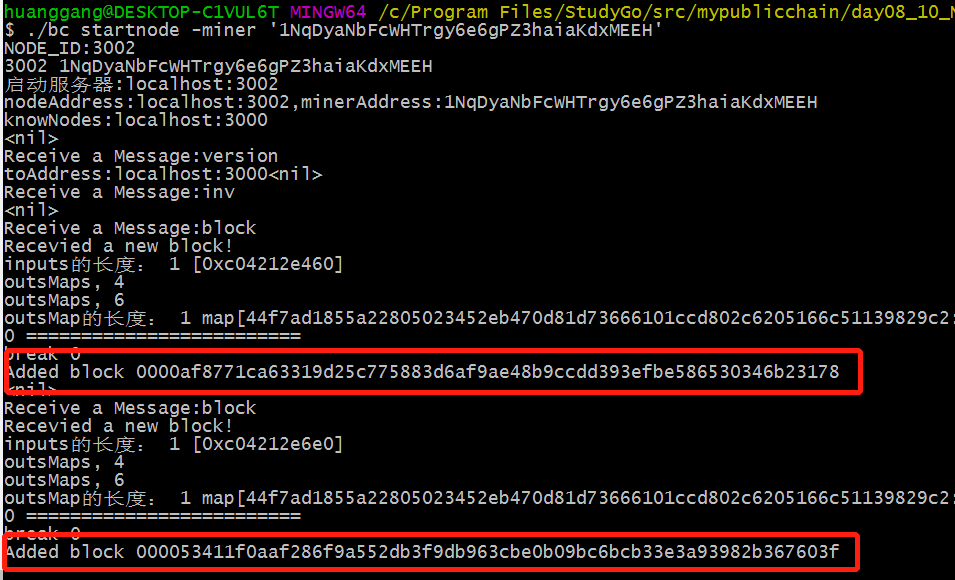
我们发现钱包节点的查询到的余额和主节点中的数据不一致，接下来我们启动节点进行数据同步，切换到主节点终端，启动启动主节点后等待钱包节点链接，如果有钱包节点链接，那么就会有消息传递，进行数据同步。



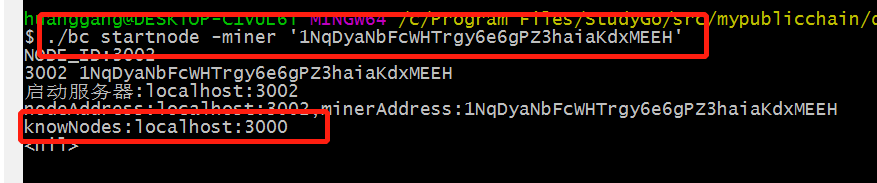
切换到节点3001进行数据同步，并查询钱包节点余额。

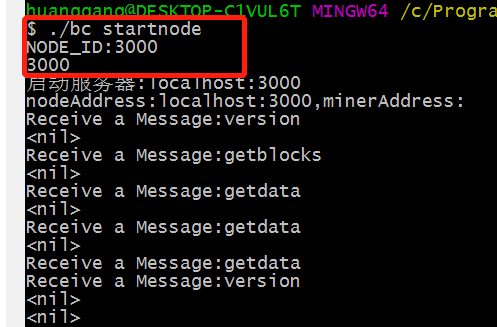


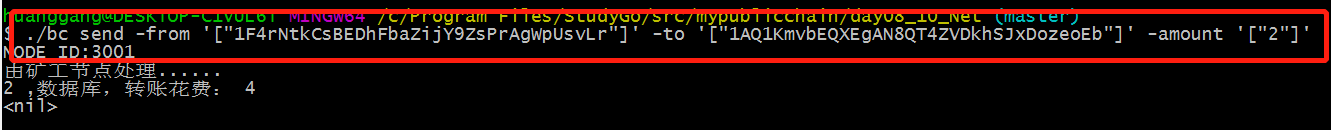
1. 另一个（矿工）节点连接到中心节点并下载区块链。启动矿工节点会先同步主节点的数据。



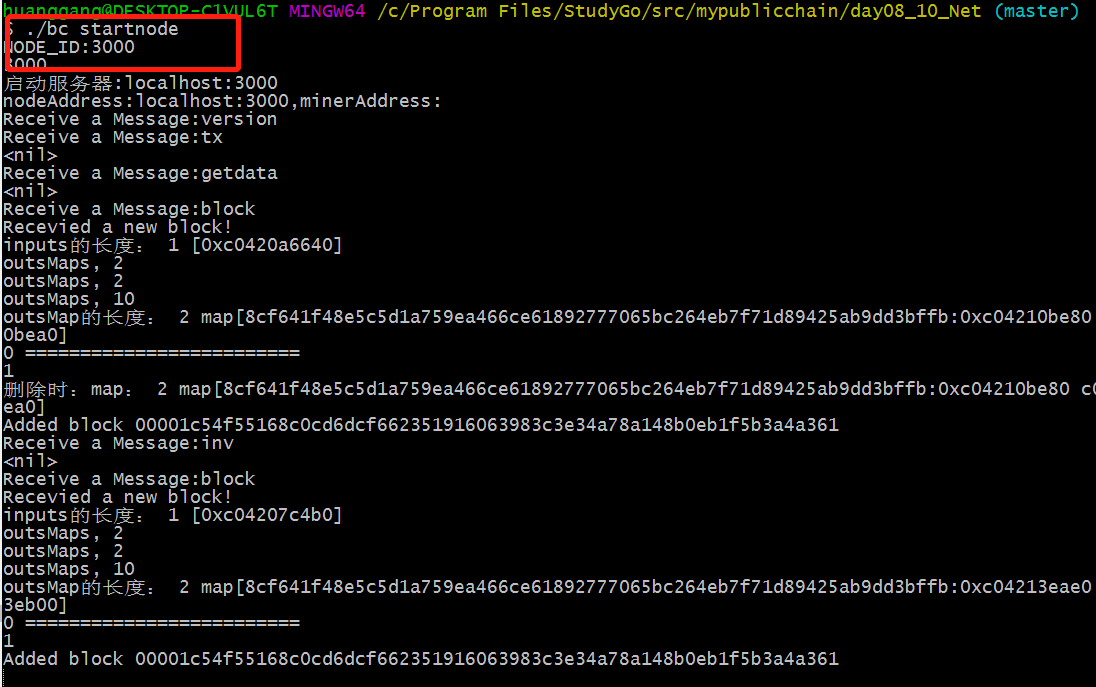
1. 钱包节点创建一笔交易。这时挖矿节点与主节点得先启动。



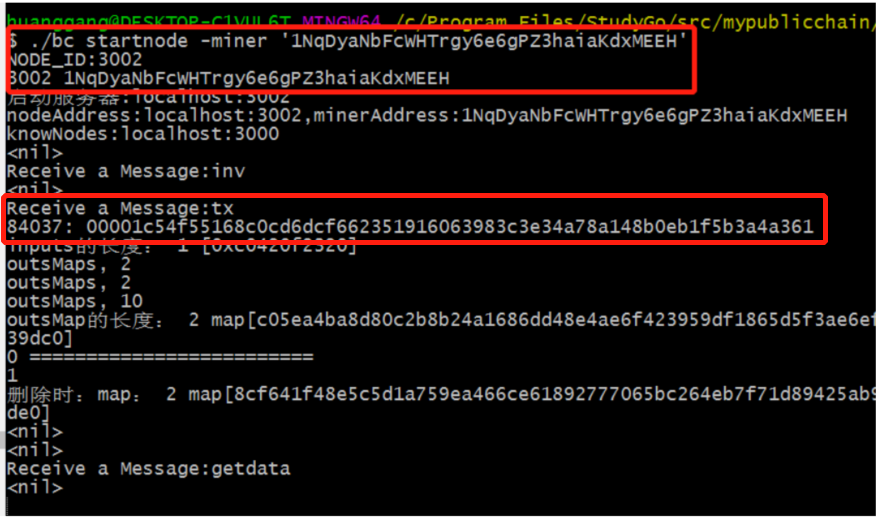




1. 矿工节点接收交易，并将交易保存到内存池中。当内存池中有足够的交易时，矿工开始挖一个新块。当挖出一个新块后，将其发送到中心节点。钱包节点与中心节点进行同步。钱包节点的用户检查他们的支付是否成功。



矿工节点确认交易，形成一个新的区块。



这就是比特币中的一般流程。尽管我们不会实现一个真实的 P2P 网络，但是我们会实现一个真实，也是比特币最常见最重要的用户场景。

**4.总结**

我们实现了简易版的网络，能够同步节点之间的数据消息，尽管这个过程比较复杂。我们已经尽可能的简化了，仅仅是通过端口来模拟不同的节点。实现了主节点，钱包节点和矿工节点之间的数据传递。

参考文献：

[1]S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf.

[2]M. Spagnuolo, F. Maggi, and S. Zanero, “BitIodine: Extracting Intelligence from the Bitcoin Network,” in Proc. Financial Cryptography, vol.8437 of LNCS, pp. 457–468, 2014.

[3]Cryptocurrency Networks: A New P2P Paradigm.Sergi Delgado Segura , Cristina Pereze Sola, Jordi Herrera Joancomartı, Guillermo Navarro Arribas , and Joan Borrell.2018

[4]王学龙,张璟. P2P关键技术研究综述[J].计算机应用研究,2010,27(3):801-805,823.