stratum协议是目前最常用的矿机和矿池之间的TCP通讯协议。先简要说明挖矿的网络架构。

## 一、挖矿的网络架构

比特币是一个去中心化的网络架构，通过安装比特币守护程序的节点来转发新交易和新区块。而矿机、矿池也同时形成了另一个网络，我们称之为矿工网络。

矿工网络分成矿机、矿池、钱包等几个主要部分，有时矿池软件与钱包安装在一起，可合称为矿池。

矿机与矿池软件之间的通讯协议是stratum，而矿池软件与钱包之间的通讯是bitcoinrpc接口。

stratum是JSON为数据格式，具体协议如下：

## 二、stratum协议

#### 1、任务订阅

矿机启动，首先以mining.subscribe方法向矿池连接，用来订阅工作。

矿池以mining.notify返回订阅号、ExtraNonce1和ExtraNonce2\_size。

Client:{"id":1,"method":"mining.subscribe","params":[]}

Server:{"id":1,"result":[["mining.notify","ae6812eb4cd7735a302a8a9dd95cf71f"],"08000002",4],"error":null}

其中：

ae6812eb4cd7735a302a8a9dd95cf71f是订阅号；

08000002是ExtraNonce1，用于构建coibase交易；

ExtraNonce2\_size为4，矿机ExtraNonce2计数器的字节数。

#### 2、任务分配

该命令由矿池定期发给矿机，当矿机以mining.subscribe方法登记后，矿池应该马上以mining.notify返回该任务。

Server:{"params":["bf","4d16b6f85af6e2198f44ae2a6de67f78487ae5611b77c6c0440b921e00000000", "010000000100000000000000000000000000000000000000000000000000000000000000 00ffffffff20020862062f503253482f04b8864e5008", "072f736c7573682f000000000100f2052a010000001976a914d23fcdf86f7e756a64a7a9688ef9903327048ed988ac00000000",["c5bd77249e27c2d3a3602dd35c3364a7983900b64a34644d03b930bfdb19c0e5", "049b4e78e2d0b24f7c6a2856aa7b41811ed961ee52ae75527df9e80043fd2f12"], "00000002","1c2ac4af","504e86b9",false],"id":null,"method":"mining.notify"}

其中：

任务号：”bf”；

前个区块HASH：

"4d16b6f85af6e2198f44ae2a6de67f78487ae5611b77c6c0440b921e00000000"；

coinbase第一部分：

"010000000100000000000000000000000000000000000000000000000 00000000000000000ffffffff20020862062f503253482f04b8864e5008"；

coinbase第二部分：

"072f736c7573682f000000000100f2052a010000001976a914d23fcdf86f7 e756a64a7a9688ef9903327048ed988ac00000000"；

交易ID列表：

["c5bd77249e27c2d3a3602dd35c3364a7983900b64a34644d03b930bfdb19c0e5", "049b4e78e2d0b24f7c6a2856aa7b41811ed961ee52ae75527df9e80043fd2f12"]；

区块版本号：”00000002″；

nBit:”1c2ac4af”；

当前时间：”504e86b9″；

清理任务：如果为true,则矿机中止所有任务，马上开始新任务；如果是false则等当前任务结束才开始新任务。

#### 3、矿机登录

矿机以mining.authorize方法，用某个帐号和密码登录到矿池，密码可空，矿池返回true登录成功。该方法必须是在初始化连接之后马上进行，否则矿机得不到矿池任务。

Client:{"params":["miner1","password"],"id":2,"method":"mining.authorize"}

Server:{"error":null,"id":2,"result":true}

#### 4、结果提交

矿机找到合法share时，就以”mining.submit“方法向矿池提交任务。矿池返回true即提交成功，如果失败则error中有具体原因。

Client:{"params":["miner1","bf","00000001","504e86ed","b2957c02"],"id":4,"method":"mining.submit"}

Server:{"error":null,"id":4,"result":true}

其中：

用户名：”miner1″；

任务号：”bf”；

ExtraNonce2：”00000001″；

当前时间：”504e86ed”；

nonce:”b2957c02″；

#### 5、难度调整

难度调整由矿池下发给矿机，以mining.set\_difficulty方法调整难度，params中是难度值。

Server:{"id":null,"method":"mining.set\_difficulty","params":[2]}

矿机会在下一个任务时采用新难度，矿池有时会马上下发一个新任务并且把清理任务设为true，以便矿机马上以新难度工作。

## 三、一般通讯过程

一般的矿机与矿池通讯过程就如下所示：

