

## 区块来源

区块的来源有三个：网络，命令产生，文件导入

区块的处理：从区块来源中接收到一个区块，最终都会进入block的处理流程

### POS命令产生：

首先bitcoin收到rpc命令创建一个pos区块，首先判断钱包是否被锁，然后判断钱包中是否存在有可用的utxo,然后创建一个空的block，然后进入signblock,将block修改为posblock

这一步主要作用的创建空的coinbase，和coinstake，填充区块头的其他信息，添加交易池中的交易。然后再一次signblock，signblock后检测block的prev和时间，如果这些都通过了，进入checkstae，这一步主要是再一次检测当前生成的posblock的合法性，主要验证，coinstake的交易是否被花费，深度是否大于500，block时间，计算的kernalhash是否合法，block的签名。然后再进入processnewblock。

备注：signblock功能

找出所有utxo交易，放入coinstake的交易

从所有utxo交易中，找出一笔交易能够通过checkkernalhash检查，并将这笔交易放入coinstake的第一笔输入中，并将该笔交易的公钥作为coinstake交易的公钥。

将coinsate创建时间作为block的创建时间

然后使用第一笔交易对应的私钥对block的hash进行签名，将签名放入block中

### POS命令产生：

首先bitcoin收到rpc命令创建一个pos区块，首先判断钱包是否被锁,创建powblock，主要是创建coinbase交易，签名coinbase，填充区块头，添加交易，然后进入CheckProofOfWork，如果hash小于网络难度值那么需要迭代nonce再次验证CheckProofOfWork直到有合法的block 进入processnewblock

### 网络：

根据bitcoin协议当从网络收到Blocks类型消息时，在messagehandle中会调用processmessge，然后调用processnewblock函数，这样就进入了block的验证流程