

## 5.3 Endorser、Committer与分布式背书策略

- Hyperledger Fabric是一个提供分布式账本解决方案的平台，它由模块化架构支撑，并具备极佳的保密性、伸缩性、灵活性和扩展性。
- Hyperledger Fabric被设计成支持不同的模块组件直接拔插启用，并能适应经济生态系统中错综复杂的各种场景。
- 区块链是一个分布式系统，由许多相互通信的节点组成。区块链运行的程序称为Chaincode，保存状态和账本数据、执行交易。Chaincode是核心要素，交易操作在Chaincode上调用。
- 在进行Chaincode invoke调用时，会产生一笔交易的proposal，然后执行模块化的流程（背书、共识、验证、提交）。**交易必须被“背书”，只有经过背书的交易才可以提交，并对状态产生影响。背书、提交就是由Endorser与Committer来完成的。**

### 什么是背书者？

背书是指一个peer执行一个交易并返回YES-NO给生成交易proposal的client app 的过程。那么执行背书操作的Peer节点就是背书者(Endorser)。chaincode具有相应的背书，其中指定了背书节点。

### 什么是提交者？

一个通道中的每个peer节点都会验证交易的有序区块，然后将区块提交（写或追加）到该通道上账本的各个副本。peer节点也会标记每个区块中的每笔交易的状态是有效或者无效。那么对区块进行存储并标记交易有效性的peer节点即为提交者(Committer)。

## 什么是背书策略？

背书策略用于指示区块链节点交易验证的规则，定义了依赖特定chaincode执行交易的channel上的peer和响应结果（endorsements）的必要组合条件（即返回Yes或No的条件）。背书策略可指定对于某一chaincode，对交易进行背书的最小背书节点数或者最小背书节点百分比。背书策略由背书节点基于应用程序和对抵御不良行为的期望水平来组织管理。在安装和实例化Chaincode（deploy tx）时需要指定背书策略。

所以，在Fabric中，节点是通过背书策略来确定一个交易是否被正确背书的。不同的智能合约可根据业务需求设置不同的背书策略。

在Hyperledger Fabric的大框架中，有众多的参与节点，每种节点都有自己的分工任务，比如说：

- ✓ Ca节点进行证书颁发
- ✓ Peer节点进行模拟交易的执行以及区块的落账
- ✓ Orderer节点对模拟交易进行排序并形成区块进行派发
- ✓ Kafka节点和Zookeeper节点构成了一套基本的消息队列网络，提供给Orderer节点网络进行消息的传达。

**背书者和提交者的概念也不是绝对的，哪个Peer节点进行了背书操作，它就可以被称为背书者。哪个节点进行了区块落账提交操作，它就可以被称为提交者。然而并不是所有的Peer节点都是背书者或提交者。**

**第一步，客户端创建交易，并发送给它选择的背书节点调用交易。**

客户端发送一个PROPOSE消息到它选择的一组背书节点。给定chaincodeID的背书节点的设置由客户端通过peer节点实现，从背书策略就可以知道背书peer节点的设置。例如，交易能被发送给所有给定chaincodeID的背书者，那也就是说，一些背书者能够离线，其它人可能反对，也可能不为交易背书，客户端选择满足背书策略的方式表达。

## 第二步，背书节点模拟交易和产生背书签名

客户端（SDK）把交易提议（TX Proposal）发给指定的一个或多个背书节点(endorsing peer)。接收提议的背书节点在SDK的交易提议请求中指定，最终进行背书的节点由交易所属的ChainCode和该Chaincode所定义的背书策略（Endorsement Policy）共同决定。背书节点收到交易提议后，首先用客户端（SDK）的公钥验证它的签名、客户端是否可以在该channel进行操作、交易是否已被提交、交易提议组织是否正确。验证通过后模拟执行chaincode（不会将结果写入到账本里），将执行的结果反馈给客户端。注意背书者在这一步不能改变账本。

## 第三步，提交客户端收集的交易背书并通过排序服务广播它

客户端一直等待直到它收集到“足够”的消息和签名来推断出交易提案已背书。对于一个具有有效背书的交易，客户端会发送给排序服务。



#### 第四步，排序服务向peer节点提交交易

当一个区块事件发生并且一个peer节点已经为所有序列号低于seqno的区块更新状态，peer节点执行如下流程：

- 它检查背书是否是有效的。
- 检查读写集合是否是有效的。

经过上面4步，一笔交易的背书和提交就完成了。