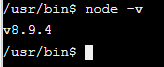
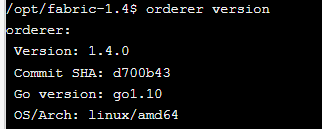
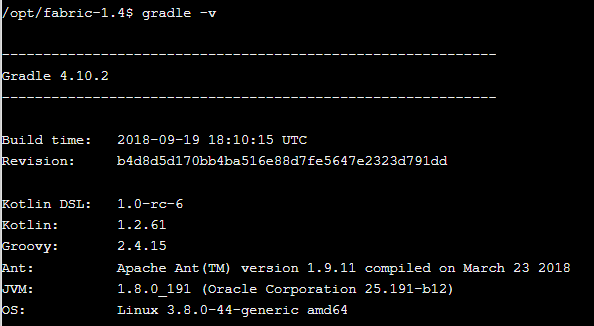
## 快速上手Fabric区块链开发

* 了解PKI和X509证书
* 使用OpenSSL建立最小CA
* 构造最简Fabric网络
* 开发计数器链码
* 开发去中心化计数器应用。

## 各种环境版本

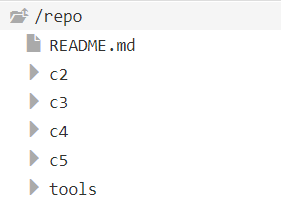
 





### 代码目录结构：

/home/user/repo



#### README.md内容

# Fabric区块链Java开发详解

本课程适合Java开发人员快速掌握超级账本Fabric区块链的设计思路、

核心概念、网络搭建、链码开发、应用开发等方面的知识和技能。

## 一、预置代码

- ~/repo/c2：第二章预置代码

- ~/repo/c3：第三章预置代码

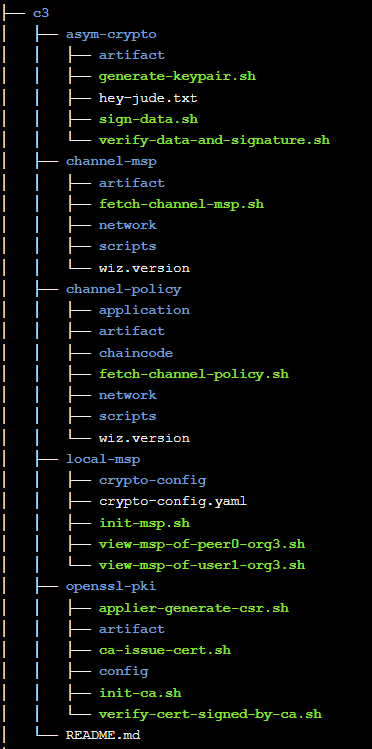
- ~/repo/c4：第四章预置代码

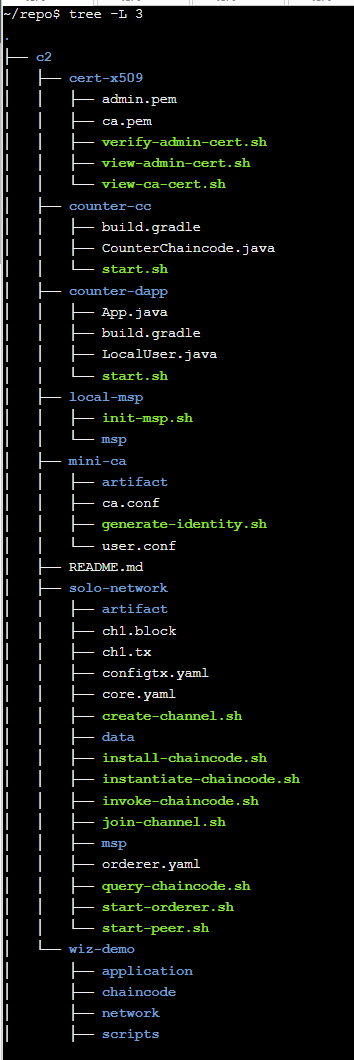
- ~/repo/c5：第五章预置代码

## 二、开发工具箱

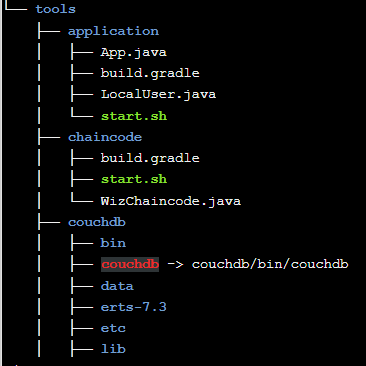
代码目录：~/repo/tools

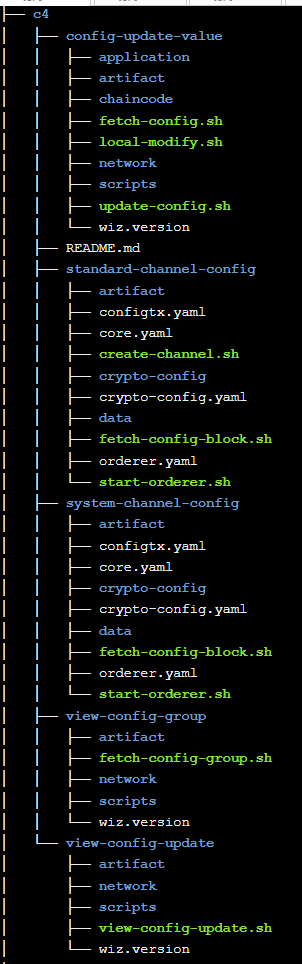
#### 详细目录结构（只截取了3级目录）

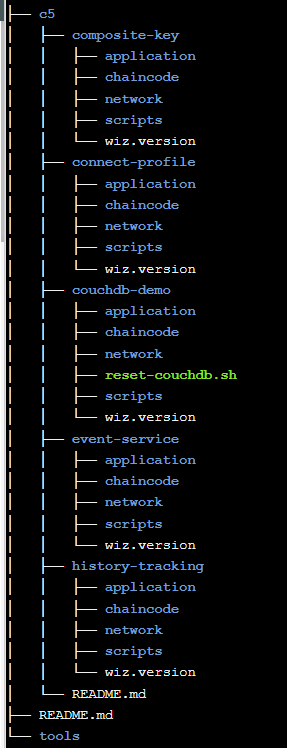




|--- wiz.version







### 使用预置代码

#### 1、查验X509证书

在1#终端进入项目目录：

~$ cd ~/repo/c2/cert-x509

查看CA根证书和Admin用户证书：

~/repo/c2/cert-x509$ ./view-ca-cert.sh

~/repo/c2/cert-x509$ ./view-admin-cert.sh

验证Admin证书是否由CA签发：

~/repo/c2/cert-x509$ ./verify-admin-cert.sh

#### 2、发行X509证书

使用openssl建立一个CA，并发行用于Fabric网络的X509V3证书。

在终端1#执行如下命令：

~$ cd ~/repo/c2/mini-ca

~/repo/c2/mini-ca$ ./generate-identity

查看artifact目录下生成的证书：

~/repo/c2/mini-ca$ ls artifact/\*-cert.pem

#### 3、组织本地MSP目录

在1#终端进入项目目录，执行脚本初始化本地MSP目录：

~$ cd ~/repo/c2/local-msp

~/repo/c2/local-msp$ ./init-msp.sh

查看本地msp目录的结构和内容：

~/repo/c2/local-msp$ tree msp

#### 4、启动最小Fabric网络

##### 4.1 启动排序节点

在1#终端进入项目目录,启动Fabric排序节点：

~$ cd ~/repo/c2/solo-network

~/repo/c2/solo-network$ ./start-orderer.sh

##### 4.2 启动对等节点

在2#终端进入项目目录，启动Fabric对等节点：

~$ cd ~/repo/c2/solo-network

~/repo/c2/solo-network$ ./start-peer.sh

##### 4.3 创建通道

在3#终端进入项目目录，创建通道ch1：

~$ cd ~/repo/c2/solo-network

~/repo/c2/solo-network$ ./create-channel.sh

然后将当前对等节点加入通道：

~/repo/c2/solo-network$ ./join-channel.sh

##### 4.4 启动Fabric链码

在4#终端进入项目目录，启动链码：

~$ cd ~/repo/c2/counter-cc

~/repo/c2/counter-cc$ ./start.sh

##### 4.5 在Fabric通道安装并激活链码

在3#终端执行如下命令安装并激活counter-cc链码：

~/repo/c2/solo-network$ ./install-chaincode.sh

~/repo/c2/solo-network$ ./instantiate-chaincode.sh

##### 4.6 测试链码调用

在3#终端的网管环境内执行如下命令查询链码：

~/repo/c2/solo-network$ ./query-chaincode.sh

使用如下命令提交计数器增长交易：

~/repo/c2/solo-network$ ./invoke-chaincode.sh

#### 5、运行Fabric应用

在5#终端进入项目目录，启动应用并观察其输出：

~$ cd ~/repo/ch2/counter-dapp

~/repo/ch2/counter-dapp$ ./start.sh

#### 6、使用WIZ工具箱

在1#终端进入项目目录，启动网络：

~/repo/c2/wiz-demo$ wiz net reset && wiz net start

在2#终端进入项目目录，启动链码：

~/repo/c2/wiz-demo$ wiz cc start

在3#终端进入项目目录，启动通道环境，然后进入管理终端查看已激活链码

~/repo/c2/wiz-demo$ wiz ch start

~/repo/c2/wiz-demo$ wiz admin

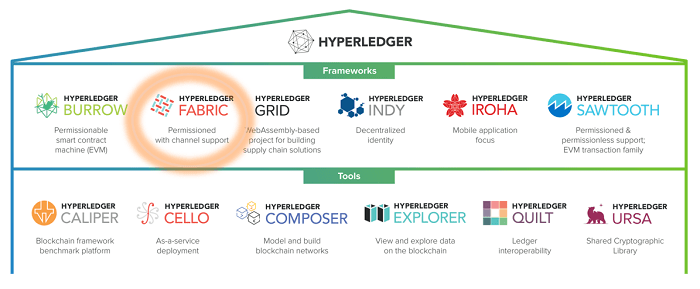
admin@org1> peer chaincode list --instantiated -C ch1

在4#终端进入项目目录，启动应用：

~/repo/c2/wiz-demo$ wiz app start

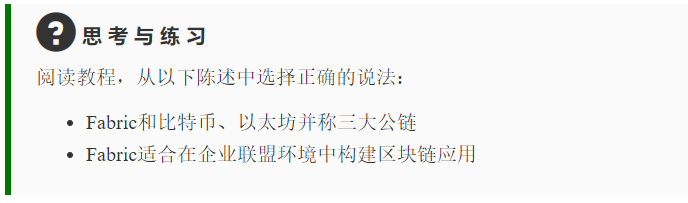
## Hyperledger及Fabric项目概述

Hyperledger 是一个旨在推动区块链跨行业应用的开源项目， 由 Linux基金会在2015年12月主导发起该项目， 成员包括金融、银行、物联网、供应链、制造和科技等多个行业的领头羊，托管了众多面向企业的区块链 开源框架和工具：



Hyperledger Fabric（后文简称Fabric）是其中发展最好的一个**企业级区块链平台**，最初由Digital Asset和IBM 贡献，目前已经应用于沃尔玛的食物溯源链（Foodtrust）和马士基的物流跟踪链（TradeLens）中， 代表了当下企业级区块链应用的最高水平。可以认为Fabric是一种联盟链（Consortium Blockchain）平台， 它适合构建跨越多个企业边界的去中心化应用。

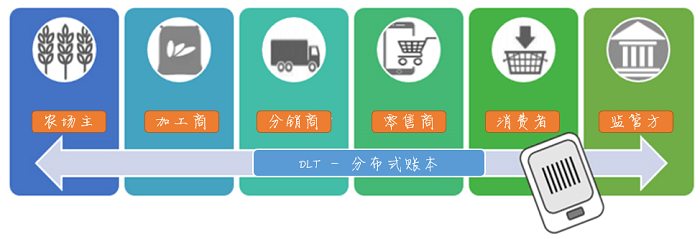
由于Fabric项目的目标是应用于相对可信的企业联盟环境，因此其设计思路与比特币、以太坊 等公链平台有明显的差异。Fabric借鉴了区块链的数据结构，但引入了相当多的身份验证与 权限控制机制，以及数据隐私保护机制，以适应企业级应用的要求。同时由于企业联盟环境 要比完全开放的公链环境可控，**因此Fabric没有强调其共识体系对拜占庭容错的实现，允许使用非拜占庭容错算法建立共识，从而可以达到相当实用的交易吞吐量。**



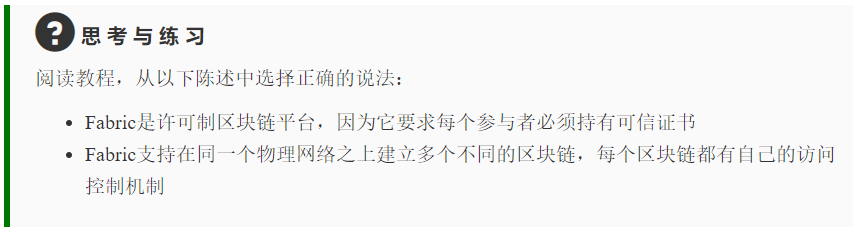
## Fabric的定位与特点

毫无疑问，Fabric是受到比特币的启发而诞生的，因此它借鉴了比特币、以太坊这些公链中的一些 核心特性，例如采用不可篡改的区块链结构来保存数据、采用非对称加密技术来进行身份识别 与认证、支持智能合约等等。

但是Fabric定位于企业级的分布式账本技术（**DLT** - **D**istributed **L**edger **T**echnology）平台， 它的主要目的是为跨越多个企业边界的活动提供不可篡改的分布式记账平台。例如在食物溯源 应用中，为了让消费者可以了解到所购买食物是否安全，就必须将从农场到加工商、分销商、 零售商乃至监管机构等各个环节的检验与放行信息记录到区块链上，以保证溯源信息的透明与可信：



因此Fabric是一种联盟链（Consortium Blockchain），它适合在多个企业间实现分布式记账，这一 定位使Fabric的实现与以太坊这样的公链有了明显的差异：



### 分布式账本 vs. 区块链

分布式账本是比区块链更加宽泛的概念，可以认为区块链只是分布式账本的一种实现技术， 其他的分布式账本实现还包括哈希图等。

### 去中心化 vs. 分布式

Fabric淡化了去中心化（Decentralized），而以分布式（Distributed）代替，这一思路带来了系统设计 与实现上的巨大影响。 例如，在Fabric中，采用中心化的CA机制来发放证书，只有持有有效证书的节点和用户才可以访问区块链 上的账本数据。因此Fabric是许可制 / Permissioned的区块链，这与不需要许可 / Permissionless 的以太坊这样的公链形成了鲜明的对比。

### 拜占庭容错 vs. 崩溃容错

由于采用许可机制，Fabric也淡化了对不可信（Trustless）环境下共识达成的依赖性，而假设 联盟链中的企业有可能是值得信赖的，因此并不依赖于工作量证明这样的拜占庭容错算法 —— 虽然 Fabric模块化的设计可以支持引入不同的共识算法实现，但目前的产品化方案是Kafka共识，它显然 是不能对抗拜占庭错误的 —— 不过对不可信环境支持的淡化处理有利于提高交易的吞吐量，这对于企 业级应用也是有益的。

### 数据隐私保护

在另一方面，Fabric强化了隐私保护能力。例如，Fabric支持在同一套企业网络上建立多个不同 的**通道/Channel**，每一个通道都有自己的区块链和访问控制，彼此互不影响，这有利于 复用基础设施，例如不同企业间的销售部门可以建立一个通道来分享市场数据，而这些企业间的 研发部门可以建立另一个通道来分享技术数据。

Fabric并不是唯一的联盟链解决方案，但目前可以说是最复杂的企业联盟链实现，这种复杂性 源于设计者对应用场景的假设和推演，以及对Fabric广泛适用性的考量，这是我们在学习过程 中需要换位思考的一点。

### 课程内容概述

本课程适合Java开发人员快速掌握超级账本Fabric区块链的设计思路、 核心概念、网络搭建、链码及应用开发等知识点，课程主要内容简述如下：

**第一章、课程概述**

简介Fabric项目来源、定位特点、适用场景以及其与公链平台的重要区别。

**第二章、初识Fabric**

创建一个最小CA，搭建一个最小Farbic网络，开发一个最小Fabric链码，实现 一个最小Fabric应用，从零开始学习并掌握Farbic中的核心概念、设计思路、 实用工具与开发模型。

**第三章、身份与权限管理机制**

深入学习Fabric中的身份验证机制与权限管理机制，理解证书、成员服务提供器、 策略、访问控制清单等核心概念并掌握其创建、部署和使用方法。

**第四章、通道配置与更新**

深入学习Fabric的通道配置初始化与更新流程、相关数据结构以及配置工具的 操作方法。

**第五章、链码与应用开发进阶**

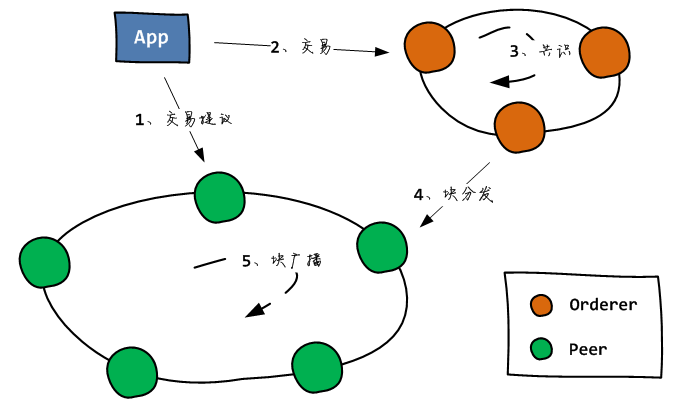
学习理解链码运行机制、掌握状态历史跟踪、富查询、通道事件监听等链码与应用 开发进阶知识。



## 初识Fabric

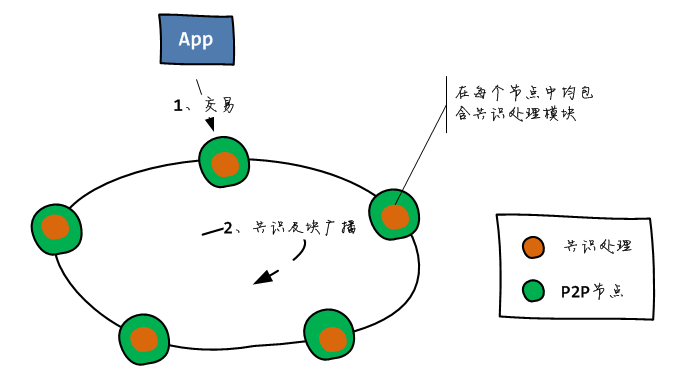
### Fabric架构概述

Fabric的架构中包含相当多的细节，为了便于理解，我们先观察最基本的两个 组成部分 - 对等节点（Peer）和排序器（Orderer）：



Fabric的设计采用分布式系统中经典的[状态机复制模型](https://en.wikipedia.org/wiki/State_machine_replication" \t "_blank)， 对等节点负责交易区块链的保存以及状态的更新，而排序器则负责**确定应用所提交的交易的先后 执行顺序**，并**将交易打包成块**后分发给**主导**对等节点，再由主导对等节点通过gossip协议扩散至其他对等节点，对等节点进行验证后执行交易从而更新其状态。

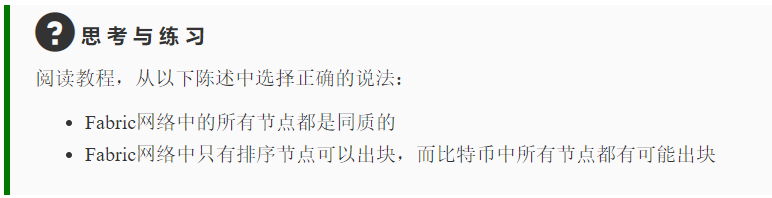
这一架构与大部分的区块链实现有显著的不同 —— 共识处理模块通常总是包含在每一个区块链的节点实现当中，例如比特币或者以太坊 —— 这使得所有的节点完全是同质的：



为什么Fabric要搞的这么复杂？

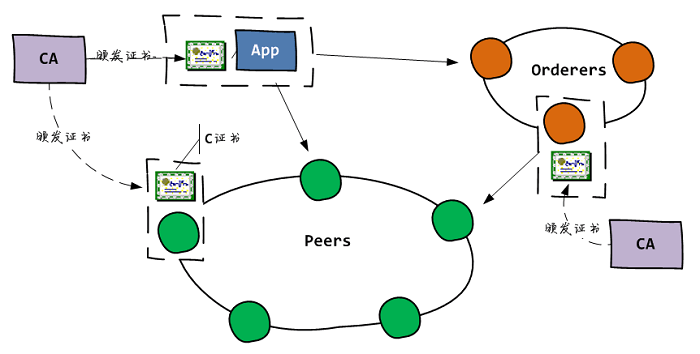
根据官方的说法，将共识处理从节点的功能中单独抽取出来作为一个可插拔的模块， 是为了能更好地利用已有的各种共识算法实现，例如崩溃容错（CFT）和拜占庭容错（BFT） 都已经有现成的实现工具包，这样就容易为Fabric添加各种共识支持。

例如，在当前的1.4版本中，Fabric提供了一个基于Kafka和Zookeeper实现的崩溃容错排序器，在接下来的发布中，还将提供一个基于etcd的**raft共识排序器**以及一个真正去中心化的**BFT排序器**。



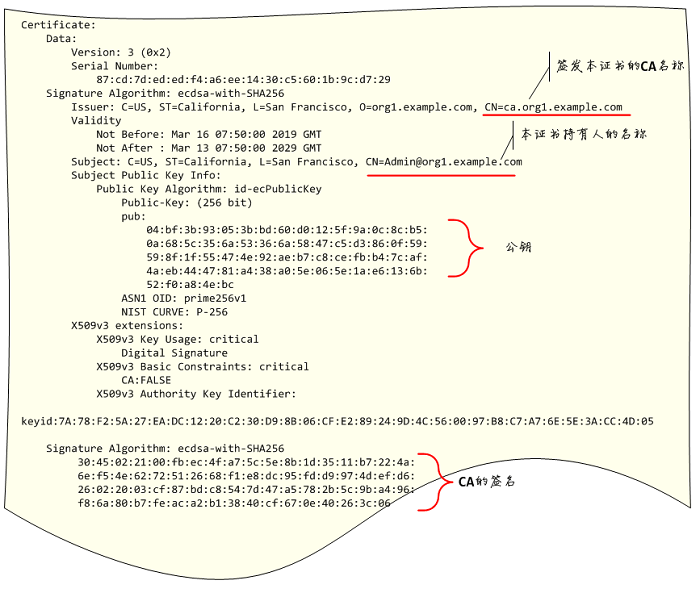
### 身份标识与验证机制

和大多数区块链一样，Fabric也采用**非对称加密技术**来标识用户的身份，**区别在于 Fabric取消了用户自己生成身份标识的权利，而采用中心化的CA来统一颁发证书作为**区块链参与各方（对等节点、排序器、应用用户等）的身份标识：



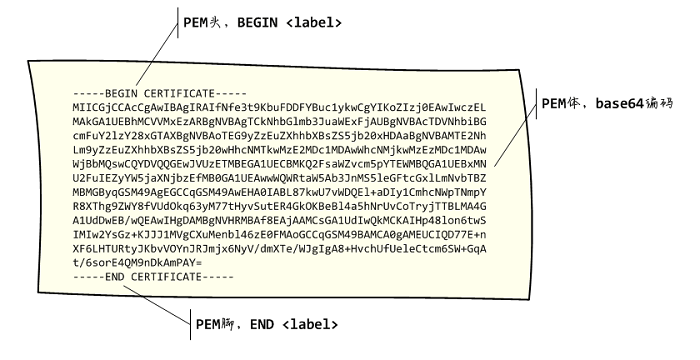
**在一个Fabric网络中可以使用单一的CA，也可以存在多个不同的CA，例如每个参与机构都由自己的CA为自己组织内的节点和用户颁发证书，并单独为排序节点建立一个CA。**

CA颁发的证书中包含了用户公钥和唯一标识名称等信息，同时也包含了CA的签名， 因此第三方可以验证用户持有的证书是否由CA签发，从而验证用户的身份。下图 展示了Fabric网络中使用的X509证书的主要内容：



在X509证书中，Issuer字段标识签发此证书的CA机构的唯一标识名，Subject字段 标识此证书持有者的唯一标识名。在唯一标识名中最常用的字段是常用名（CN：Common Name） 字段，例如上图中的ca.org1.example.com或者Admin@org1.example.com。

由于证书中包含用户公钥以及CA签名这些二进制数据，为了便于在网络环境中传输交换，通常会编码为仅包含ASCII码的 [PEM](https://en.wikipedia.org/wiki/Privacy-Enhanced_Mail) 格式，即**Privacy-Enhanced Mail** - 隐私增强邮件：



需要指出的是，证书是公开的，任何人都可以查看验证，因此在证书中并不包含用户的私钥信息。

可以使用openssl命令来查看一个证书的内容，例如：

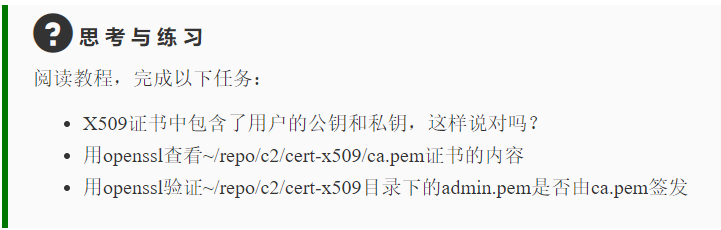
openssl x509 -in admin.pem \ *# 查看证书admin.pem的内容*

-text \ *# 输出格式为文本*

-noout *# 不显示原始PEM内容*

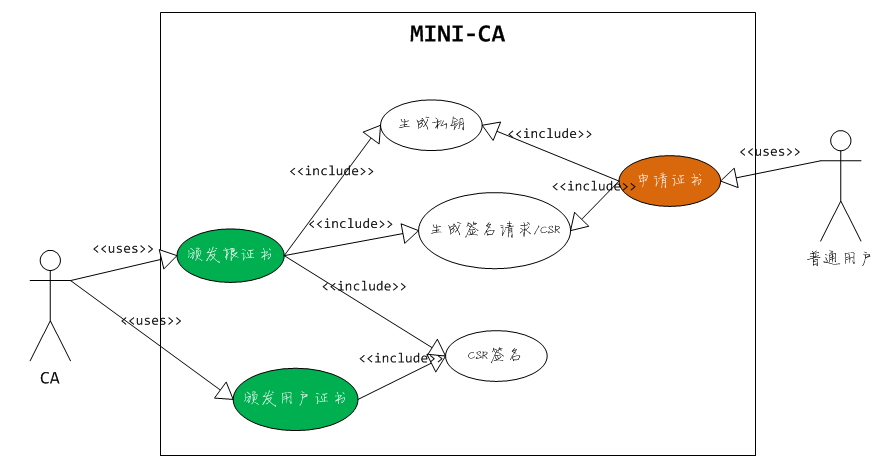
利用CA的证书可以验证一个指定的证书是否由该CA签发，例如：

**openssl** **verify** **-CAfile** **ca**.pem **admin**.pem



### 使用OpenSSL构建小型CA

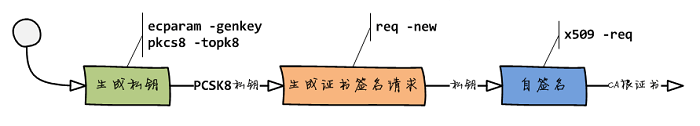
我们可以使用OpenSSL来建立一个CA，并为Peer、Orderer和用户颁发证书：



由于CA需要为自己签名，因此我们首先需要生成CA的自签名证书。

**CA自签名证书**

生成CA自签名证书主要包括三个环节：



首先使用ecparam子命令选择prime256v1椭圆曲线参数创建CA根密钥，这是Fabric中使用 的非对称加密算法：

openssl ecparam -genkey \ *# 生成椭圆曲线私钥*

-name prime256v1 \ *# 使用prime256v1椭圆曲线参数*

-out ca-key\_.pem *# 生成的EC私钥存入ca-key\_.pem文件*

然后将上述输出文件转换为不加密的PKCS8格式私钥并保存在ca-key.pem文件中， 以便后续在其他命令中利用私钥签名：

openssl pkcs8 -topk8 \ **# 将输入私钥转换为PKCS8格式**

-nocrypt \ **# 不加密输出的PKCS8私钥**

-**in** ca-key\_.pem \ **# 输入私钥为ca-key\_.pem**

-**out** ca-key.pem **# 输出存入ca-key.pem**

PKCS8的全文是Private Key Cryptography Standard #8，即私钥密码学8#标准， 是以ASCII存储密钥的互联网标准，可以点击[这里](https://tools.ietf.org/html/rfc5208) 查看规范原文。

现在利用私钥生成证书签名请求（CSR：Certificate Signing Request）文件，其中的配置文件 ca.conf中声明了CSR相关信息，例如唯一标识名称、启用的扩展等信息：

**openssl** **req** **-new** \ # 生成证书签名请求

**-key** **ca-key**.pem \ # 使用**ca-key**.pem中的私钥

**-out** **ca-csr**.pem \ # 输出的**CSR**存入**ca-csr**.pem文件

**-config** **ca**.conf # 使用**ca**.conf中的信息

由于我们是要生成**自签名的根证书**，因此直接使用根密钥签发请求文件ca-csr.pem， 就得到了自签名的根证书ca-cert.pem：

openssl x509 -req \ **# 生成x509证书**

-extensions ca\_cert \ **# 在证书中添加ca\_cert段声明的扩展**

-extfile ca.conf \ **# 包含扩展声明的文件**

-**in** ca-csr.pem \ **# 输入文件为ca-csr.pem**

-**out** ca-cert.pem \ **# 输出文件为ca-cert.pem**

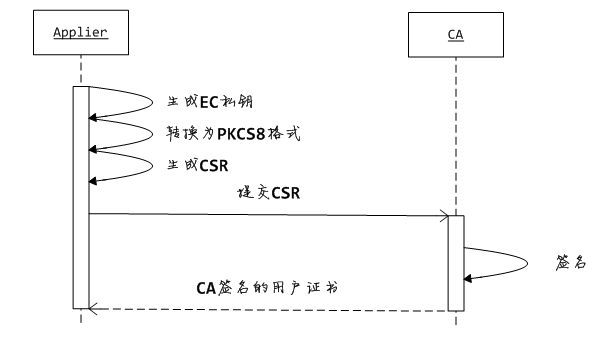
-signkey ca-key.pem \ **# 用来自签名的私钥**

-CAcreateserial \ **# 创建证书序列号**

-days 3650 **# 证书有效期为3650天，大约10年**

**签发用户证书**

一旦有了根证书，我们就可以签发用于节点、排序器或应用用户的证书了。 前面的步骤基本一样，都是生成EC私钥、转换为PCKS8格式、生成证书签名请求，只是分别由申请用户和CA完成：



申请用户首先生成私钥及证书签名请求：

**openssl** **ecparam** **-name** **prime256v1** **-genkey** **-out** **user-key\_**.pem

**openssl** **pkcs8** **-topk8** **-nocrypt** **-in** **user-key\_**.pem **-out** **user-key**.pem

**openssl** **req** **-new** **-key** **user-key**.pem **-out** **user-csr**.pem **-config** **user**.conf

最后的签名是由CA完成的，因此改为如下命令：

openssl x509 -req \

-extensions user\_cert \

-extfile ca.conf \

-**in** user-csr.pem \

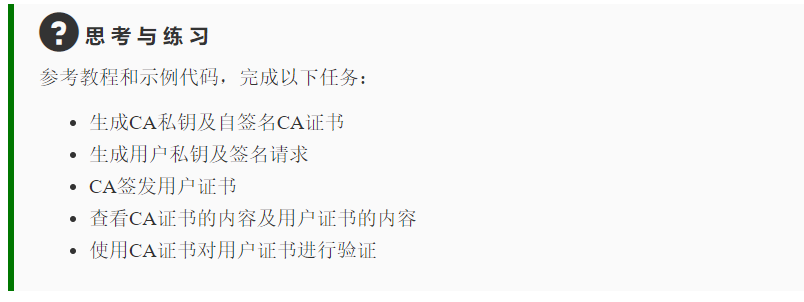
-**out** user-cert.pem \

-CA ca-cert.pem \ **# CA证书**

-CAkey ca-key.pem \ **# CA私钥**

-CAcreateserial \

-days 3650



### MSP：成员服务提供器

在许可制的系统中，仅有身份标识还不够，还需要一种机制来判定一个身份 标识是否是系统可接受的。例如，你可能有好几张不同银行发行的信用卡， 但在某个特定的超市却只能使用其中的一部分卡进行支付：



在Fabric中，这一判定机制由成员服务提供器（MSP：**M**embership **S**ervice **P**rovider） 来实现。每一个需要保护的资源都有自己的MSP，并利用MSP实现从身份向 角色的转换。

例如，对于Orderer和Peer而言，它们都需要一个本地的MSP配置（默认为：msp）目录来建立 其MSP实例，并且按照约定的目录结构来组织各种文件：

* admincerts：该目录中的所有PEM证书对应有管理员角色
* cacerts：该目录的每个PEM证书都是CA根证书
* keystore：该目录中包含节点私钥的单一PEM证书
* signcerts：该目录中包含节点的X509证书
* crls：可选，该目录中包含所有已回收的证书
* intermediatecerts：可选，该目录中的PEM证书对应中间CA证书
* config.yaml：可选
* tlscacerts：可选，该目录中包含用于TLS的CA根证书
* tlsintermediatecerts：可选，该目录中包含用于TLS的CA中间证书

我们可以将之前使用openssl创建的证书和user私钥整理为MSP配置目录，例如， 下面的命令创建必要的MSP目录并将相应的证书或密钥拷贝如对应的目录：

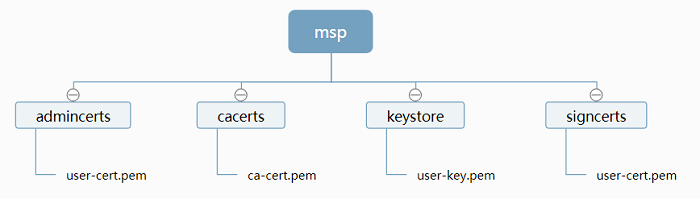
**mkdir** -p msp/admincerts && cp ../mini-ca/user-cert.pem msp/admincerts *# 赋予user管理员角色*

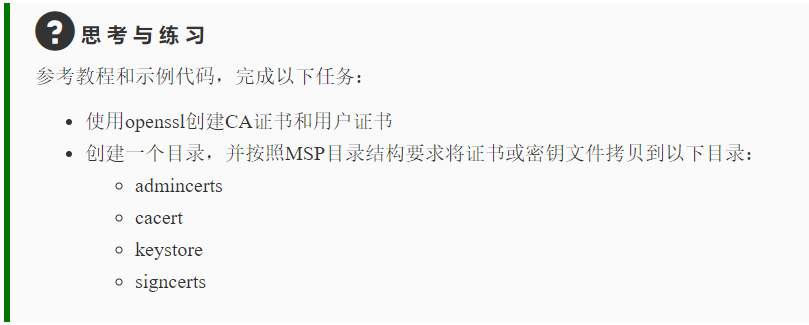
**mkdir** -p msp/cacerts && cp ../mini-ca/ca-cert.pem msp/cacerts *# CA证书*

**mkdir** -p msp/signcerts && cp ../mini-ca/user-cert.pem msp/signcerts *# 当前身份为user*

**mkdir** -p msp/keystore && cp ../mini-ca/user-key.pem msp/keystore *# 当前身份的私钥*

最终的目录结构如下图所示：



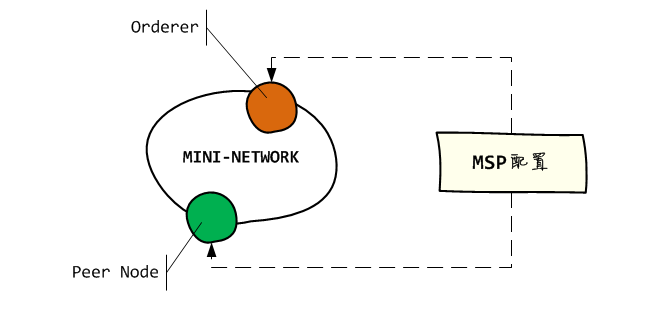


### 启动最小Fabric网络（终端1、终端2）

$ cd ~/repo/c2/solo-network

注意！！！需要清理之前的数据，比如data和artifact文件夹。不然会报错。

有了MSP配置，我们就可以启动一个最简单的Fabric网络了：



在这个网络中，只包含一个Orderer节点和一个Peer节点，而且两个节点使用同一个MPS配置 —— 这样做的好处是我们可以暂时忽略身份的差异对系统功能的影响，以便将注意力集中在对Fabric的整体理解上。

**启动排序节点（终端1）**

**启动排序节点之前，需要首先生成一个创世块，排序节点将利用这个创世块启动整个Farbic网络的系统通道。**

**可以使用官方提供的configtxgen工具来生成Farbic网络系统通道的创世块（**注意它不同于peer节点加入到普通通道!!!**）。configtxgen依赖于配置文件configtx.yaml中定义的网络结构 、访问策略等信息，并提供了不同的Profile以便应用于不同的场景， 可以认为Profile是网络结构、访问策略等网络配置信息的组合套餐。**

**例如，下面的命令使用SampleInsecureSolo套餐配置生成适用于单节点网络 的创世块并存入genesis.pb文件：**

$ configtxgen -outputBlock genesis.block \ *# 生成创世块并存入genesis.block*

-profile SampleInsecureSolo *# 使用SampleInsecureSolo配置套餐*

（也可以加入生成genesis.block的步骤，否则会在后续通道初始化出错）

有了创世块，我们就可以启动排序节点了。**排序节点程序依赖于配置文件 orderer.yaml**。同样，Fabric提供了默认的配置文件，我们只需要做简单的个性化调整即可。

例如，下面的命令使用刚才生成的创世块genesis.block启动排序节点：ORDERER\_GENERAL\_GENESISMETHOD=file \ # 使用创世块文件

ORDERER\_GENERAL\_GENESISFILE=./genesis.block \ # 创建块文件的路径

ORDERER\_FILELEDGER\_LOCATION=./data/orderer \ # 系统通道账本（区块链）数据的路径

（注意！！！将提供的start-orderer.sh中的前两行换成这里的两行）（貌似不需要？）

orderer *# 排序节点程序*

需要指出的是，上面的命令使用环境变量来调整排序节点的配置项，你也可以直接修改orderer.yaml中的对应配置项。例如，环境变量ORDERER\_GENERAL\_GENESISMETHOD 对应于orderer.yaml中的General.GenesisMethod配置，而ORDER\_FILEGEDGER\_LOCATION 则对应于orderer.yaml中的FileLedger.Location配置。

**启动对等节点（终端2）**

类似的，对等节点依赖于配置文件core.yaml，我们也可以在Farbic提供的 默认配置文件上进行自定义调整。例如：

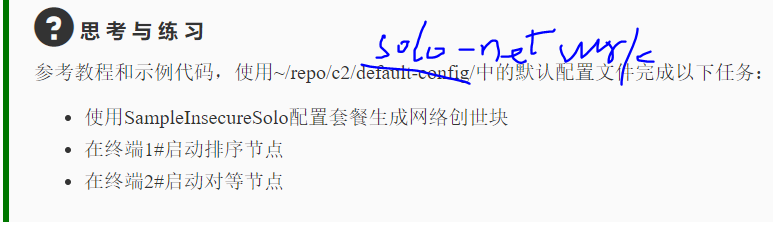
CORE\_PEER\_FILESYSTEMPATH=./data/peer \ # 通道账本（区块链）数据的路径

CORE\_PEER\_LISTENADDRESS=127.0.0.1:7051 \ # 节点监听地址

CORE\_PEER\_CHAINCODELISTENADDRESS=127.0.0.1:7052 \ # 节点链码服务监听地址

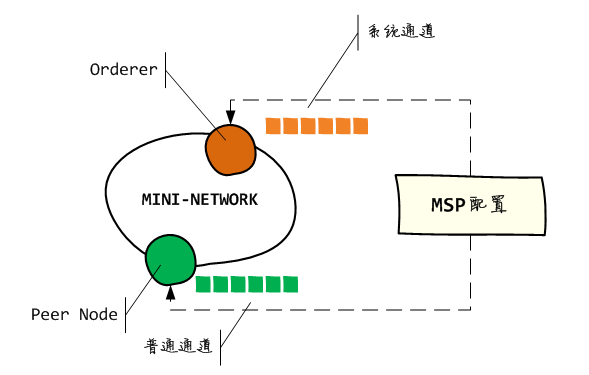
CORE\_CHAINCODE\_MODE=dev \ # 链码服务设置为开发模式

peer node start



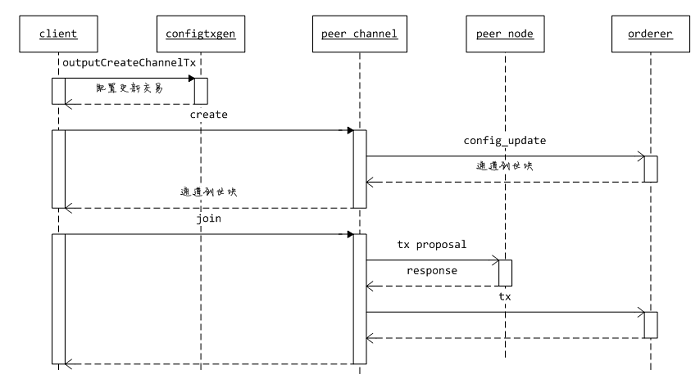
### 通道初始化与节点加入（终端3）

当我们启动排序节点时，利用创世块也同时启动了保存整个网络配置的系统通道：



不过我们通常提到的通道，都是指的由对等节点维护的**普通通道**，一个对等节点可以加入多个普通通道，通道彼此是隔离的，都有自己的区块链和访问控制机制。

节点在初始启动后是没有加入任何通道的，因此我们需要先创建一个通道并让节点加入这个通道。整个流程分为三个步骤：**生成通道创建交易**、**创建通道**和 **节点加入通道**：



* **首先使用configtxgen工具生成通道创建交易：**

configtxgen -outputCreateChannelTx ch1.tx \ # 输出通道创建交易并存入指定文件

-profile SampleSingleMSPChannel # 使用的配置套餐

-channelID ch1 #指定通道ID

* **然后生成通道创世块ch1.block：**

peer channel create -c ch1 \ *# 创建通道ch1* #这个通道id貌似有问题，改成testchainid?

-f ch1.tx \ *# 使用交易文件ch1.tx*

-o localhost:7050 \ *# 排序器节点地址*

--outputBlock ch1.block *# 输出创世块文件*

（注意！！！如果完全按照教程来的话，这里会出错，是因为之前已经创建过通道ch1的原因。删除data目录：rm -rf data，删除data目录就可以清理之前的数据），然后从启动orderer节点开始。

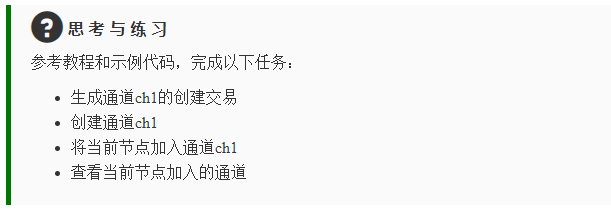
* 最后将当前对等节点加入通道：

peer channel join -b ch1.block -\ *# 通道创世块文件*

-o localhost:7050 *# 排序节点地址*

* 可以使用channel list命令查看当前节点加入的通道：

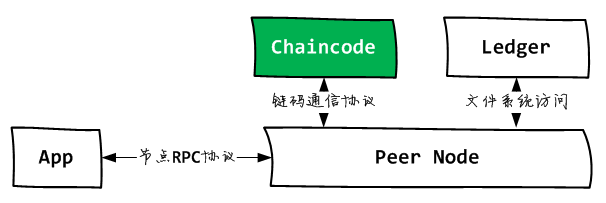
peer channel list



### 开发计数器链码（终端4）

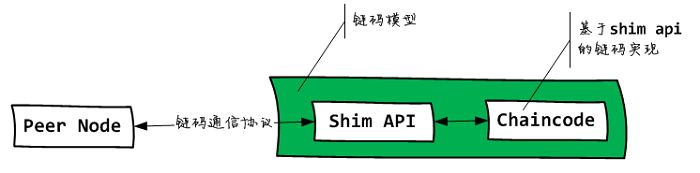
（注意！！！这一节要新的终端进入/repo/c2/counter-cc这个文件夹操作。）

在Fabric中，**智能合约**被称为链码（Chaincode），**链码负责定义区块链交易以及状态，应用程序则通过链码来访问通道区块链**：



与以太坊不同，Fabric并没有实现专门的智能合约虚拟机，链码实际上就是一个 操作系统进程，它通过链码通信协议与Peer节点通信，负责执行节点转发的调用 请求，同时也利用节点提供的API访问通道账本（区块链）。因此理论上可以使用 任何图灵完备的语言开发Fabric链码，不过目前官方仅提供了NodeJS、Java和GO 的链码开发包。

使用Java链码开发包中的[shim API](https://github.com/hyperledger/fabric-chaincode-java" \t "_blank) 开发链码非常简单：只需要实现init()和ivoke() 这两个接口即可。当Fabric通道激活链码时将执行init()方法，而当应用调用链码 方法时，将执行invoke()方法。shim API封装了链码通信协议：



下面的Java代码实现了一个最简的链码，当链码激活时，初始化计数器值为0， 当调用链码方法时，计数器值加1：

**package** com.hubwiz.demo;

**import** org.hyperledger.fabric.shim.ChaincodeBase;

**import** org.hyperledger.fabric.shim.ChaincodeStub;

**public** **class** **CounterChaincode** **extends** **ChaincodeBase**{ *//继承ChaincodeBase*

**@Override**

**public** Response **init**(ChaincodeStub stub){ *//init接口实现*

stub.putStringState("value","0");

**return** newSuccessResponse("init"); *//返回调用端的信息*

}

（注意！！！：示例代码提供的repo/c2/counter-cc/ CounterChaincode.java错误，原因是init方法缺少对value变量的初始化）

**@Override**

**public** Response **invoke**(ChaincodeStub stub){ *//invoke接口实现*

String valueStr = stub.getStringState("value");

**int** value = Integer.parseInt(valueStr);

stub.putStringState("value",(value+1)); *//更新链码状态*

**return** newSuccessResponse(String.format("value updated: %d",value));

}

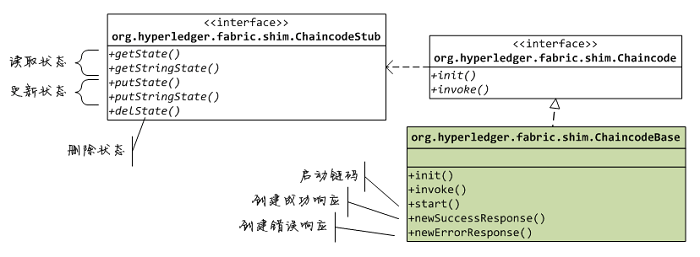
**public** **static** **void** **main**(String[] args){

**new** CounterChaincode().start(args); *//****启动链码***

}

}

链码的基类ChaincodeBase封装了链码通信协议，因此我们开发的链码需要继承这个类， 并重写init()方法和invoke()方法：



init()和invoke()方法的stub参数是Shim API传入的对**通道账本**的**抽象封装**，可以 使用它的putState()方法设置**通道Key-Value状态库**的指定键值，例如上面的代码中在初始化激活时将counter状态的值设置为0；类似的，使用stub对象的getState() 方法获取状态库中指定键的值。需要指出的是，**getState()和putState()的值都采用 byte[]类型**，因此我们使用了语法糖getStringState()和putStringState()，可以方便地处理字符串类型的状态值。

链码实例的start()方法将启动与节点链码服务的连接，因此在上面代码的最后，使用该方法启动Counter链码实例。

**启动链码（终端4）**

**在开发模式下（**在“启动最小Fabric网络”这一节中，就是以开发模式启动peer节点的**），需要自己启动链码，启动链码和运行普通的Java程序一样**， 只是需要指定节点的链码服务访问地址和链码的名称，例如直接用gralde运行：

gradle run --args='--peer.address 127.0.0.1:7052 --id counter-cc:0' # 最后一个参数是：链码ID:版本号

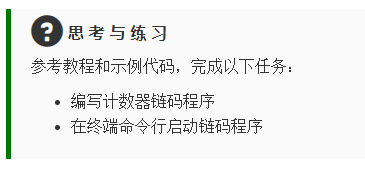
peer.address参数声明链码要连接的节点链码服务地址，id参数声明链码包含版本号的标识名称。

也可以生成jar包后再运行，例如，用下面的终端命令生成jar包：

gradle clean shadowJar # 生成的jar包在build/lib/chaincode.jar

然后直接启动生成的jar包：

java -jar build/lib/chaincode.jar --peer.address 127.0.0.1:7052 --id counter-cc:0



### 链码方法的路由

Fabric的Shim API仅仅定义了init()和invoke()这两个链码接口，如果我们需要细化链码 方法，就需要在这两个接口中进行方法的路由了。不过由于init()方法仅在链码激活时调用，因此通常我们只需要处理invoke()接口的实现。

可以将链码invoke()接口的实现方法进行改进，以便路由到链码实例的其他方法。例如下面的代码为链码定义了两个新的方法，并根据用户请求的第一个参数（视为方法名）分别路由到inc()方法和value()方法，或者返回一个错误响应：

@Override

**public** Response **invoke**(ChaincodeStub stub){

String fcn = stub.getFunction(); **# 链码请求中的第一个参数**

List<String> args = stub.getParameters(); **# 链码请求中的其他参数**

**switch**(fcn){

**case** "inc": **return** inc(stub,args); **# 路由到inc()方法**

**case** "value": **return** **value**(stub,args); **# 路由到value()方法**

}

**return** newErrorResponse("unimplemented method");

}

**private** Response **inc**(ChaincodeStub stub,List<String> args){...}

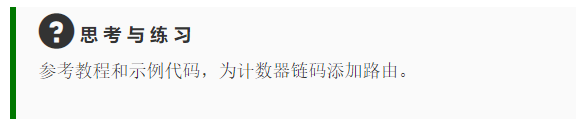
**private** Response **value**(ChaincodeStub stub,List<String> args){...}

当调用链码时，传入的第一个参数对应于上面代码中的fcn变量，而后续的参数则对应于 params数组。例如，对inc()方法的调用方法如下（注意！！！只是个例子，目前链码还没安装和激活，不可请求）：

peer chaincode invoke -n counter-cc \ *# 调用counter-cc链码*

-c '{"Args":["inc","10"]}' *# 调用链码的inc方法，step为10*

-C ch1 *# 通道限定为ch1*



### 链码的安装与激活（终端3）

链码开发后需要部署到通道上才能生效。部署流程分为两步：**1、安装到节点；2、在通道激活。**

使用chaincode install命令安装链码到当前节点上。例如：

peer chaincode install -n counter-cc

-v 0 \ *# 链码名称及版本号*

-l java *# 链码开发语言*

-p /home/user/c2/counter-cc *# 链码全路径*

安装到节点上的链码还需要在特定通道上激活才能被访问。使用chaincode instantiate命令 激活指定的已安装链码：

peer chaincode instantiate -n counter-cc -v 0 \ *# 要激活的链码名称及版本号*

-o localhost:7050 *# 排序节点地址*

-C ch1 *# 在ch1通道上激活链码*

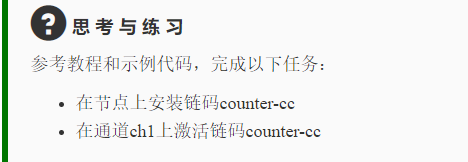
链码激活后就可以使用chaincode query或chaincode invoke命令调用链码了， 两者的区别在于，前者用于对链码状态的查询而后者用于提交交易。

例如，下面的命令提交链码交易，在执行后链码状态counter将加1：

peer chaincode invoke -n counter-cc -C ch1

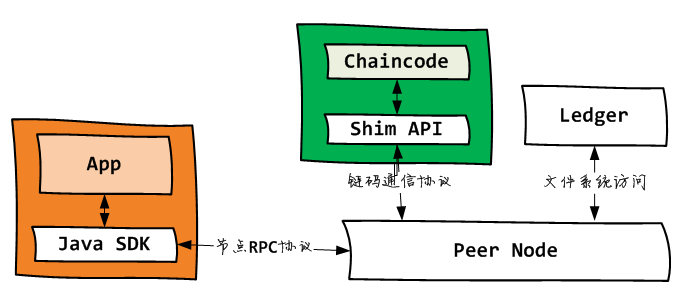
而下面的命令虽然也可以调用链码，但是它并不能更新链码状态，因此无论 调用多少次都返回相同的结果：

peer chaincode query -n counter-cc -C ch1

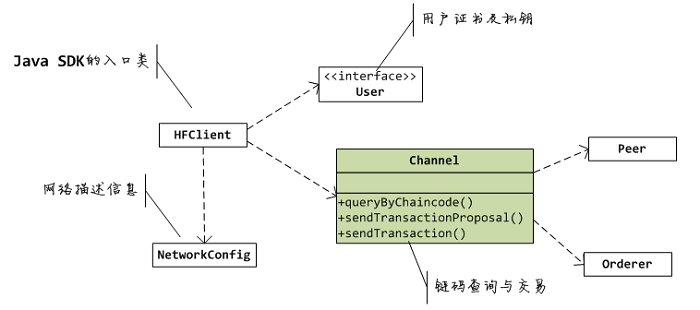


### 在应用中访问链码

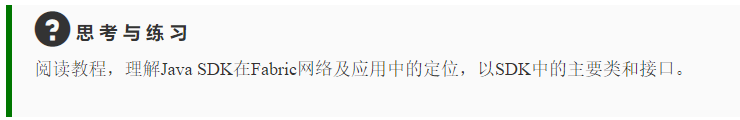
在Fabric中，应用通过节点的RPC协议接口访问链码：



类似于Shim API对链码通信协议的封装，Fabric Java SDK提供了对节点RPC协议接口的封装，其入口**类为HFClient**，对**链码的查询**和**交易操作**则封装在**Channel类**中：

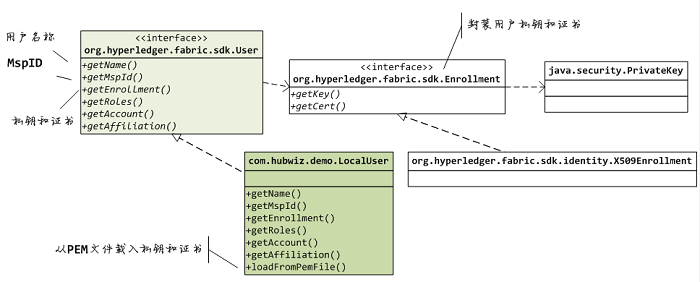


由于Fabric是许可制区块链，因此应用也需要持有证书和私钥，HFClient实例 依赖于User接口的实现对象来访问一个特定身份的证书和私钥，**因此在访问 链码之前，我们需要首先定义一个简单的User接口实现类。**



### User接口实现类

HFClient实例访问Fabric网络的身份使用User接口实现对象来表征。因此我们需要实现一个简单的User接口实现类：



首先完成实现类LocalUser的骨架：

**import** org.hyperledger.fabric.sdk.User;

**import** org.hyperledger.fabric.sdk.security.CryptoPrimitives;

**public** **class** **LocalUser** **implements** **User**{ *//实现User接口*

**private** String name;

**private** String mspId;

**private** Enrollment enrollment;

LocalUser(String name,String mspId){

**this**.name = name;

**this**.mspId = mspId;

}

**private** Enrollment **loadFromPemFile**(String keyFile,String certFile){ */\*见下文说明\*/* }

**@Override** **public** String **getName**(){ **return** name; }

**@Override** **public** String **getMspId**() { **return** mspId}

**@Override** **public** Enrollment **getEnrollment**() { **return** enrollment; }

**@Override** **public** String **getAccount**() { **return** **null**; }

**@Override** **public** String **getAffiliation**() { **return** **null**; }

**@Override** **public** Set<String> **getAccounts**() { **return** **null**; }

}

在Fabric Java SDK中，**Enrollment接口用来提供对用户的私钥和证书的访问**， 并且预置了一个适合X509证书的实现类X509Enrollment，因此我们可以从本地 MSP目录中的PEM文件中载入**用户私钥**和**签名证书**：

**private** Enrollment **loadFromPemFile**(String keyFile,String certFile) throws Exception{

**byte**[] keyPem = Files.readAllBytes(Paths.**get**(keyFile)); *//载入私钥PEM文本*

**byte**[] certPem = Files.readAllBytes(Paths.**get**(certFile)); *//载入证书PEM文本*

CryptoPrimitives suite = **new** CryptoPrimitives(); *//载入密码学套件*

PrivateKey privateKey = suite.bytesToPrivateKey(keyPem); *//将PEM文本转换为私钥对象*

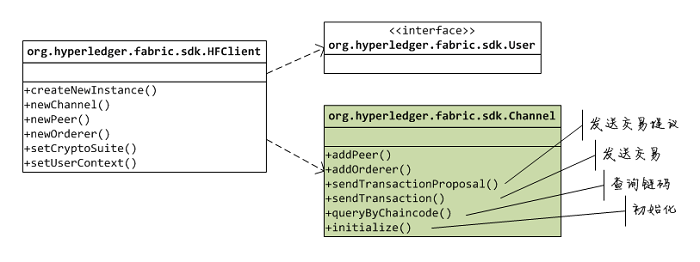
**return** **new** X509Enrollment(privateKey,**new** String(certPem)); *//创建并返回X509Enrollment对象*

}



### 通道访问参数设置

如前所述，Java SDK的入口类是HFClient，不过我们要访问链码则主要是 通过Channel对象来完成的，例如查询链码或者向链码提交交易：



因此首先创建一个HFClient实例，并设置它的密码学套件和用户身份：

HFClient client = client.createNewInstance();

client.setCryptoSuite(CryptoSuite.Factory().getCryptoSuite());

LocalUser user = **new** LocalUser("admin","SampleOrg");

user.loadFromPemFile("msp/keystore/user-key.pem","msp/signcerts/user-cert.pe");

client.setUserContext(user);

接下来就可以创建Channel对象了。由于Channel对象需要向背书对等节点 发送交易提议，也需要向排序节点发送交易，因此还需要为Channel对象 添加对等节点和排序节点，并在配置之后进行必要的初始化：

Channel channel = client.newChannel("ch1");

Peer peer = client.newPeer("peer1","grpc://127.0.0.1:7051");

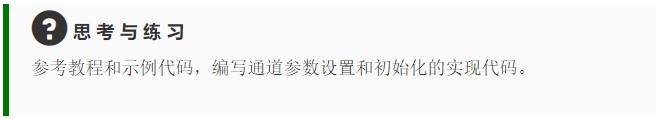
channel.addPeer(peer);

Orderer orderer = client.newOrderer("orderer1","grpc://127.0.0.1:7051");

channel.addOrderer(orderer);

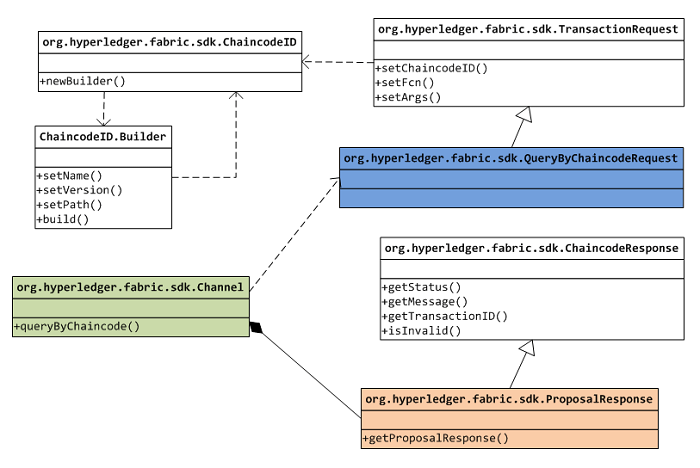
channel.initialize();

（注意！！！这一段代码的意思应该是该客户端节点加入通道ch1，并以orderer1和peer1节点为锚点，与orderers节点和peers节点交互）



### 链码查询

通道对象Channel提供了链码的查询方法queryByChaincode()，其输入参数为一个 QueryByChaincodeRequest对象，而返回值则是ProposalResponse的集合：



下面我们通过对counter-cc链码的value方法的调用，来详细学习如何在Java代码 中实现链码查询功能。

首先按照要求准备请求对象，由于链码的value方法不需要参数，因此我们只需要 设置链码的ID和方法名即可：

QueryByChaincodeRequest req = client.newQueryProposalRequest();

ChaincodeID cid = ChaincodeID.newBuilder().setName("counter-cc").build();

req.setChaincodeID(cid);

req.setFcn("value");

现在把准备好的请求对象传入通道的queryByChaincode()方法，以便它提交给节点处理：

Collection<ProposalResponse> rspc = channel.queryByChaincode(req);

**queryByChainCode()返回的是一组ProposalResponse，为什么？**

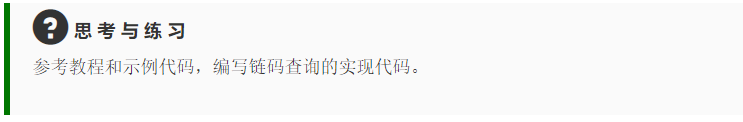
这是因为如果在通道对象上添加了多个对等节点（一个客户端节点可以添加多个peer节点为它服务？），queryByChaincode()方法会向所有的节点发送请求并收集所有的响应到一个集合对象中再返回：

**for**(ProposalResponse rsp: rspc){

System.**out**.format("status: %d\s",rsp.getStatus().getStatus());

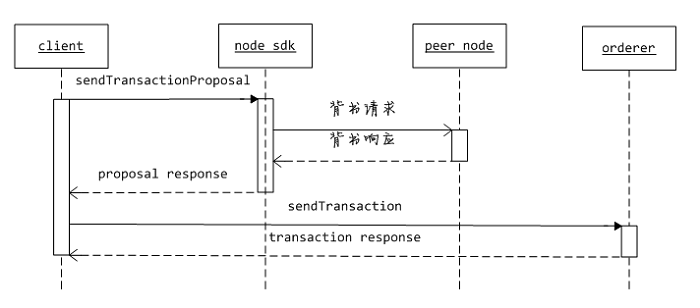
System.**out**.format("payload: %s\n", rsp.getProposalResponse().getResponse().getPayload().toStringUtf8());

}



### 链码交易

向链码提交交易则复杂一些，需要依次使用通道的sendTransactionProposal()和sendTransaction() 这两个方法，分别向对等节点和排序器提交请求。这个过程的时序表示如下：



首先构造请求对象TransactionProposalRequest：

TransactionProposalRequest req = client.newTransactionProposalRequest();

ChaincodeID cid = ChaincodeID.newBuilder().setName("counter-cc").build();

req.setChaincodeID(cid);

req.setFcn("inc");

req.setArgs("10");

然后向对等节点提交提议，等待节点背书结果集：

Collection<ProposalResponse> rsp = channel.sendTransactionProposal(req);

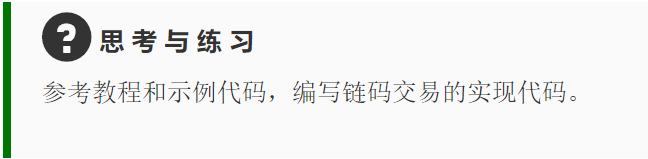
可以对背书结果集进行检查，以避免将无效的响应提交给排序节点，也可以简单 地直接提交给排序节点：

CompletableFuture<TransactionEvent> rsp = channel.sendTransaction(rsp);

TransactionEvent **event** = rsp.**get**();

System.**out**.format("txid: %s\n", **event**.getTransactionID());

System.**out**.format("valid: %b\n", **event**.isValid());

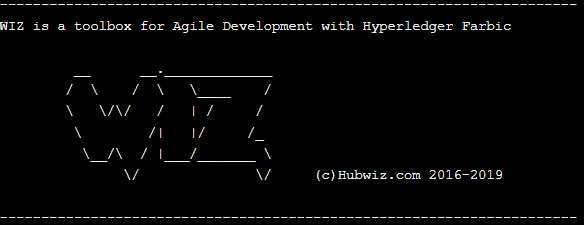


### 运行/repo/c2/counter-dapp（终端5）

（注意！！！：示例代码提供的repo/c2/counter-dapp/ App.java中的” Peer peer = client.newPeer("peer1`","grpc://127.0.0.1:7051");”错误，删除`即可）

### 使用WIZ开发工具箱（终端1-5）

**Fabric的环境配置相当繁琐**，为了提高开发效率，课程提供了一个便利的开发工具箱**WIZ**：



wiz提供了一个简单的Fabric应用开发模板，以及一组用于提高效率的脚本。

**初始化项目目录**

创建一个新目录，然后执行wiz init命令初始化目录结构：

~$ mkdir -p ~repo/test-wiz && cd ~/repo/test-wiz

~/repo/test-wiz$ wiz init

wiz项目的目录结构组织如下：

* network：fabric网络定义与配置数据目录
* chaincode：链码源代码目录
* application：应用源代码目录
* script：脚本目录

**启动网络（终端1）**

在wiz项目目录内，使用wiz net start命令启动网络，在初次启动网络前 需要使用wiz net reset命令初始化网络配置。例如，在1#终端执行如下命令：

~/repo/test-wiz$ wiz net rest

~/repo/test-wiz$ wiz net start

**启动链码（终端2）**

在wiz项目目录内，使用wiz cc start命令启动链码。例如，在2#终端 执行如下命令：

~/repo/test-wiz$ wiz cc start

**启动通道环境（终端3）**

在wiz项目目录内，使用wiz ch start命令启动通道并进行必要的环境初始化， 包括将当前节点加入通道、安装并激活链码。例如，在3#终端执行如下命令：

~/repo/test-wiz$ wiz ch start

**启动管理终端（终端4）**

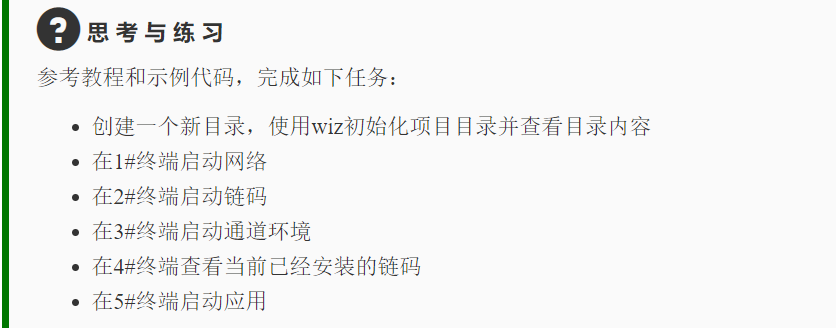
在wiz项目目录内，使用wiz admin命令进入管理终端，管理终端配置了必要的环境变量，因此可以直接以管理员身份执行peer命令。例如，在4#终端执行如下命令进入管理终端，并查看当前节点加入的通道：

~/repo/test-wiz$ wiz admin admin@org1> peer channel list

**启动应用（终端5）**

在wiz项目目录内，使用wiz app start启动项目应用。例如，在5#终端执行 如下命令：

~/repo/test-wiz$ wiz app start

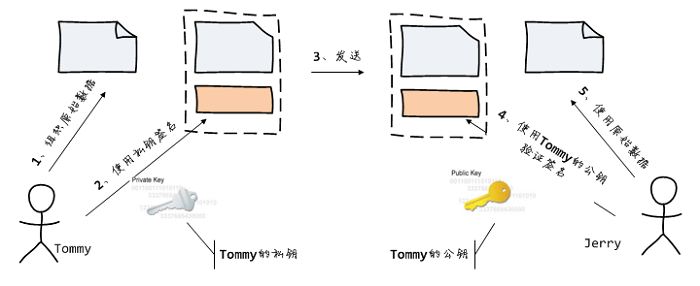


## 身份与权限管理机制

### 非对称密码学

非对称密码学是密码学中的一种算法，也被称为公钥密码学，因为它需要两个密钥：一个 是可以公开的密钥即公钥，另一个则是需要保密的私有密钥即私钥。

对称加密采用一对密钥（私钥、公钥）进行数据的加密或解密： 用私钥加密，则需要用 公钥解密；用公钥加密，则需要用私钥解密。 这一非对称特性使得其非常适合用于身份 表示与验证 —— 公钥用于 身份的表示，而私钥则用于身份的验证：



在上图中，当tommy需要向jerry发送原始数据时，他首先使用自己的私钥对 原始数据进行签名， 得到的签名数据附加在原始数据后面，一同发送给jerry。 jerry收到数据后，使用tommy的公钥 就可以验证签名是否是由tommy的私钥签发的， 从而确认该数据确实来自于tommy。

例如，我们可以用openssl来实践这一过程。

首先为tommy创建私钥，然后导出公钥，分别保存在tommy-priv.pem和tommy-pub.pem中：

openssl ecparam -genkey \ **# 生成私钥**

-name prime256v1 \ **# 椭圆曲线参数为prime256v1**

-**out** tommy-priv.pem **# 输出保存文件**

openssl ec -pubout \ **# 生成公钥**

-**in** tommy-priv.pem \ **# 输入私钥文件**

-**out** tommy-pub.pem **# 输出公钥文件**

然后使用tommy的私钥对hey-jude.txt文件签名，并将得到的二进制签名文件signature.sha256 进行base64编码得到签名的ASCII表示并存入文件signature.base64，以便通过邮件等形式发送：

~$ openssl dgst -sha256 \ *# 生成sha256哈希*

-sign tommy-priv.pem \ *# 签名私钥*

-out signature.sha256 \ *# 输出文件* hey-jude.txt *# 待签名文件*

~$ openssl base64 -**in** signature.sha256 \ *# 输入哈希文件*

-out signature.base64 *# 输出base64编码文件*

当jerry收到hey-jude.txt和signature.base64后，首先将base64的编码还原回二进制格式， 然后就可以利用tommy的公钥进行签名验证：

~$ openssl base64 -d -**in** signature.base64 \ *# 输入base64编码文件*

-out signature.bin *# 输出解码后的哈希文件*

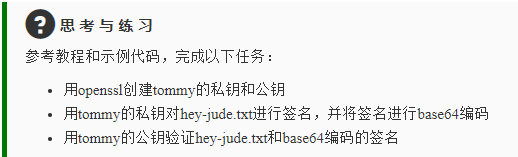
~$ openssl dgst -verify tommy-pub.pem \ *# 使用指定的公钥验证签名*

-sha256 \ *# 签名哈希算法为sha256*

-signature signature.bin \ *# 签名文件*

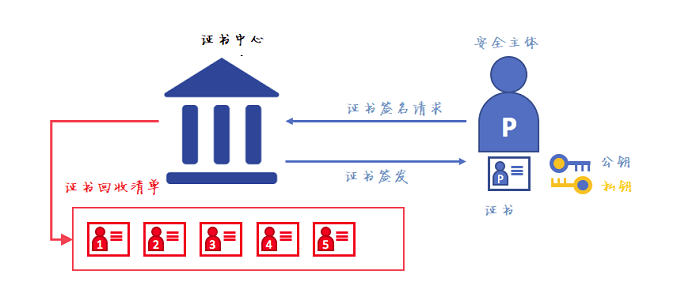
hey-jude.txt *# 原始数据文件*

一旦认证OK，就可以表明：1、签名确实是jerry的 2、hey-jude.txt原文未被篡改。



### PKI体系与MSP机制

在去中心化的区块链中，例如比特币和以太坊，采用公钥或者将公钥单向变换为地址， 就可以作为用户身份标识了，因此在这些区块链平台，并不需要中心化的身份生成与 验证。但是在Fabric中，应该是考虑到要实现相对复杂的**访问权限控制**，因此引入了中心化的PKI体系：



在PKI中，首先需要一个证书颁发机构（CA：Certificate Authority）来统一 的为用户签发证书（Certificate），在证书中包含有用户的公钥，因此第三方可以 方便地验证某个用户的证书是否是指定的CA所颁发。

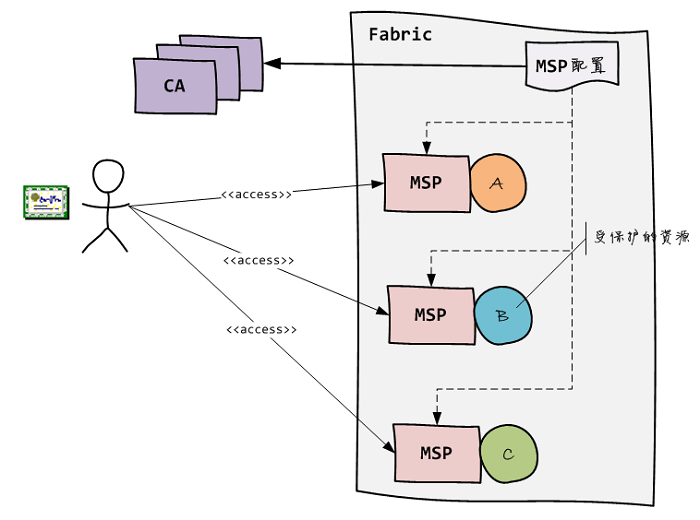
需要指出的是，密钥对还是由用户自己生成，CA只负责为用户提交的信息进行签名即可得到证书。 在上述过程中，用户提交的信息被称为证书签名请求（CSR：Certificate Signing Request）， 它除了需要包含用户的公钥之外，还需要包含关于持有者（Subject）的一些额外信息， 例如所属机构名称等等。

**MSP：会员许可机制**

我们知道，Fabric是许可制区块链平台，因此它需要PKI这种中心化的机制 来管理证书的发放与回收，同时也是利用CA来验证用户持有的证书是否有效。

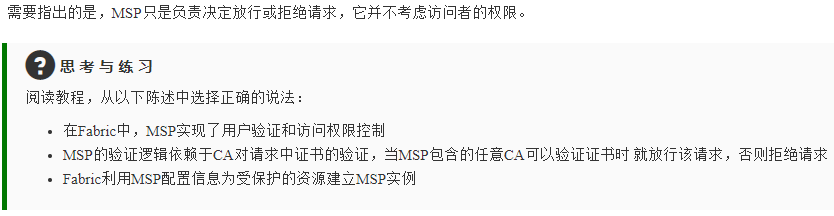
可以认为CA本身就提供了一种会员（Membership）机制：只有持有CA签发证书的用户，才可以访问区块链，否则将被拒之门外——会员制是一种有效的身份验证机制。

Fabric将会员验证机制定义为MSP（Membership Service Provider）组件， 它使用MSP来保护区块链上的每一个资源：当用户访问区块链时，**相应资源对应 的MSP**将验证用户是否属于该资源的会员，并根据检查结果拒绝或放行用户的访问：



Fabric会利用MSP配置信息为每个受保护资源（例如**链数据、排序节点**等）建立一个MSP实例，当用户试图访问受限资源时，首先需要通过MSP的验证。验证的逻辑 很简单：Fabric提取用户请求中的证书信息，然后验证是否是**MSP中的CA**签发的证书，是的话就放行，不是的话就拒绝。

需要指出的是，MSP只是负责决定放行或拒绝请求，它并不考虑访问者的权限。



### 使用cryptogen配置本地MSP