**Hyperledger Fabric的部署与使用**

# 一、 实验目标

实验目标概述如下：

1. 熟悉Fabric联盟链的系统架构，了解其基本运作模式
2. 搭建一个简单的Fabric网络
3. 部署并调用简单的链码
4. 拓展实验：在Fabric中使用CouchDB进行富查询

# 二、 基本知识

### 区块链的分类，联盟链

区块链系统根据应用场景和设计体系的不同，一般分为公有链、联盟链和私有链。其中：公有链的各个节点可以自由加入和退出网络，并参加链上数据的读写，运行时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点。私有链的各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放。私有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。

联盟链本质上仍然是一种私有链，只不过它比单个小组织开发的私有链更大，却又没有公有链这么大的规模，可以理解为它是介于私有链和公有链之间的一种区块链。

联盟区块链是指其共识过程受到预选节点控制的区块链；例如，不妨想象一个有15个金融机构组成的共同体，每个机构都运行着一个节点，而且为了使每个区块生效需要获得其中10个机构的确认（2/3确认）。区块链或许允许每个人都可读取，或者只受限于参与者，或走混合型路线，例如区块的根哈希及其API对外公开，API可允许外界用来作有限次数的查询和获取区块链状态的信息。这些区块链可视为“部分去中心化”。

联盟链有以下特点：

（1）部分去中心化。与公有链不一样，联盟链在某种程度上只属于联盟内部的成员所有，且很容易达成共识，因为毕竟联盟链的节点数是非常有限的。

（2）可控性较强。公有链是一旦区块链形成，将不可篡改，这主要源于公有链的节点一般是海量的，比如比特币节点太多，想要篡改区块数据，几乎不可能，而联盟链，只要所有机构中的大部分达成共识，即可将区块数据进行更改。

（3）数据不会默认公开。不同于公有链，联盟链的数据只限于联盟里的机构及其用户才有权限进行访问。

（4）交易速度很快。和私有链一样，联盟链本质上还是私有链，因此由于其节点不多的原因，达成共识容易，交易速度自然也就快很多。

### 超级账本（Hyperledger）和Fabric项目

超级账本（Hyperledger）是由Linux基金会于2015年发起的推进区块链数字技术和交易验证的开源项目，吸引了包括华为、腾讯云、百度金融、三星、IBM、英特尔、Fujitsu、Cisco、 Redhat、Oracle 等众多公司参与，目前已经有超过200家会员单位。超级账本项目的目标是让成员共同合作，共建开放平台，满足来自多个不同行业的用户案例，并简化业务流程。Fabric是该项目的子项目。也是目前Hyperledger下最为成熟和流行的一个项目。

Fabric项目具备企业级的网络安全性、可扩展性、保密性等特性，是一种模块化的区块链架构，可实现联盟链的身份管理、隐私保护、数据高效处理、智能合约等功能。具体而言，节点必须经过授权认证后才能加入，从而避免了挖矿资源开销，大幅提高了交易处理效率，满足企业级应用对处理性能的诉求。同时，为了满足灵活多变的应用场景，Fabric采用了高度模块化的系统设计理念，将权限认证模块（MSP）、排序服务模块（Ordering Service）、背书模块（Endorsing peers）、区块提交模块（committing peers）等进行分离部署，使开发者可以根据具体的业务场景替换模块，实现了模块的插件式管理。

### Fabric机理：节点分类

Fabric中的节点主要分为两大类：peer节点和orderer节点。

每个Peer节点可以担任如下多种角色：

（1）Anchor Peer（锚节点）

锚节点是在一个channel上可以被所有其他peer发现的peer，channel上的每个成员都有一个anchor Peer（或多个anchor peer 来防止单点故障），允许属于不同成员的peer发现channel上的所有现有peer。

（2）Endorser peer（背书节点）

所谓背书（Endorsement），就是指特定peer执行交易并向生成交易提案的客户端应用程序返回YES/NO响应的过程。也只有在应用程序向节点发起交易背书请求时才成为背书节点，其他时候是普通的记账节点，只负责验证交易并记账。

（3）Leader Peer（主节点）

主节点负责和Orderer排序服务节点通信，从排序服务节点处获取最新的区块并在组织内部同步。

（4）Committer Peer（记账节点）

记账节点使用基于Gossip的p2p数据分发，节点会定期跟其他节点交换信息。如果在这个过程中有节点发生故障，则会从存活的节点中删除这个节点的信息。对于故障节点，还会定时检查是否已经恢复，恢复存活的节点会更新到存活节点列表中。如果有新加入的节点，也能通过节点信息的交换获取到，添加到存活列表中，广播给其他节点。由于超级账本采用基于反熵的状态同步，每个节点周期性的和邻居节点交换保存的数据，然后对比本地数据和邻居节点所保存的数据，检查是否有缺失或者过期的数据，然后更新本地节点的数据为最新的数据，因此故障的节点重新连接到网络时会自动恢复数据。这些都能通过Gossip协议学习到，自动调整网络的拓扑结构，适应网络节点的变化，保证整个网络正常运行。

（5）Orderer（排序服务节点）

orderer负责接收包含背书签名的交易，对未打包的交易进行排序生成区块，广播给peer节点。排序服务可以采用集中式服务（solo，不适合实际生产环境），也可以采用分布式协议（目前正是发布的版本只支持Apache Kafka集群，只能实现崩溃故障容错）。

其中**主节点、背书节点、记账节点属于组织内节点，排序节点属于组织外节点**。值得注意的是作为公链，比特币、以太坊的节点必须全部连入公网，否则无法参与到网络交易中。而Fabric只需要把组织外节点（即排序节点）部署在公网中，而每一个参与其中的企业主体，只暴露一个主节点就可以了。这种巧妙的设计可以帮助企业不用大动干戈就可以用上区块链，同时还保证企业内网的安全。

### Fabric机理：通道（channel）

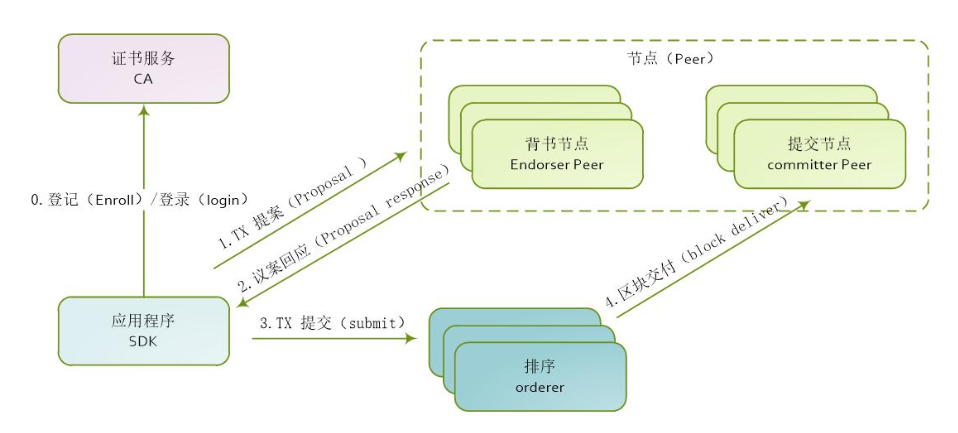
通道是Fabric中非常重要的概念，它实质是由排序节点划分和管理的私有原子广播通道，目的是对通道的信息进行隔离，使得通道外的实体无法访问通道内的信息，从而实现交易的隐私性。

目前通道分为系统通道（System Channel）和应用通道（Application Channel）。排序节点通过系统通道来管理应用通道，用户的交易信息通过应用通道传递。对一般用户来说，通道是指应用通道。系统通道与应用通道的关系如下图所示：



### Fabric机理：交易

Fabric是应用于联盟链的场景，在处理每一笔交易时，每个环节上需要对交易信息进行权限校验。Fabric交易流程图如下所示：



交易过程详细流程：

（1）应用程序客户端通过SDK调用证书服务（CA）服务，进行注册和登记，并获取身份证书。

（2）应用程序客户端通过SDK向区块链网络发起一个交易提案（Proposal），交易提案把带有本次交易要调用的合约标识、合约方法和参数信息以及客户端签名等信息发送给背书（Endorser）节点。

（3）背书（Endorser）节点收到交易提案（Proposal）后，验证签名并确定提交者是否有权执行操作，同时根据背书策略模拟执行智能合约，并将结果及其各自的CA证书签名发还给应用程序客户端。

（4）应用程序客户端收到背书（Endorser）节点返回的信息后，判断提案结果是否一致，以及是否参照指定的背书策略执行，如果没有足够的背书，则中止处理；否则，应用程序客户端把数据打包到一起组成一个交易并签名，发送给Orderer。

（5）Orderer对接收到的交易进行共识排序，然后按照区块生成策略，将一批交易打包到一起，生成新的区块，发送给记账（Committer）节点。

（6）记账（Committer）节点收到区块后，会对区块中的每笔交易进行校验，检查交易依赖的输入输出是否符合当前区块链的状态，完成后将区块追加到本地的区块链，并修改世界状态。

### 6. Fabric机理：一些名词解释

（1）证书（certificate）是Fabric中权限管理的基础。目前采用了基于ECDSA算法的非对称加密算法来生成公钥和私钥，证书格式则采用了X.509的标准规范。Fabric中采用单独的Fabric CA项目来管理证书的生成。每一个实体、组织都可以拥有自己的身份证书，并且证书也遵循了组织结构，方便基于组织实现灵活的权限管理。

（2）成员（Member）是拥有网络唯一根证书的合法独立实体。在Fabric区块链中，peer节点和app client这样的网络组件实际上就是一个Member。

（3）组织（organization）代表一组拥有共同信任的根证书（可以为根CA证书或中间CA证书）的成员。这些成员由于共享同样的信任根，彼此之间信任度很高，可以相互交换比较敏感的内容。同一个组织的成员节点在网络中可以被认为是同一个身份，代表组织进行签名。组织中成员可以为普通成员角色或者管理员角色，后者拥有更高的权限，可以对组织配置进行修改。组织一般包括名称、ID、MSP信息、管理策略、认证采用的密码库类型、一组锚点节点位置等信息。通常情况下，多个组织为了进行数据沟通，可以加入到同一个channel中。

（4）联盟（Consortium）是若干组织构成的集合，是联盟链场景所独有的结构形式。联盟一般用于多个组织相互合作的场景，例如某联盟中指定需要所有参与方同时对交易背书，才允许在网络中进行执行。

（5）MSP是Membership Service Provider的缩写，直译为成员关系服务提供者，是一个提供抽象化成员操作框架的组件。MSP将颁发与校验证书，以及用户认证背后的所有密码学机制与协议都抽象了出来。一个MSP可以自己定义身份，以及身份的管理（身份验证）与认证（生成与验证签名）规则。也就是说，在一个运行的fabric系统网络中有众多的参与者，MSP就是为了管理这些参与者，可以辨识验证哪些人有资格，哪些人没资格，既维护某一个参与者的权限，也维护参与者之间的关系。为了处理网络成员身份和身份，成员服务提供者(MSP)管理用户id，并对网络中的所有参与者进行身份验证。一个Fabric区块链网络可以由一个或多个MSPs控制。这提供了成员操作的模块化，以及跨不同成员标准和体系结构的互操作性。

（6）成员服务MS（Member Service）在许可的区块链网络上认证、授权和管理身份。在peer和orderer中运行的成员服务的代码都会认证和授权区块链操作。它是基于PKI的MSP实现。

综上所述，成员是最基本的元素，它对应的是我们Fabric网络中的Peer节点或者Order节点或者Fabric-CA。MSP就是对这些成员进行身份的管理与验证的实现。总结为一句话，成员关系服务提供者，给成员提供成员服务。这种服务是基于PKI的MSP实现的。