2019~2020 学年冬学期《区块链与数字货币》课程作业 4

应承峻 3170103456

1. Fabric 中使用何种身份验证方法和模型？

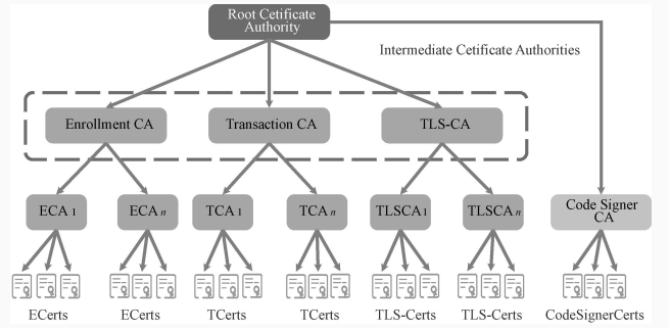
Fabric 区块链是一个许可链网络，因此 Fabric 提供了一个成员服务（MemberService）用于管理用户 ID 并对网络上所有的参与者进行认证。

区块链网络中的每一个参与者：peer，orderers，客户端应用程序，管理员等，要想参与区块链网络，都必须具有封装在 X.509 数字证书中的数字身份，这些身份确定了参与者在区块链网络中对资源的访问权限。而要使身份可以验证，它必须来自可信任的权威机构。会员服务提供商（MSP）在 Fabric 中就充当权威机构的角色。Fabric 中 MSP 默认使用 X.509 证书作为身份，采用传统的公钥基础结构（PKI）分层模型。

2. Fabric 系统实现中，成员服务 PKI 体系有哪几个基本实体组成？

如下图所示，PKI 体系由以下基本实体组成：

- Root Certificate Authority
- Enrollment CA、Transaction CA、TLS-CA
- ECA、TCA、TLSCA、Code Signer CA
- ECerts、TCerts、TLS-Certs、CodeSignerCerts



3. 什么是背书策略？简述一次交易（chaincode 调用）背书的过程

(1)背书策略是用于指定区块链节点交易验证的规则，从而来确定一个交易是否被正确的背书。当一个节点接收到一个交易时，它会调用与该交易的 Chaincode 相关的 VSCC 作为交易确认流程的一部分来确定交易的有效性。因此一个交易需要得到包含一个或多个背书节点的背书。VSCC 的背书校验需要满足：

- 背书的数量是否符合要求
- 背书是否来自预期的来源

- 所有来自背书节点的背书是否有效

(2)背书的过程：

- **客户端发送交易提议给指定背书节点：**客户端创建交易后，发送请求到其选择的背书节点，即发送一个 PROPOSE 消息到交易所选择的背书节点集合。
- **背书节点模拟交易，然后生成背书签名：**背书节点收到客户端的<PROPOSE,tx,[anchor]>消息之后，它会先验证客户端的签名，验证通过后就会模拟执行交易的内容。
- **客户端收集交易背书后并通过共识服务广播：**提交客户端获取交易的背书，通过排序服务进行广播。在一定的时间间隔内，如果客户端收到了“足够的”背书节点发回的背书消息，如果背书策略被满足，这个交易就会被认为背书成功。否则客户端就会抛弃该笔交易或者稍后进行重试。如果背书逻辑决定拒绝为这个交易背书，它则会发送(TRANSACTION-INVALID,tid,REJECTED)消息给客户端。对于有效的背书成功的交易，客户端会通过 broadcast(blob)方法调用共识服务。
- **共识服务传送区块给 Peer 节点：**在共识服务对交易进行排序并达成区块之后， 共识服务将会触发 deliver(seqno, prevhash,blob)事件，然后将这一区块广播给所有链接在 Fabric 和同一通道上的 Peer 节点，Peer 节点在收到共识服务广播的区块之后会进行两类校验。