**Lecture 4-10 Notes**

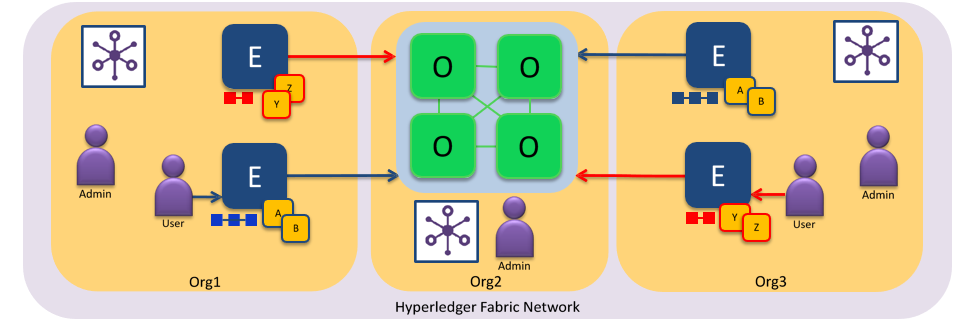
**The identity management and membership aspects of Hyperledger fabric**

The identity management and membership aspects of Hyperledger fabric, this is going to be delving into some of the primitives that Hyperledger fabric uses for some of the security and privacy properties that need to achieve for enterprise applications.

**Organizations**

* Notion of organization: In the enterprise world you can think of these organizations as legal entities, they all have business that they are running. These organizations can be recognized with identities that they are provided on the blockchain network.
* Each organization for instance will have our membership service provider for the identities for the users belonging to that organization.
* The organization can also define a set of administrators, these administrators will be the ones who are running peers, join the channel they might be installing chain code on behalf of these peers, they might also be executing ordering services.
* For one or more channel each organization can participate in one or more channels in the block chain network and all that information is captured in the network itself.
* There will be one membership service provider per organization, it is possible to have one MSP serving multiple organizations and it is also possible for one organization to have multiple MSPs those are possible but the recommended use is to have one MSP per organization. Each organization is going to have an id on the blockchain.

**Consortium Network**

****

* Here is an example of a consortium network. There are 3 organizations in this consortium. Organization 1 and 3 are the ones that are running peers. Organization 2 provides only the ordering service in this example.
* Organization 1 is running 2 peers, organization 3 is also running 2 peers. Each of these organizations have their admin and one or more users and there are chain codes or smart contracts deployed on the channel.
* In this network there are 2 channels the blue and the red. There are chain codes that are deployed on both the channels. A and B on the blue network and Y and Z on the red network both of them are using the same ordering service that org 2 is running.
* Org 2 has an administrator who is in charge of running this ordering service. The ordering service is going to maintain 2 chains of blocks. One blockchain is going to be for the blue channel one for the red channel.

**Membership service provider**

* There is a distributed network with a set of identities, there are identities that are provided for every concept or entity in the network.
* There are identities for peers and identities for the orders, the ordering services here and the peer is here. Each of them is issued identities they will use these identities to communicate with each other.
* There are client applications and we can provide our identities to the client applications, Here could be a peer, for the peer there will be an admin, for the order there will be an admin.
* That bunch of administrators who are managing this network themselves and those administrators have identities and these identities are issued by some certificate authority.
* This can be the fabric certificate authority; it is issuing these identities, or it could be an external certificate authority.
* There is a TLS which is Transport Layer Security, this is used for encrypting all the communications across the network. In the peers to order communication, user to the peer communication, between peers and chain codes on that communication all of it is secured through TLS.

**Transport Layer Security**

* It is a cryptographic protocol it is a standard that secures all communications over a computer network.
* It provides 2 important properties.
  + - * The notion of privacy
      * The notion of data integrity
* What do we mean by privacy? Is that only a certain set of nodes or certain set of people should be able to see what that communication is, that is the notion of privacy.
* The data integrity is when a node sends communication to another node the recipient should get the same data as was sent by the sender ok. So, that data should not get changed or over the course of the communication.
* TLS uses symmetric cryptography to encrypt the data that is transmitted.
* If this encryption, who does not have this key will not be able to decrypt this message and will not be able to know what this communication was about. So, that provides privacy.
* Only the participants who hold the key typically it is just 2 entities A sending a message to B that communication is encrypted.
* It uses public-key cryptography to authenticate the identities of the communicating parties, this provides a part of the data integrity to say that only A is sending this message and B can verify the fact that it was.
* There are message integrity checks that are included to prevent loss or alteration of the data. Every communication in fabric between client and peer, between peer and peer and order, between orders themselves, all of this is secured using TLS. So, it provides this privacy and data integrity for all communications.

**User Identities**

* Every user in the network is going to be issued an identity, an enrollment certificate, the enrollment certificate has 2 paths.
* One is it has a private key, and this private key has to be private to that user nobody else should know what that private key is and the user will be using that private key to digitally sign transactions there submitting onto the network. That is the private key and it is stored in a secure key store.
* The second part of the identity is a signcert which is a public x.509 certificate in the fabric implementation, this public certificate will include is your public key. Using this public key will be able to validate whether it was indeed this user who signed that transaction. The public key is used to for that validation and it also includes certain attributes that the certificate authority might provide to the user.

**Admin Identities**

* The admin identity is very similar in concept to the user identity, every administrator has a local MSP to store their identity and every admin is connected to a local MSP.
* As the user identity it has a private key that is stored in a key store and it has a public x.509 certificate that forms signcert.
* It could have TLS credentials and it could be using a hardware security module to store and unsigned transaction.

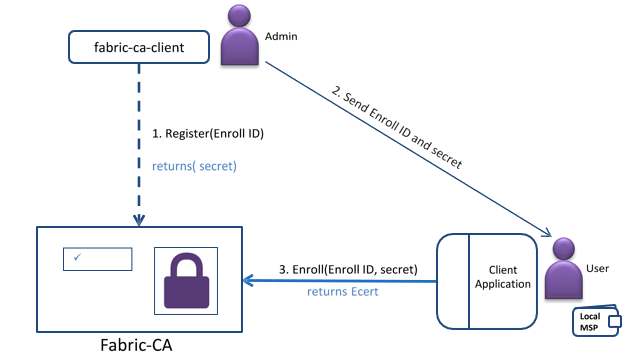
**Peer and Orderer Identities**

* The peer and I order identities it is similar it has a private key and a public x.509 certificate; it has a local MSP attached to the peer which holds these identities.
* The peer MSPs can identify authorized administrators, It could have one or more administrators for this peer and the admincerts are also included.
* An organization who is running the peer can designate one of users as an administrator and that administrator will be included in the admincerts.
* The admin apart from that can store the public certificates of CAs that it will recognize. This is needed to recognize the user certificate was issued by a certificate authority, a certificate authority that user certificate is actually signed by the CA.
* The cacerts and there are also certification revocation lists, these are crls and this revocation is important over a period of time to manage, which are legitimate users which are not.

**Channel MSP Information**

* The channel MSP has information about which peers and which orders can join that channel and this can be dynamic.
* It is possible that some peers join the channel at a later point of time other peers might leave the channel all that is dynamically configured in the channel MSP.
* The channel MSP is also query able, a new peer joining the channel can query the channel MSP to find out which other peers are participating in this channel.
* It also determines which client applications can connect to this channel and can perform transactions on this channel.
* It also stores all the configuration blocks in the ledger, any new peers joining the channel any orders joining the channel are all configured as transactions on the blockchain.
* There are again the certificate authorities who are recognized by this channel for authenticating the identities they are all signed by the CA.
* The CAs public certificate for validating that and again you could have certification revocation lists like before.
* It is an important thing here is that it does not include any private keys for identity. So, this channel information is all public information of who are the administrators, who are the CAs, what are the peers and authors as part of this channel. It does not have any private information.

**New User Registration and Enrollment**



* A new user enrollment work- registration and enrollment.
* The organization is a part of this network, they have an administrator and that administrator must first the administrator has to register.
* The administrator calls the register function with a identity, to say I want to register this new user with this blockchain.
* It contacts the CA and the CA returns a secret.
* Then the administrator sends this enrollment id and the secret to the user.
* This forms the long-term identity that the user will be using to transact on the blockchain. Once it has received these credentials, the secret also includes the certificate that they need to use.
* Once user received these credentials, they will then use that secret to enroll with the fabric CA and that returns the enrollment certificate for them.

**Use Case on Hyperledger Fabric**

**Use Case: Interoperability of Assets**

**Description:** Interoperability of assets means the exchange of assets among a group of people.

**Problem statement**: If an organization requires 20,000 units of asset B but instead owns 10,000 units of asset A, it needs a way to exchange asset A for asset B. Though the current market might not offer enough liquidity to fulfill this trade quickly, there might be plenty of liquidity available between asset A and asset C, and also between asset C and asset B.

*Now there are market limits on direct trading between A & B, so what can be the probable solution?*

**Solution:**  In this case, a chain network connects buyers with “buried” sellers, finds the best match (which could be buried under several layers of assets), and executes the transaction. So basically a business network of a group of individuals can be set up on the Hyperledger Fabric and the assets can be exchanged among the buyer and the sellers.

**Difference between Bitcoin, Ethereum and Hyperledger Fabric**

