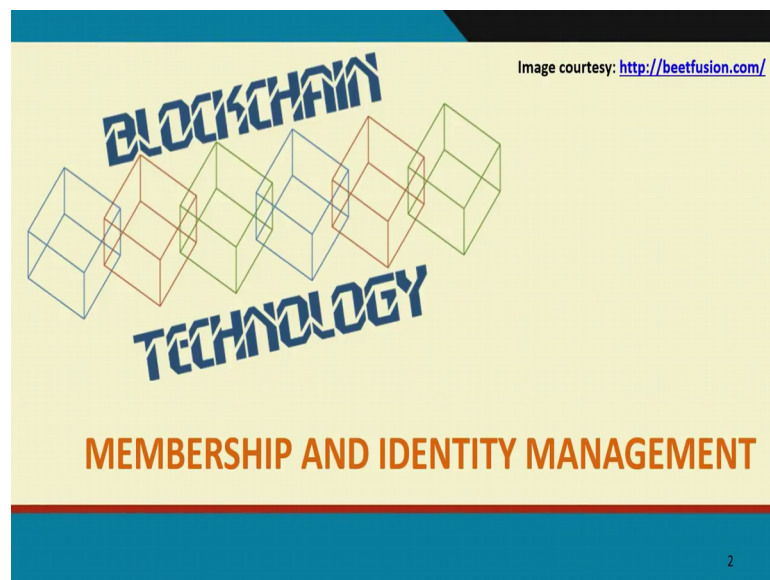


**Blockchains Architecture, Design and Use Cases**  
**Prof. Praveen Jayachandran**  
**IBM Research, India**  
**Prof. Sandip Chakraborty**  
**Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture - 23**  
**Fabric - Membership and Identity Management**

Hello everyone welcome to the next lecture of our Blockchains course. So, in this lecture we are actually going to go much more deeper into hyperledger fabric itself.

(Refer Slide Time: 00:22)



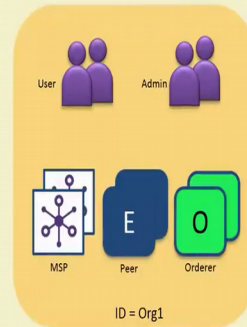
Looking at some of the identity management and membership aspects of hyperledger fabric so, this is going to be delving into some of the primitives that hyperledger fabric uses for some of the security and privacy properties that we want to achieve for our enterprise applications.

(Refer Slide Time: 00:40)

# Organisations

Organisations define boundaries within a Fabric Blockchain Network

- Each organisation defines:
  - Membership Services Provider (MSP) for identities
  - Administrator(s)
  - Users
  - Peers
  - Orderers (optional)
- A network can include many organisations representing a consortium
- Each organisation has an ID



Getting into the details now so, first of all I think an important notion to understand is the notion of organization. In the enterprise world you can think of these organizations as legal entities, say they all have business that they are running. And we can recognize these organizations with identities that they are provided on the blockchain network.

So, each organization for instance said it will have our membership service provider for the identities for the users belonging to that organization. So, we have users of that organization. The organization can also define a set of administrators. So, these administrators will be the ones who are running peers, maybe the ones who are helping these peers, join the channel they might be installing chain code on behalf of these peers. Or they might also be executing ordering services. So, what are the different components.

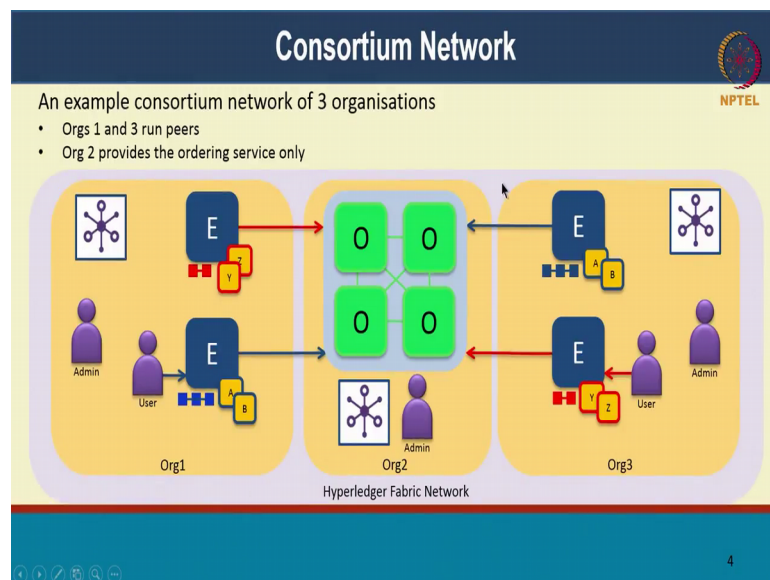
So, you have administrators and users and the organization could be running one or more peers in the network some might be endorsing peers, some might be only committing peers and optionally they can also run ordering nodes right.

For one or more channel so, each organization can participate in one or more channels in the block chain network. And all that information is captured in the network itself. So, each channel configuration in the genesis block or in subsequent blocks where gets modified, the organization information is also captured there. The network can include of course, many organizations and it could be a consortium ok.

So, I can let us say a group of 10 banks might form a consortium, and each bank can be represented as an organization on the network. So, this is a boundary that we define in 2 of identity. And these identities of these organizations are separated out using the membership service provider.

So, typically there will be one membership service provider per organization. Where although 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 with the recommended use is to have one MSP per organization. And like I mentioned you each organization is going to have an id on the blockchain.

(Refer Slide Time: 02:54)

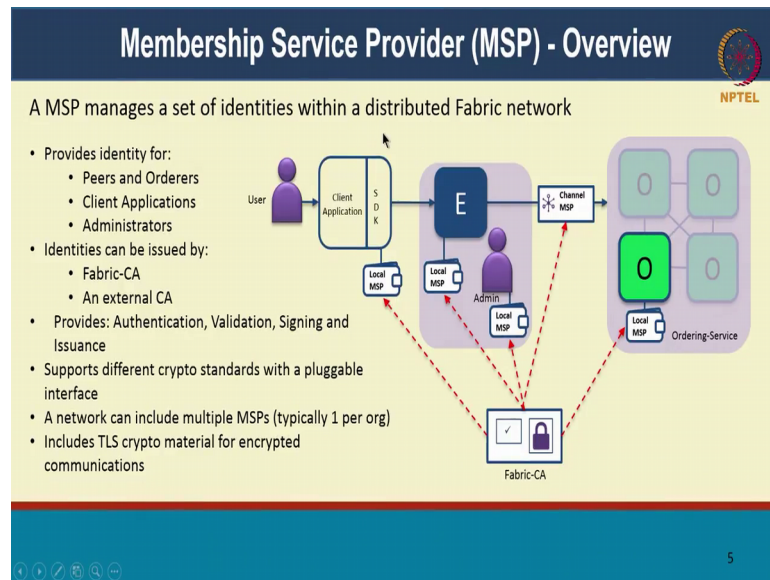


So, here is an example of a consortium network. There are 3 organizations in this consortium. Organization 1 and 3 are the ones that are running peers. Organization 2 provides only the ordering service in this example.

So, organization one is running 2 peers is shown here. Organization 3 is also running 2 peers. Each of these organizations have their admin and one or more users. Likewise, all 3 also has the same. And there are chain codes or smart contracts deployed on the channel. So, in this network there are actually 2 channels the blue and the red. And there are chain codes that are deployed on both the channels. So 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 or 2 is running.

And there are 2 has an administrator who is in charge of running this ordering service right. And 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. And the transactions on these 2 as I mentioned are going to be kept separate.

(Refer Slide Time: 04:01)



So, going to the membership service provider what; that means, is there is a distributed network with a set of identities. And there are identities that are provided for every concept or entity in the network. So, there are identities for peers there are identities for the orders. So, the ordering services here and the peer is here. Each of them are issued identities they will use these identities to communicate with each other.

There are client applications and we can we provide our identities to the client applications also. So, there could be a peer for the peer there will be an admin for the order there will be an admin. So, that bunch of administrators who are managing this network themselves and those administrators have identities. And these identities are issued by some certificate authority.

So, this can be the fabric certificate authority, there are that is issuing these identities or it could be an external certificate authority, that is issuing these identities. So, as long as the root CA is recognized by the network you can bring in any certificate authority of your choice. Now what are the benefits of having all of these identities right; what sort of properties are we providing? Of course, there is authentication. So, every time a user

transacts on the blockchain they are authenticating themselves by signing the transaction. And this sign is verified by the peer or any other entity on the in the network. So, the peer is going to validate this signature provided by the user. So, that is the validation part.

So, if you are not a registered user on the network, you cannot perform transactions or you cannot see what the blockchain status, you cannot read that set of channels you cannot see what channels are available. So, none of that information will be available to you. You have to be authenticated on the network to transact on the network.

It also has the ability for you to sign information for instance the user will sign transactions send it to the peer. The peer will execute the transaction and when it endorses it is actually going to sign the endorsement. Likewise, the ordering service when it creates a block and sends it to the peers the each block is going to be signed by the ordering service.

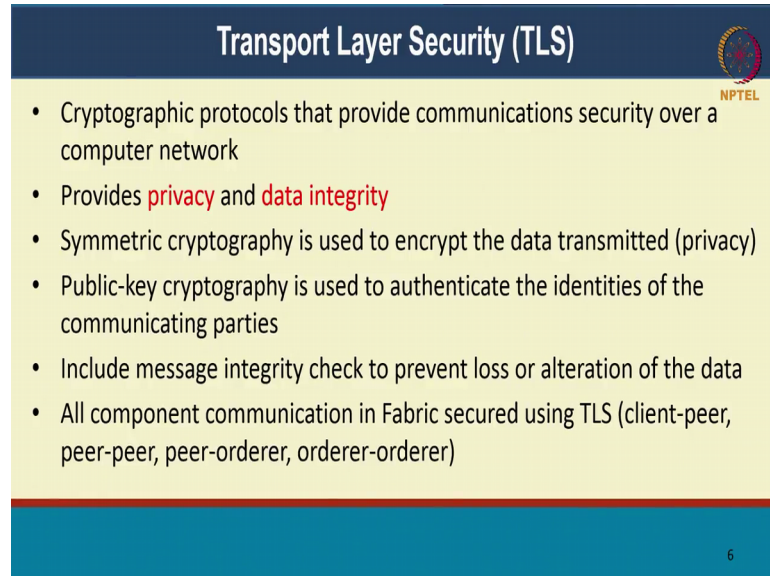
So, you can validate that all of this is coming from the authorized entity to perform that (Refer Time: 06:19). So, if someone else they say one of the peers tries to maliciously sign a block and send it all the other peers will know that this was did not come from the ordering service it came from somebody else. So, it will reject that message. So, signing and issuance are all possible because of the security framework that we have through the membership service provider. Those MSP can support different crypto standards.

This is meant as a pluggable interface. And the main reason for this is that different applications might need different security properties that might be provided by different CAs difference crypto standards. So, all of that becomes pluggable and it is also the fact that security itself as a domain as a field of knowledge has been flowing so, rapidly that over a few years you might find better security standards better ways of securing our systems and we want to be able to allow that.

And so, all of these are provided as pluggable features and a network then have multiple MSPs, like I mentioned we want to the recommended way is to have one MSP per organization. So, based on the number of organizations you have, you might have that many MSPs in the network. And there is also TLS which is Transport Layer Security and this is used for encrypting all the communications across the network. So, the peers amongst themselves when they communicate peers to order communication, user to the

peer communication between peers and chain codes that there on that communication all of it is secured through TLS.

(Refer Slide Time: 07:57)



**Transport Layer Security (TLS)**

- Cryptographic protocols that provide communications security over a computer network
- Provides **privacy** and **data integrity**
- Symmetric cryptography is used to encrypt the data transmitted (privacy)
- Public-key cryptography is used to authenticate the identities of the communicating parties
- Include message integrity check to prevent loss or alteration of the data
- All component communication in Fabric secured using TLS (client-peer, peer-peer, peer-orderer, orderer-orderer)

6

So, what is really this TLS? It is a cryptographic protocol it is actually a standard that secures all communications over a computer network. So, it provides 2 important properties. It provides the notion of privacy and the notion of data integrity. So, 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 so, 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 so, that is the data integrity.

So, how is this achieved? TLS uses symmetric cryptography to encrypt the data that is transmitted. So, because if this encryption, no one who anyone 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.

So, only the participants who hold the key typically it is just 2 entities A sending a message to B that communication is encrypted. And because of the fact that only A and B have this key only they will know what the contents of this communication are kind of this communication is.

So, that is the privacy part of it. And it uses publicly cryptography to authenticate the identities of the communicating parties. So, this again 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 actually A that sent it and that is achieved use it using public key crypto cryptography.

And there are message integrity checks that are included to prevent loss or alteration of the data. So, let us say the communication between A and B there might be packet loss. There might be an pack our trying to manipulate, this message in the middle in the network. So, to prevent all of that there is a message integrity check. So, think of it as the equivalent of like a hash or a checksum. So, you can check that the message that you received was exactly what the message that was sent.

So, that is the message integrity is check and all of this together forms the protocol itself. And 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.

(Refer Slide Time: 10:30)

**User Identities**

Each client application has a local MSP to store user identities

- Each local MSP includes:
  - **Keystore**
    - Private key for signing transactions
  - **Signcert**
    - Public x.509 certificate
- May also include TLS credentials
- Can be backed by a Hardware Security Module (HSM)

user@org1.example.com	
keystore	<private key>
signcert	user@org1.example.com-cert.pem

So, getting a little more into what these identities are. So, I told you that every user in the network is going to be issued an identity, an enrollment certificate right. 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. So, 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, but like I mentioned other crypto standards can also be used. This public certificate will include is your public key. So, everyone will know will know using this public key will be able to validate whether it was indeed this user who signed that transaction. So, the public key is used to for that validation. And it also includes certain attributes that the certificate authority might provide to the user.

For instance, some of the attributes might be to say that this user let us say for me, I let us say I have a digital certificate. My public certificate will include the fact that maybe I belong to a organization IBM research. It might have other attributes saying I am actually a researcher and it might have certain authorizations certain roles that I have on the network.

For instance, if this is a supply chain blockchain network, then it might even have a rule that says I am an exporter in this network. So, those sorts of attributes can also be embedded within the certificate. And we can use those attributes to authorize transactions on the network. So, the smart contract can include aspects saying only a user who is an exporter who has an attribute called exporter will be allowed to perform this transaction.

So, anyone else let say someone else who is let us say a carrier or a freight forwarder in this network, will not be able to perform that particular transaction. Like invoking that particular spot contract function. So, all those capabilities are then possible through attributes embedded in your certificate. And it also optionally includes your TLS certificates, TLS credentials and that is important for let us say the peer when it is for the peer identity the peer needs a TLS credential for it to be communicating with other peers and orders in the network and all of this can be backed by a hardware security module where these keys are securely stored.

And the HSM can be used to can be it is a hardware model and that can be used to assign transactions without anyone else any other component in your system getting access to the private keys right. So, that is the user identity itself.

(Refer Slide Time: 13:19)

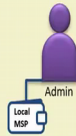


## Admin Identities

NPTEL

Each Administrator has a local MSP to store their identity

- Each local MSP includes:
  - Keystore**
    - Private key for signing transactions
  - Signcert**
    - Public x.509 certificate
- May also include Transport Layer Security (TLS) credentials
- Can be backed by a Hardware Security Module (HSM)



admin@org1.example.com	
keystore	<private key>
signcert	admin@org1.example.com-cert.pem

8

The admin identity is very similar in concept to the user identity. And every each administrator has a local MSP to store their identity. So, every admin is connected to a local MSP. And just 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 that is forms it is signcert.

And again it could have TLS credentials and it could be using a hardware security module to store and unsigned transaction.

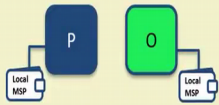
(Refer Slide Time: 13:50)

## Peer and Orderer Identities

NPTEL

Each peer and orderer has a local MSP

- Each local MSP includes:
  - keystore**
    - Private key for signing transactions
  - signcert**
    - Public x.509 certificate
- In addition Peer/Orderer MSPs identify authorized administrators:
  - admincerts**
    - List of administrator certificates
  - cacerts**
    - The CA public cert for verification
  - crls**
    - List of revoked certificates
- Peers and Orderers also receive channel MSP info
- Can be backed by a Hardware Security Module (HSM)



peer@org1.example.com	
admincerts	admin@org1.example.com-cert.pem
cacerts	ca.org1.example.com-cert.pem
keystore	<private key>
signcert	peer@org1.example.com-cert.pem
crls	<list of revoked admin certificates>

9

So, what do the peer and I order identities look like? Again 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. And in addition the peer and MSPs can identify authorized administrators. So, it could have one or more administrators for this peer and the admincerts are also included.

So, for instance an organization who is running the peer can designate one of its users as an administrator. And that administrator will be included in the admincerts. And there are specific functions that only the administrator can do for instance joining a particular channel can only be performed by that administrator user. If a regular user who is not an administrator tries to perform that transaction it will be denied by the network.


And the admin apart from that it can also store the public certificates of CAs that it will recognize. So, this is needed to recognize let say a user if the user certificate was issued by a certificate authority, a particular certificate authority then that user certificate is actually signed by the CA. So, we need the public certificate of that CA to be able to validate users who are connecting to this peer. So, that is part of the cacerts and there are also certification revocation lists. So, these are crls and these revocations are important to over a period of time manage, which are legitimate users which are not. And even for a legitimate user it is advisable to change your certificates every now and then for security purposes.

So, maybe you hold your certificate for a certain length of time and then you will revoke that certificate and have a new certificate issued for the same user right. For security purposes it is advisable to rotate your certificates. So, you can have certification revocation lists to say which certificates have been revoked and should no longer be admissible on the blockchain. And peers and orders also receive the channel MSP information. Since the channel also has a MSP the peers and orders will know which channels they are connected to. So, that is also happening through the MSP in a secure manner.

Again the peer and ordered identities can be backed by a HSM.

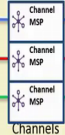
(Refer Slide Time: 16:03)

## Channel MSP Information



Channels include additional organisational MSP information

- Determines which orderers or peers can join the channel
- Determines client applications read or write access to the channel
- Stored in configuration blocks in the ledger
- Each channel MSP includes:
  - **admincerts**
    - Any public certificates for administrators
  - **cacerts**
    - The CA public certificate for this MSP
  - **crls**
    - List of revoked certificates
- **Does not include any private keys for identity**



ID = MSP	
admincerts	admin.org...pem
cacerts	ca.org1.e...
crls	<list of re...es>

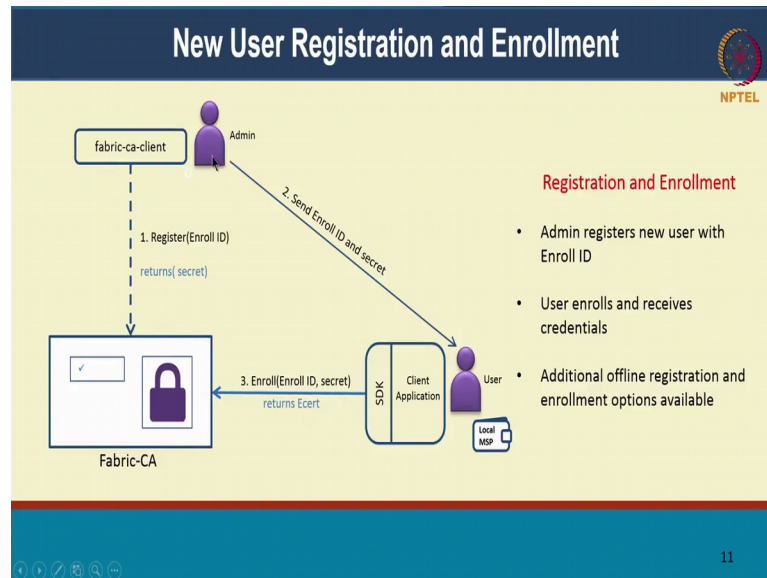
Now, what does the channel MSP look like? So, like I mentioned every concept in blocked in the hyperledger fabric is associated with an MSP. So, the channel MSP has information about which peers and which orders can join that channel and this can be dynamic. So, it is possible that some peers join the channel at a later point of time other peers might leave the channel all that is dynamically configured in the channel MSP. And the channel MSP is also query able. So, 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. So, like I mentioned any new peers joining the channel any orders joining the channel are all configured as transactions on the blockchain. And if the channel MSP stores that information as well, what is the latest channel configuration will be part of it. The channel MSP also includes administrators. So, who are the administrators for this channel for instance it could be multiple organizations administrators who are recognized as administrators for a channel right. So, they might determine when to admit a new peer and other changes in the channel configuration.

Of course, there are again the certificate authorities who are recognized by this channel for authenticating the identities they are all signed by the CA. So, you need the CAs public certificate for validating that and again you could have certification to vocation lists like before. So, 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 can 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.

(Refer Slide Time: 17:54)



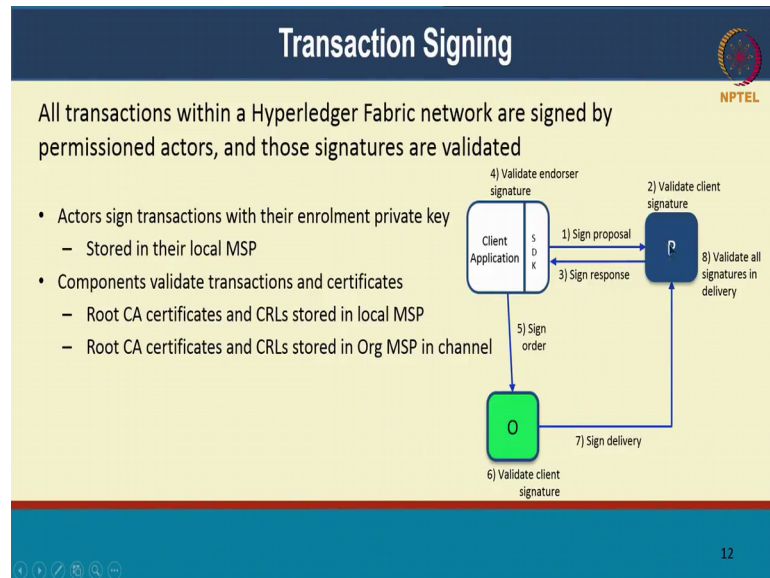
So, how does a new user enrollment work; registration and enrollment. So, let us say I am a new user on this network. So, I am part of some organization. So, there is I need to talk to some admin, maybe my organization is already part of this network. They have an administrator and that administrator has to first the administrator has to register.

So, the first the administrator register when you are creating when the peers joins the network itself the administrator has to be registered. And subsequently it will only be the administrator who can register new users from that organization. The administrator calls the register function it will with a particular identity, and will say I want to register this new user with this blockchain.

So, it contacts the CA and the CA returns a particular secret. So, then the administrator sends this enrollment id and the secret to the user. So, this forms the identity the long term identity that the user will be using to transact on the blockchain. Once it has received these credentials. So, the secret also includes the certificate that they need to use once I have received these credentials they will then use that secret to enroll with the fabric CA, and that returns the enrollment certificate for them.

So, that will be the long time long term certificate that the user will use to transact on the blockchain to. Just recap administrator has to register the user the administrator then sends the enrollment id and secret to the user, the user then contacts the CA with that enroll id and secret to obtain an enrollment certificate and you can then use that enrollment certificate for transacting on the blockchain.

(Refer Slide Time: 19:31)



So now once you have got the enrollment certificate you can use that for transaction signing. All the transactions submitted on the blockchain have to be signed by permission users on the network. And those signatures are validated. Users sign transactions with their private key that is that private key will be part of the local MSP of the client. The peer will have the public key and there will be able to validate the signature.

So, the user is going to sign the proposal and the peer will sign the response. And will validate the signature and it will sign the response there is the 3 here. So, the user signed the proposal submitted to the peer; peer executed before executing the transaction it is going to validate the client signature. And when it creates response to be sent to the client application it is going to sign the response with the peer's private key.

So, then the client application can validate the peer signature to make sure the legitimate peer has signed this. It will then sign the entire endorsed transaction it might do this from with multiple peers you collect all the signatures and it will then sign the transaction to

be sent to the ordering service. The ordering service will validate the client signature again and it is going to when it sends the block to the peer it is going to sign the block there is the 7 here. The peer can again verify that it was indeed the order that signed and sent the block to the pure and it will validate that order a signature and only then it will validate the transactions and commit the transaction. So, at every step every communication you will see that there is a signature and a validation performed on the blockchains.

So, this provides for secure communication across all the entities in the blockchain network.

(Refer Slide Time: 21:14)



The slide is titled "Fun Reading" and features the NPTEL logo in the top right corner. It contains a bulleted list of four Wikipedia articles related to security and digital identity. The articles are: Transport Layer Security (TLS), Digital Identity, Digital Signatures, and X.509 Certificate. Each item includes a blue hyperlink to the respective Wikipedia page. At the bottom of the slide, there are navigation icons and the number 13.

- Transport Layer Security (TLS), Wikipedia article: [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)
- Digital Identity, Wikipedia article: [https://en.wikipedia.org/wiki/Digital\\_identity](https://en.wikipedia.org/wiki/Digital_identity)
- Digital Signatures, Wikipedia article: [https://en.wikipedia.org/wiki/Digital\\_signature](https://en.wikipedia.org/wiki/Digital_signature)
- X.509 Certificate, Wikipedia article: <https://en.wikipedia.org/wiki/X.509>

With that I hope you have a good sense of how the membership service provider works, how the security secure communications work, how signing of transactions and verification of transactions work across the network. So, there is a good set of reading material again I hope you go through some of these. If you have not seen transport layer security before I would encourage you to read the Wikipedia article it gives you a good overview this is our standard practice in the internet today, and for any kind of secure communications.

So, I would encourage you to read that. So, even beyond just knowing about block chain will help you learn some of these concepts again the concept of digital identity is something much beyond just block chain it is used in multiple systems today. So, you

can read up again from Wikipedia there is a very good articles on what digital identity is. Using the digital identity, you can have digital signatures, again excellent Wikipedia articles on that I would encourage you to read that for sure. And a specific implementation of these identities and signatures is the x.509 standard for certificates and again this good reading material on that.

So, with that I hope you get a good overview of how we have use traditional security concepts. Although I say traditional they are the most cutting edge technology that we haven we have today for security and how that is used to secure communication and transactions on hyperledger fabric so.

Thanks a lot for your time. So, we will see you in the next lecture.