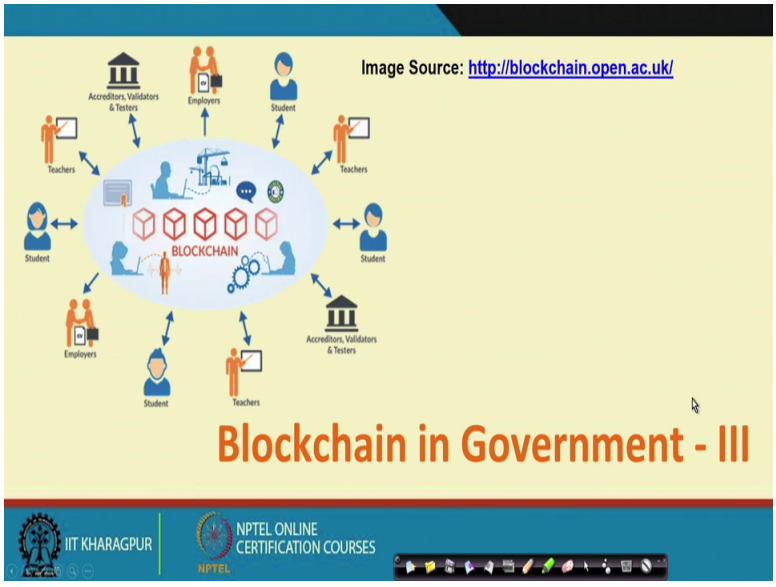
Blockchains Architecture, Design and Use Cases
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 41
Blockchain in Government – III (Digital Identity)

Welcome back to the course on Blockchain. So, in the last two lectures we have looked into different use cases of a blockchain usage for government applications. So, we have broadly looked into various government applications where blockchain can be utilized. So, in the next couple of lectures we will broadly look into three different use cases in details, where we look into that how different companies startups or different project proposals; they are utilizing this blockchain technology for developing application for government uses.

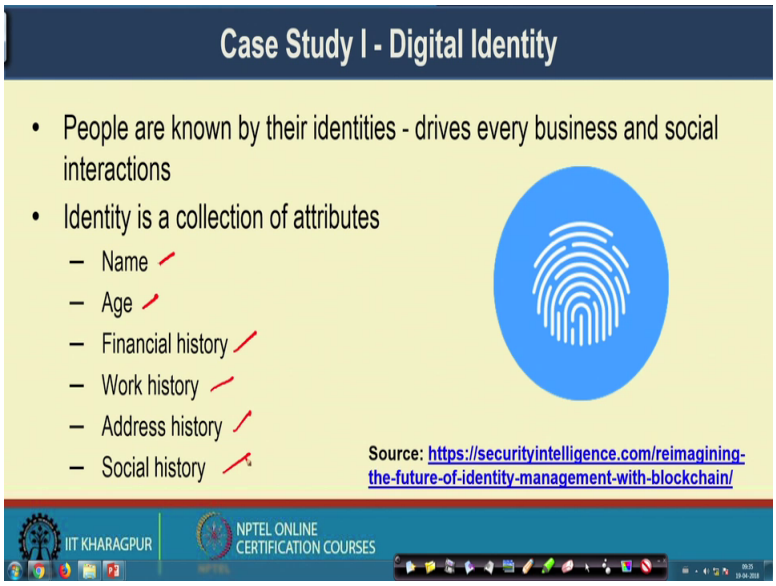
So, we will primarily look into three different aspect, the first one is using blockchain for digital identity. The second one is using blockchain for taxation and the third one is using blockchain for land registry record management.

(Refer Slide Time: 01:23)



So, let us start with our discussion on blockchain usage in government where we look into that how the blockchain technology can be utilized for the digital identity management.

(Refer Slide Time: 01:35)



So, in one of our earlier lectures you are looking into that how blockchain can be widely utilized for digital identity management. Here we look into some specific use cases and what we have seen that digital identity that is something a debatable concept like how you can utilize or what type of attribute or parameter can be utilized to identify ones identity. And, the different privacy concept or the privacy concern which are associated with your identity.

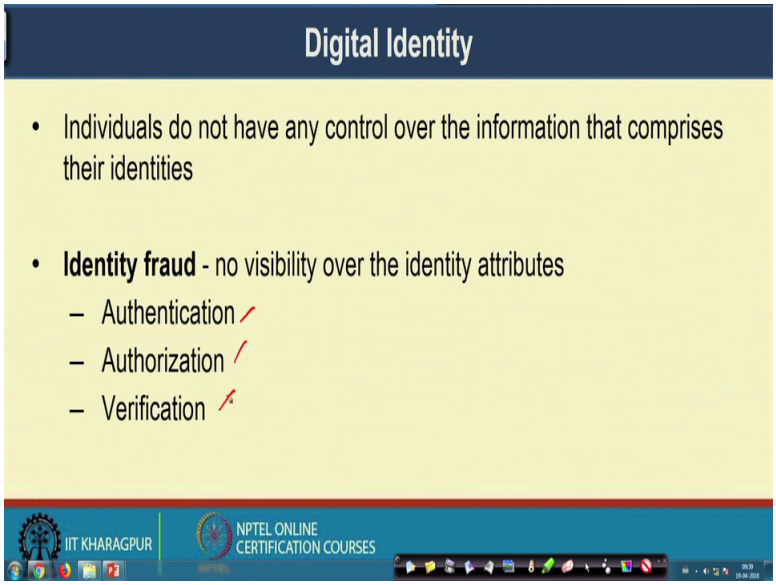
So, in case of digital identity that people they are known by their identities, this identity can be different for business applications and for the social applications. So, for a particular business people can use one particular form of identity to express himself or to express herself. Whereas, for several other social interactions, other identities like the nickname or that kind of attributes can be utilized for identify a people. Say if you broadly look into these aspects of identity from different domains.

Say whenever you are going for a foreign trip, you need to have a custom clearance at the airport, during that time your passport is your identity. On the other hand whenever you are interacting with your friends over say Facebook or this kind of social networking platform during that time your name, your nickname, your profile picture this constitutes your identity. Now, that way if you look into this identity concept this identity is a collection of various attributes ranging from the name of the person, the age of the

person. Say for a banking transactions your financial history can be used as an your identity.

Your work history can be used as an identity for your employment purpose, your address history can be a part of your identity say whenever you are applying for certain government services. Your social history can be your identity whenever you are interacting over a social networking platform. So, from this wide concept let us look into the aspects of digital identity or why digital identity are preserving digital identity is important. In general for different kind of applications where we utilize this concept of identity nowadays, the individuals they do not have any control over the information that comprise their identities.

(Refer Slide Time: 04:30)



So, different applications or different platforms can utilize, different types of attributes to identify yourself or identify an individual. Say for example, as I have mentioned that whenever you are moving to a foreign country and you need to pass through the custom clearance, during that time your passport is your identity and whenever you are in a foreign land during that time your passport and your visa is your identity.

On the other hand the concept of identity is completely different whenever you are in a social platform. During that time people identify yourself by looking into your social networking profile, by looking into your name, attribute with whom you have interacted; what are your different post in your social networking platform. So, all this different

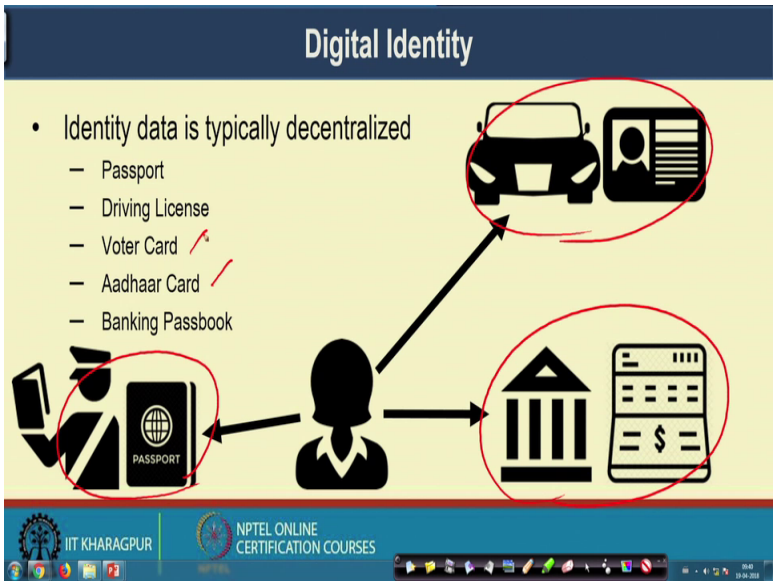
concept together they constitute our identity, but the message that I want to convey at this part that as an individual you do not have any control over this particular digital identity architecture that which attributes will uniquely identify you. So, because of this we observe there different kind of identity fraud where the users do not have any particular visibility on identity attributes.

So, the identity fraud can come from authorization perspective, the identity fraud can come from authorization perspective, where false person or a intruder can get can get authorized as a normal person because, of this identity fraud. For authentication purpose the identity fraud can be utilized, where you a false person can get authenticated to a server if they are able to access your identity.

So, say for example, in a social networking platform some time it happened that your some attacker or some intruder tries to impersonate one profile and in that case they create a same profile with the name and possibly by stealing the profile picture from someone else and impersonate that person to create a false or fake Facebook profile. And in that case this kind of authentication problem comes into picture that the other persons in the social networking platform they do not have any control or it is difficult for them to find out whether this particular social networking profile is a original profile or is a fake profile.

So, nowadays you see many such news or many such concern regarding this identity fraud due to in person (Refer Time: 07:22) attack or this kind of authentication attack kind of problem. And, similarly the verification purpose where the environment becomes difficult to verify the original identity of a person. So, as I have mentioned that your identity data is typically decentralized.

(Refer Slide Time: 07:43)



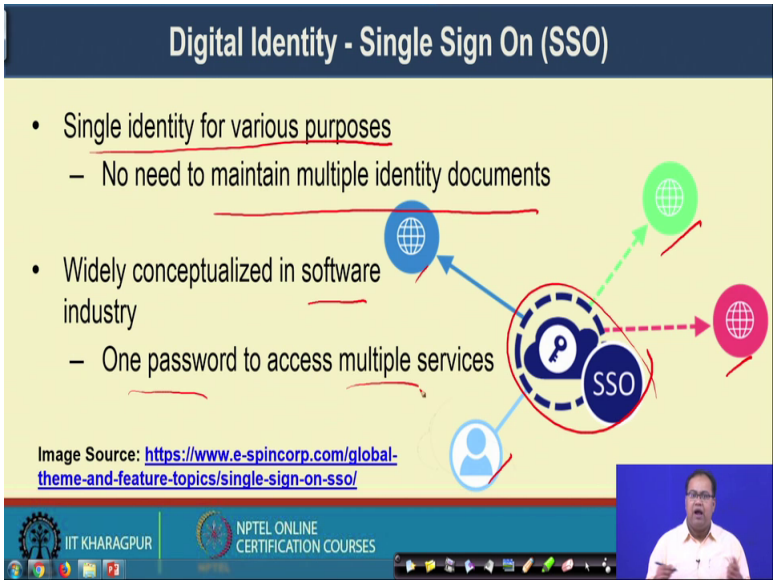
So, different organization they make different control of your passport, different control of your identity data. Say for example, in a custom environment you have your passport which is utilized as an identity data, say whenever you are on road and you are driving a car during that time your driving license become your identity say whenever you are going to a bank in that bank your bank passbook becomes your identity and now for some social networking services your Aadhaar card may become your identity. Whenever you are going for participating in a general election during that time your voter card can become your identity.

Now, that way for the same person different organization imposes different form of identity. And they maintain their own identity database. So, that way this identity data is typically decentralized and it is managed by multiple authoritative domains, but many of the times it may happen that you need to prove your identity through the identity information that was provided by a separate organization.

So, for example, whenever you are going to a bank to open a new account during that time you have to give your identity proof and during that time you can form, you can fill up the form called KYC or know your customer form where you have to provide your details and at the same time some kind of identity proof. So, during that time you may provide your passport as an identity proof, you may provide your driving license as an identity proof. So, any kind of photo identity card can work as identity proof that way the

multiple organizations need to transfer the identity information from one place or one organization to another organization. And those organizations need to verify the identity information for authenticate or for authorizing a person to provide some kind of services.

(Refer Slide Time: 09:52)



So, from this concept of having problem with the your physical identity where you need to maintain multiple identity cards or multiple identity certificates. So, we are gradually moving towards the domain called digital identity in the domain of digital identity what is named as a single sign on.

So, a single sign on is something like that where you have one identity information and that identity information can be utilized to get services from multiple partners or multiple organization. So, the single identity is utilized for various purposes. So, in that case you do not need to maintain multiple identity documents; so, the same identity that can be utilized to obtain the services from multiple service organizations. So, this concept is known as a single sign on SSO.

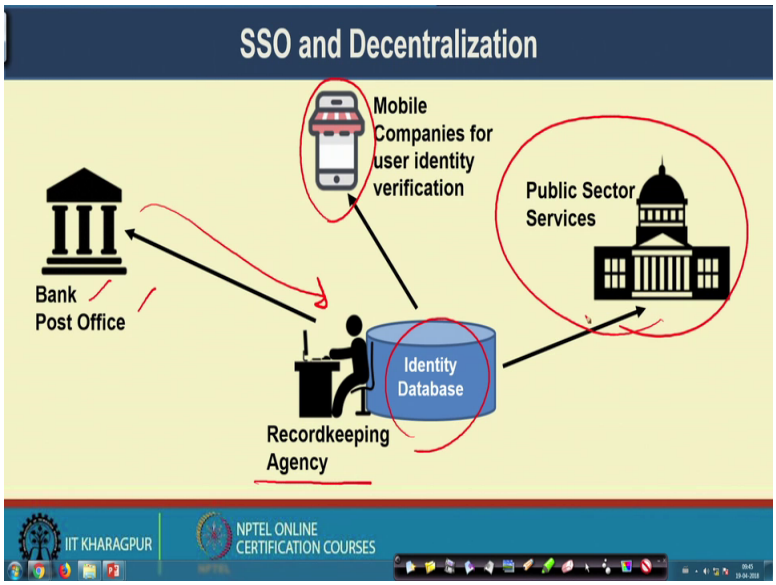
Now, the concept of a SSO is although in a physical environment we do not use this SSO till now at least in India, we are trying to utilize that by the means of Aadhar card or that type of identity certificate, but it is already widely conceptualized in the software industry. So, it is just like that you have a single password and using that single password you can access multiple services. So, you have you have multiple service providers or

multiple vendors. So, using that single sign on identity element you can you can be able to login to multiple services.

So, one typical example can be come from your Google user ID and password. So, possibly you have seen that using your Google email ID and the password you can get services from multiple service providers at least for the services which are provided by Google or which are provided by Google associated services like YouTube Google drive, different kind of Google forms all these Google provided services. And at the same time some third party services can also be utilized or where you can get the authorization by utilizing your Google ID and the password.

So, in that case you can utilize the Google your Google login to make a login to that particular service portal where that service portal get your ID verified from Google and they get your certain information with your consent from Google. So, this is Google is a kind of example of a single sign on or SSO where you have a single identity or a single user ID and password that can be utilized for getting multiple services.

(Refer Slide Time: 12:35)



Now, let us look into that how this SSO and decentralization can be can become a trouble for managing ones identity. So, here you have your identity in the identity database. So, the record keeping agency like the Aadhar center UIDAI they are maintaining your identity data. Now, whenever you are going to bank or post office to getting certain

services during that time your subscribing with your Aadhar data and the bank and post office they will get it validated from this record keeping agency.

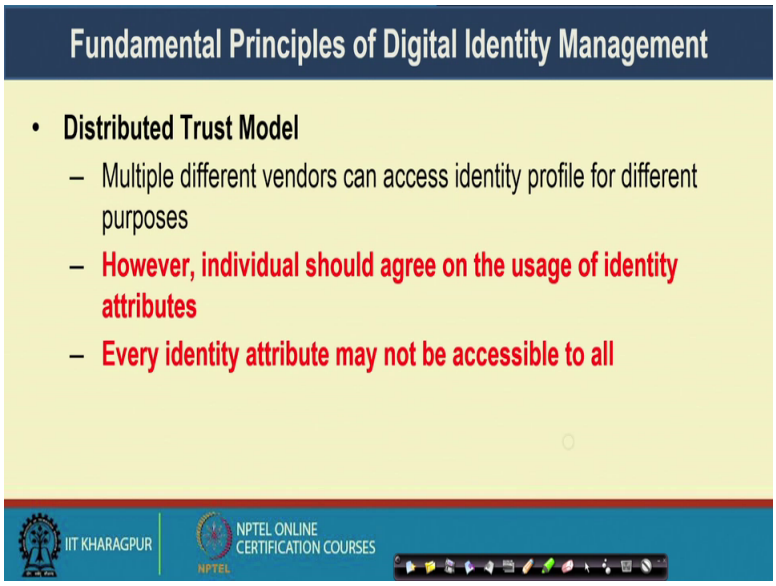
So, they will they will get it validated from the Aadhar database that whatever document you are submitting to them that document is ended correct document which will be able to get you authenticated for obtaining the service. Similarly whenever you are applying for some mobile SIM card, the mobile company may ask for your identity card like your Aadhar card and from your Aadhar card they may get verified or get authenticated you to find out that well you are a citizen of India and you are authorized to get a Indian SIM card.

Similarly, the public sector services. So, we have seen like various public sector services nowadays it utilizes the Aadhar card concept. So, this public sector services. So, whenever you want to obtain certain service you submit a copy of your Aadhar card which provides your identity. So, that service agency they get it again verified from the UIDAI.

So, in general what is happening here that your Aadhar data or your identity data that is getting decentralized into multiple hand into multiple authoritative domain or authorization domain, where everyone gets it verified individually. Now, ideally what is happening the same copy of the identity data is getting distributed among multiple authoritative domain or multiple authorization domain. And, when it happens during that time the possibility of identity fraud becomes more severe where there will be a high possibility that certain kind of identity fraud would be there.

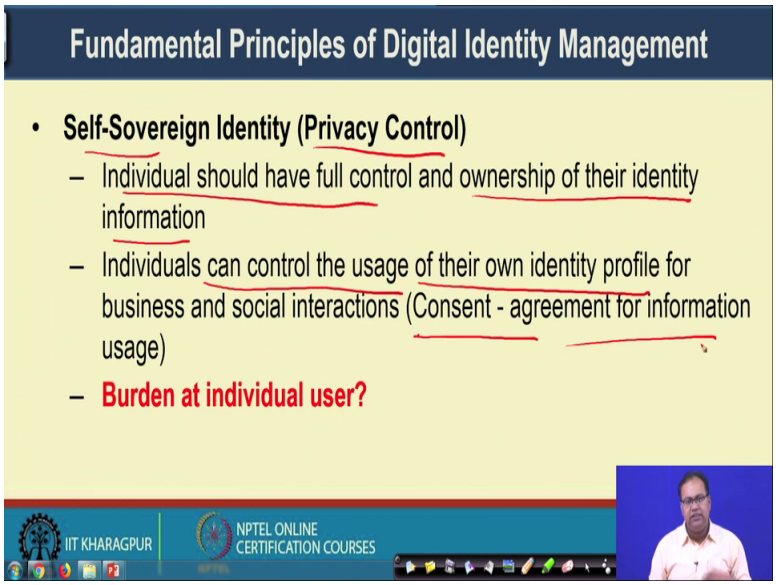
So, it may happen that well your record keeping agency is not revealing your identity data the identity data is not getting tampered or not getting accessed from the record keeping agency. Rather the third party organizations which are keeping a copy of your identity data from their information can get reveal or can get public. So, that way your identity information which we normally consider as a private information are that may get public or that may get reveal in the open and which may increase the possibility of identity fraud for several aspects.

(Refer Slide Time: 15:47)



So, in the concept of this Digital identity Management, there are two fundamental principles that we will talk about one is called a Self Sovereign Identity and the second one is called a Distributed Trust Model.

(Refer Slide Time: 15:51)



So, let us look first look into this concept of Self Sovereign Identity. So, the concept of self sovereign identity it is utilized to provide privacy control to the identity data of individuals.

So, the self sovereign identity says that individuals should have full control and ownership of their identity the information. So, it is just like that whatever identity information you are revealing to public as it is your private information. So, you are the only person who will manage this entire information. So, it is not like the way we use today the example that I had given earlier that individuals do not have any control over their identity attributes.

So, the self sovereign identity directly attacked this principle or directly countered this principle saying that well to make a privacy control over the identity information individuals should have full control over their identity information and they will have the ownership of their identity information. So, they would be the person to say to others that see to verify me you can utilize this part of your or this set of attributes of my identity information. For a different service they may authorize other person to use another set of identity attributes from the entire identity database.

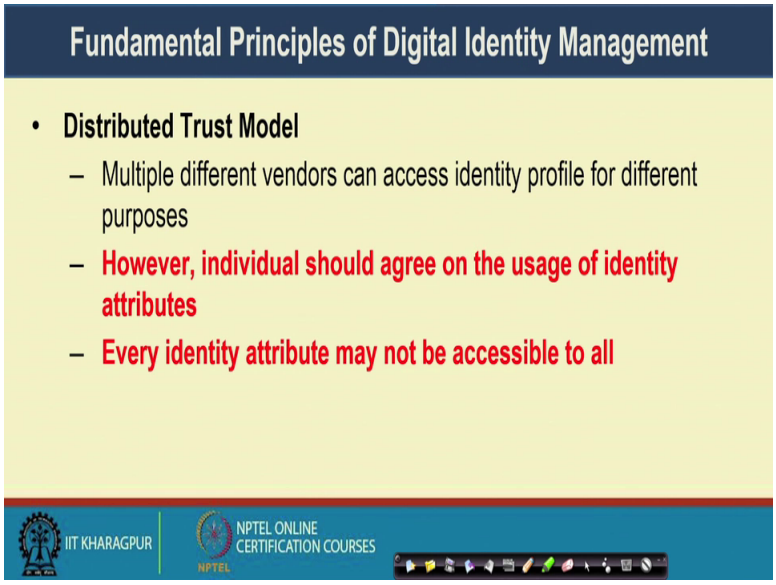
So, the first principle is that individuals should have control and ownership the second is the individual can control the usage of their own identity profile. So, here we say it is like consent or the agreement for information usage where the individual should say that well this part of my identity information can be utilized for a social interaction for a Facebook, but this part of my identity information should not be revealed to one service agency or one third party agency.

So, individuals can say that well whenever I am providing my passport information to one user for verification I can only provide this part of the purpose passport information just like my photo and the name. I will not provide my address, mobile number and all these details to this particular organization or this particular agency for verifying me. So, this particular concept where the user can give access to different attributes to different users or different at different authoritative domains or agencies to identify one user or for identification purpose or for authorization purpose that particular concept we call is that as a Self Sovereign Identity.

But as you understand that this is going to be a burden to the user, like now the user need to manage their own identity profile and they have to selectively say that well this part of my identity attribute can be utilized for getting service a whereas, another part of my identity information can be utilized to get service b. So, user need to control that what

part of the identity information can get revealed or can get verified by this third person or third party agencies. So, it seems like a burden, but with the help of blockchain we can solve this will come that how we can do that.

(Refer Slide Time: 19:17)



The next part is the Distributed Trust Model. So, the distributed trust model says that whenever your identity information is going to multiple vendors or multiple agencies, they have certain access to your identity profile for different purpose. But, this individuals or this agency should agree on the usage of that the identity attribute.

So, it is just like that whenever you are providing your copy of the passport to our agency for verifying your identity, say that agency will not reveal your information to any other. One example can be like say you are going to some places for a for having your holiday trip.

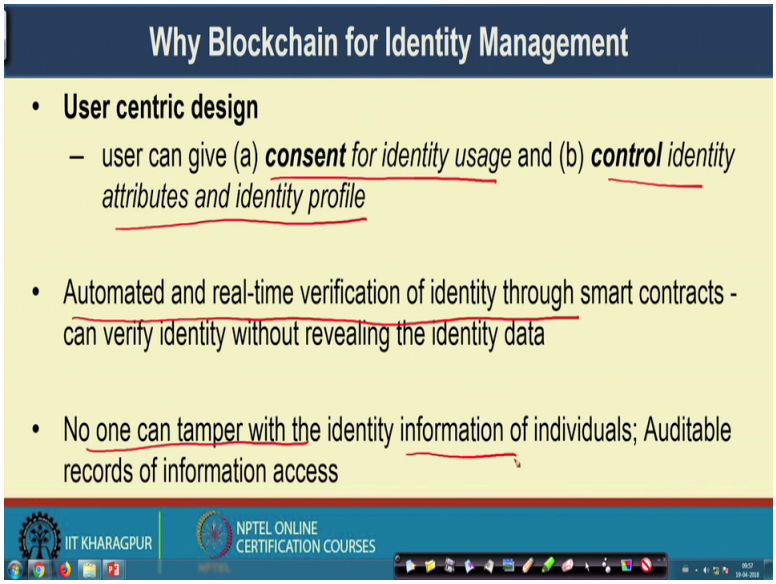
So, whenever you are going to that place you have booked a hotel. So, whenever you are making a check in to your hotel the hotel person will ask for your identity card or photo identity card. Now, whenever you are providing your photo identity card to that hostel at that hotel authority you have a kind of trust relationship with that hotel authority that that hotel authority is not going to reveal that information to any other agency for any purpose.

So, this kind of identity fraud nowadays you have seen a lot recently we had this Facebook identity fraud, where the Facebook data was share to it Cambridge analytic and Cambridge analytic used that identity information for controlling many of the aspects, global aspects including elections at certain countries. So, these kind of debates are coming up now all this identity fraud can be prevented. If we can set up a kind of trust model among individuals who are going to have access over this identity data.

So, whenever you are providing your identity information to a third person. So, the third person will not be able to define that information to any other person. And, in that case if they are going to reveal it as an individual or as an authority or as an owner of that identity information, you will get notified that your information is going to send to some third party and even before sending it to some third party a consent will be taken from you.

So, every identity attribute may not be accessible to all. So, that is why this distributed trust model ensures that your identity information without your consent that is not going to reveal from to any third party; other than the ones with whom you have agreed to share the information.

(Refer Slide Time: 22:00)



Well, now let us see with this kind of identity problem which are coming because, of this identity management problem and the second one is this distributed trust model that how blockchain can help us in identity management. So, first of all what blockchain can

provide us? Blockchain provide us a way of user centric design. So, that was the first problem of our life like whenever as an individual you are going to manage your identity attribute during that time it becomes a burden for you. Now, the blockchain can actually make it easy to manage this entire digital identity; so, with this user centric design that user can give first the consent for identity usage and the second one is the control for identity attributes and identity profile.

So, this constant and control are the two important terms that comes in this user centric design principle where as an end user you can give consent that your identity information would be utilized for this many purposes. Whereas, the control says that well you will have a control that which part of your identity attributes or which part of your identity profile will be shared for the authorization purpose. That is the first advantage of utilized blockchain for digital identity management, I will come to a use case to explain this in further details.

The second is the Automated and real time verification of the identity through smart contracts. So, it is just like that for identity verification you have written certain small code in the form of a smart contract. So, the smart contract get can get automatically executed and can purify your identity without actually revealing the identity attributes. Say one typical example can be like for your Aadhar data say a mobile agency can wants to verify your Aadhar data, verify your identity with the help of other data.

So, what the mobile agency can do that the mobile agency can set up a smart contract with you and that smart contract will have access of your identity attributes your say Aadhar number and certain other biometric data. And, this mobile that particular smart contract the code can be written in such a way so, that the data which is being provided to the smart contract it is getting obfuscated.

So, the data of obfuscated means that you are providing the data in a hidden form and the third part is like that mobile companies they will not give actual access to the data. So, the smart contract in that way they can get obfuscated copy of your data and get it automatically verified from your Aadhar agency or the UIDAI and then only send a yes-no response to the mobile companies saying that whether the identity got verified or whether the identity was not got verified.

So, that way this smart contract with the help of a smart contract you can hide your identity data, you do not need to provide a photo identity card to the mobile company or do not need to upload your Aadhar data to the mobile company; rather the smart contract can automatically fetch your identity data from your mobile phone based on your consent. And, it can execute certain codes to obfuscate the data and then provide the data to some third persons. And, the third one is that advantage a blockchain is that no one will be able to tamper with the identity information of individuals.

So, what identity information you are providing that particular identity information whichever is there in your blockchain data that information no one will be able to tamper. Because, blockchain ensures this tamper proof way of keeping the records are keeping the transactions and that also becomes auditable because, you can see from the blockchain that how your identity data got accessed by multiple vendors.

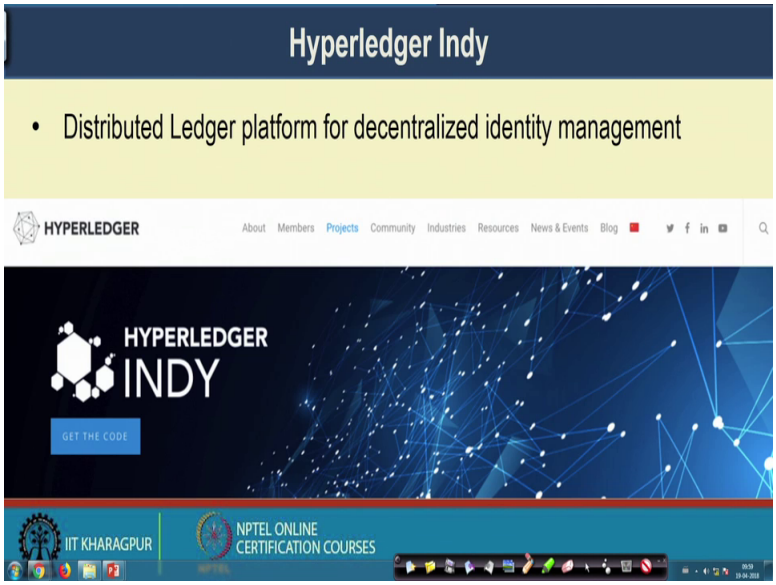
So, whenever multiple vendors or multiple agencies are going to access your blockchain data. So, going to access your identity data hide a blockchain a transaction record is put into double action and then by looking into those transactions record as an individual you will be able to find out that how your identity data was actually utilized for multiple purpose. So, if someone is sending your identity data to some third person first of all you will be able to prevent it by thereby in certain smart contracts which will have the code for preventing data, unnecessary leakage of data to the third parties.

And the second thing is that even if there is no smart contract and only the access log is put into the blockchain by looking into the access log you will be able to find out that, if you have shared your identity data with the hotel management whether that hotel management has shared that data further with any other third parties or not. So, that way the blockchain can help us to have the manage of identity data in these three aspects. The user centric design, the automated and the real time verification of the identity to the smart contracts and the third one is that providing a tamper proof auditable environment, where no one will be able to tamper with the data.

But the data is available in the form of transaction over blockchain through which you will be able to verify as an individual, that how your data has been utilized for or how your data has been shared in the among multiple agencies or multiple domains. Well so,

that is the broad idea about the problem of digital identity and how digital identity can be or what is the advantage of blockchain to manage digital identities.

(Refer Slide Time: 28:23)



So, in the next class we will look into one example of this which we call as a hyperledger indy, which is a four core which is a project under hyperledger platform. So, this hyperledger indy provides a distributed ledger platform for decentralized identity management. So, in the next class we will look into details that how hyperledger indy can be utilized to have or to manage your digital identity with the help of this blockchain or with the help of this distributed ledger platform. So, see you all in the next classes.

Thank you.