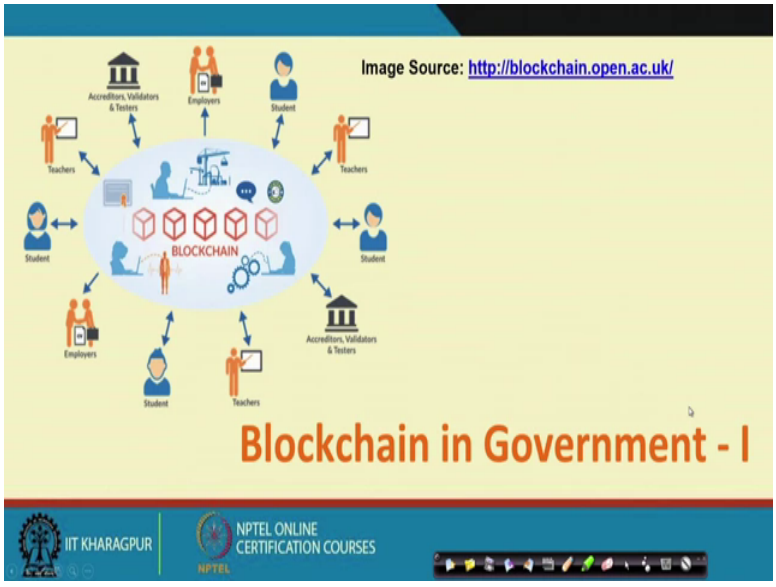
Blockchains Architecture, Design and Use Cases
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 39
Blockchain in Government – I (Advantages)

Welcome back to the course on Blockchain. So, hopefully by this time, you got a good grasp of, the theoretical concept behind blockchain along with both the permission list and the permission model of blockchain. And hopefully you got a good demo of how to implement blockchain protocol and write your own public ledger and smart contracts using this hyper ledger platform or better to say the Hyperledger Fabric platform that a Praveen has taught to you.

So, I guess that by this time you have, written certain small programs on blockchain and you have written certain smart contracts and you have a good idea about the power of blockchain and smart contract in the context of business platform. Also, during the last lecture, Praveen has given you a brought, overview of different industry use cases for blockchain. And you have looked into that supply chain management and various other financial or nonfinancial usage of blockchain technology from the perspective of an industry.

(Refer Slide Time: 01:29)



So, in this talk we will look into the blockchain from the government perspective that how this blockchain technology can give you ubiquitous or a uniform computation platform to execute different government applications. And can develop a smart environment or smart governance system by incorporating different computing technologies together including blockchain, artificial intelligence, data driven analytics and many others.

So, we will keep this discussion mostly non technical and we will look into several use cases along with different kind of examples, from different countries that how you can apply the blockchain technology to make the life of a people better. So, it will give you a aspects of using blockchain for public good on different computation platforms. So, let us look into a little details about where government can utilize this blockchain platform.

(Refer Slide Time: 02:37)

So, a broadly if you look into this concept of blockchain this entire domain of blockchain is particularly interesting or particularly useful when you have multiple organization or multiple institution under different authoritative domains and they want to share certain data among themselves. Or certain information among themselves which need to be validated, need to be audited or you want certain level of security, on top of that share data as an example, just think of like you want to send an email over a network whenever you are sending an email over a network.

You do not actually bother whether the person is in USA or the person is in Canada or the person in some eastern countries like say Singapore. What you really bother is the address of that person, by email ID of that person, and you directly send that ID over the network. Now, in this environment the whole architecture is useful because you have a controller a central control like, the email platforms which can talk with each other and their communication is not dependent on the border of a specific country. Now, on the other hand just think about a scenario of a postal in.

So, think of a use case where you want to send a postal email from say India from some small village of India to some place in say Canada. Now, if you want to do this kind of postal transfer the entire thing is handled by at least two different government: the Indian government the Indian post and the Canadian post the Canadian government. So, whenever you have this multiple organizations and multiple organizations are handling some kind of assets all together during that time the problem comes, like you need to trust the other party for the information.

So, if your parcel or if your post get lost from Canada and you are at India you cannot directly blame the Canadian post or you do not have any way to verify that why or at what location that post got stolen or the post got altered or something has happened with your post. So, the only thing then which you have to rely is on the information that is provided to you or better to say that is provided to the Indian post by the Canadian post. So, that way they are need to be certain levels of trust relationships among multiple governments, multiple individual authoritative domains and collectively they build up this entire system.

So, this postal delivery, works good in a practical environment because, this individual postal agencies they completely trust each other there is certain level of trust that if, I am delivering a post from Indian post to the Canadian post the other in will be responsible enough to deliver the post to the final destination. Another problems which comes in this entire picture is the difference of rules between these two government or the this two agencies.

So, Indian post they have their own set of rules or regulation, on the other hand the Canadian post they have their own set of rules and regulations. Now, if you want to bring them to a common platform it becomes very difficult say as such if, certain post get lost

whenever, you are sending them among multiple organization you cannot blame one person or proving something on that particular environment is really difficult because, you do not have access to the global data.

So, from that particular view or from that particular perspective this kind of blockchain technology is interesting because, it can take the idea beyond this individual borders of the countries or better to say individual border of the organization or the different authoritative domains. Now, if you look into the government perspective the government needs to maintain multiple assets in together. So, those assets can be in the digital form or can be in a printed form or can be in a paper form. So, here I have tried to listed down a few.

(Refer Slide Time: 08:01)

So, the government need to maintain the daily operations and activities of the government. So, daily operations and activities of the government in different government assets like land records, the building records, different aspects of the building the municipality need to give the information about the building they are age how old individual buildings are what are what is the current condition the civil condition of a building all these details need to be maintained. Say in the details of the people, details of the government, say different government workers, different organization or the institutes the records of the people, different business transactions.

So, the government need to deal with multiple business partners and need different aspects. So, different industries who are they are for say the supply chain management the defense industry. So, that way, the government on day to day basis they have to keep a relationship with multiple such agencies and they need to perform this kind of transaction. Now, the question comes that, how will you keep the record for those transaction?

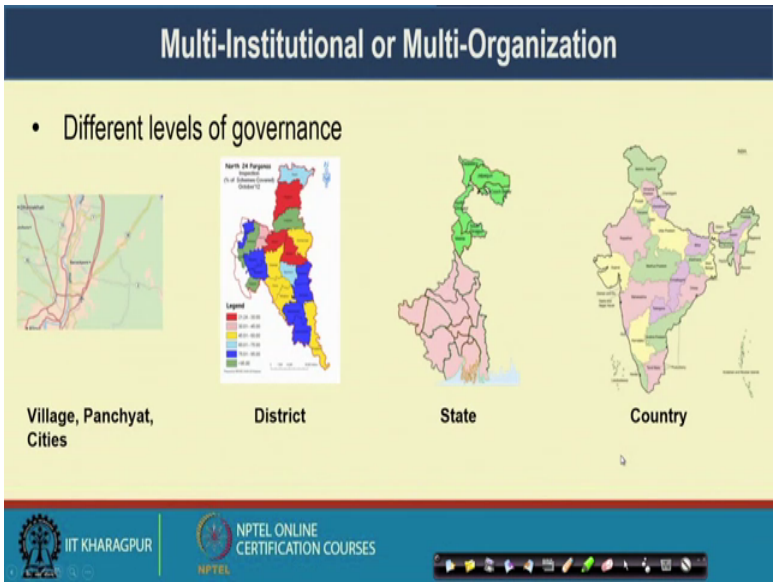
So, if you keep the record for those transaction in a paper format it is always vulnerable if, you keep it in the digital format then, who is going to host that particular information. Say today if the Indian government is having a business partnership or a business relationship with Walmart which is a private agency then, this transaction information who will be maintaining. So, one way is the government is maintaining his own part of the transaction.

And Walmart will maintain their own part of the transaction and then if, started dispute comes then that dispute need to get resolved by the auditors by the law makers in the that will go to the court and you know that it takes years of time to get it resolved. Because, proving something or proving that something bad has happened or something wrong has happened that is very difficult under this kind of mark the organizational scenario.

When the information is distributed among multiple parties now, if you want to keep all the information to a central database which on which the government can insert their transaction as well as, Walmart can also insert their transaction. So, that with this architecture the first problem is the cost like, you need to pay a huge amount of money to that third party the second problem is like you need to rely on the services provided by the third party. So, it is just like that the cloud hosting platform if, tomorrow it crushes then, all the transactions are nowhere.

So, you will not be able to recover all these transactions or you will not be have any way to validate the recover the, validate the correctness of the recovered transactions. So, those are the specific problems that a large institution like, a country government need to face on their day to day basis. So, blockchain can provide the ubiquitous or overall platform over this architecture to build or to make a kind of relationship among multiple such organizations altogether. So, let us see, some use cases that how it can be done well.

(Refer Slide Time: 11:54)

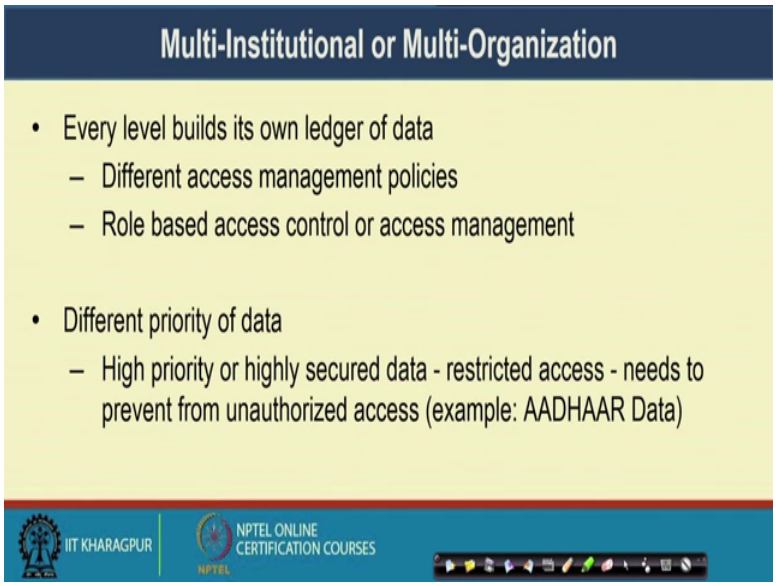


Now, whenever you look into this governance platform. So, you have different level of governance architecture. So, that is why, we call it as a multi-institutional or multi-organization. So, you have different village, panchyats then, you have the district government then, you have the state government on a large scale and on a country level scale you have the central government. And all this governments so, the state government has started relationship with the Central Government the district magistrate has certain relationship with the State Government. So, the funds are being transferred from the central government to the state government, from the district level government to the individual gram panchyats or individual city center.

So, on the that the corporation level all those individual or government organization and you need to track that how this individual assets are moving from one hand to another and then, you also need to track that how individual money that is given to different level of government they are being spent. Now, whenever you are writing it on pen and paper as I you understand that it is always vulnerable it depends on the individual. So, if the individual worker gets compromised which, it can be highly possible in an open environment if, individuals are getting compromised then the entire system may fall down.

So, we want to build up a relationship we want to develop an technical system which will help you to prevent this kind of malfunction or cheating or frauding inside the system.

(Refer Slide Time: 13:45)



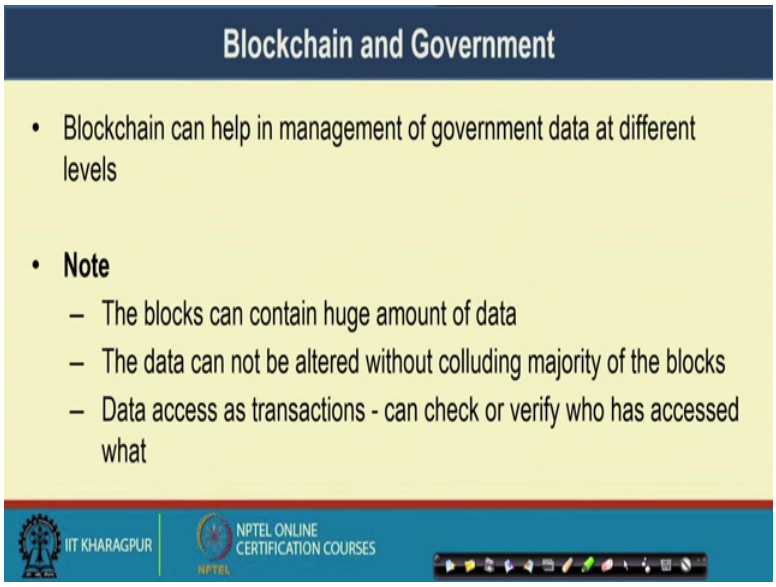
So, every level of government they build their own ledger of data and that data has different access management policies it has role based access control or the access management certain people are valid for accessing certain part of the data and not other part of the data. So, this ways somehow we try to manage this entire data all together, but as you move or as you can read from the daily newspaper that with this kind of architecture the frauds or the scams are very common and whenever there it is very difficult to prove that, someone has done certain frauds and it is also difficult to detect that who has done the fraud.

So, in this particular architecture, blockchain can play a good role and also in this architecture we have different priority of data. So, you have high priority data which need to be highly secured it need to have restricted access you need to prevent it from unauthorized access one example is the Aadhaar data in Indian context on which we have a lot of debate nowadays, whether your Aadhaar data is all secure or not.

So, Indian government is already looking into the aspect of securing the Aadhaar data with the help of blockchain. So, they are exploding these different possibilities that can be there for securing the data, but this entire blockchain environment that can give you a nice architecture where it is it is like that the entire system is tamper proof. So, whenever you write something on the blockchain, you cannot revert it back or you cannot claim that I have not written it ok. So, that is the entire platform or deceptive technology that

blockchain provides which can be utilized for multiple Government applications. So, individual blocks in a blockchain they may contain huge amount of data such kind of data.

(Refer Slide Time: 15:51)



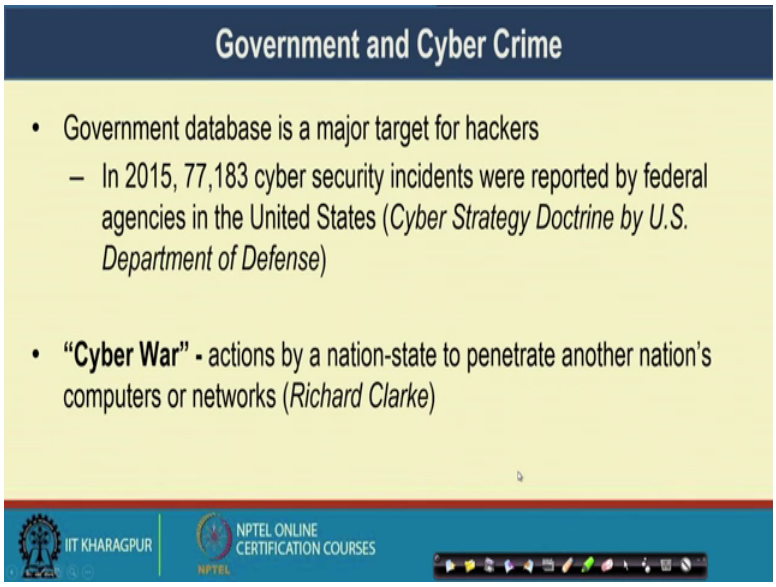
So, this data it cannot be altered without colluding majority of the blocks and the data access you can also keep the data access as a part of your blockchain. Where, individual data access is like a transaction say if, company A has access the Aadhaar data of person B then you can represent this entire thing as the form of a transaction and you can put it in the blockchain. Now, if you make an architecture like every Aadhaar data access deep to go via blockchain.

So, if you want to get access to the data Aadhaar data you have to first include a record to the transaction if that record gets committed or that record get validated that transaction record get validated by the blockchain consensus protocol then only you will be allowed to further access the data once, once the particular transaction gets committed that way with this particular architecture you can ensure that whenever someone is going to access the Aadhaar data.

There are multiple parities in the consensus protocol will validate that whether this person is actually authenticated to access the Aadhaar data or not and also once that person access the Aadhaar data person or institute that access the Aadhaar data. Then that person or institute will never be able to deny later on that it has not access the data

because, the data or the access transaction has been logged into the block chain which revertible you cannot change it later on or later on you cannot make a demand that I have not accessed it.

(Refer Slide Time: 17:45)



So, well we can use these block chain for the government platform because government data base it is always a major target for the hackers. So, there was a report from Cyber Strategy Doctrine by U.S. Department of Defense, we have reported that in 2015. So, this report was published in 2015. In 2015 around 77,183 cyber security incidents that were happened on top of the different federal agencies under U.S. government and Richard Clarke he made a nice term called "Cyber War" and a idea of this Cyber War like that one nation it is trying to penetrate the database of another nation and trying to steal the data for the admission for controlling different activities of these nations.

So, recently you have this different kind of data scam like, when this Facebook data, it got public or Facebook got actually share the data with some third agency which actually used that agency to provoke the election of different countries. So, this kind of news which are coming regularly on the news media it is yet to validate the correctness of those new but, it is very difficult inherit messages that it is very difficult to prove the validity of this kind of news or to say something against that news that this has not been happened.

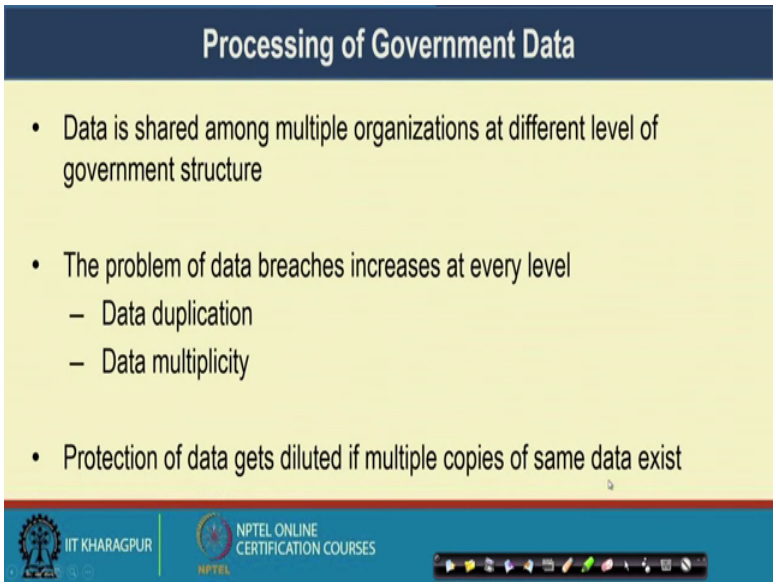
Because, there is no such log which actually, tells you that whether that happened or not and to analyze that log you need to have a huge number of cyber security expert. So, need to look into different transactions or different data transfer that have been over happened over the internet and from there they have need to find out that the data that have been shared to Cambridge Analytica by Facebook or a what type of utilization or how that data is actually being used. But, all this problem can be prevented if, the data is there in the blockchain or if, the data is accessed where the block chain because, you are actually making a public ledger or a public log of all the transactions which are being happened on this technology well.

(Refer Slide Time: 20:12)

So, I have just taken some newspaper articles which talks about different kind of privacy breach. So, this Facebook privacy breach, that was the recent attack which was there and then this debate on the Aadhaar data security which is currently a hot topic. So, we cannot say something in the for of this particular data breach or against this data breach it is yet to prove.

But, this kind of debate is there and proving that is difficult and if, you look into the Wikipedia page of list of data breaches you will find out that a large number of data breach that has happened over the past few years that is been listed in Wikipedia and that would be a nice exercise for you to look into what happened over the years there.

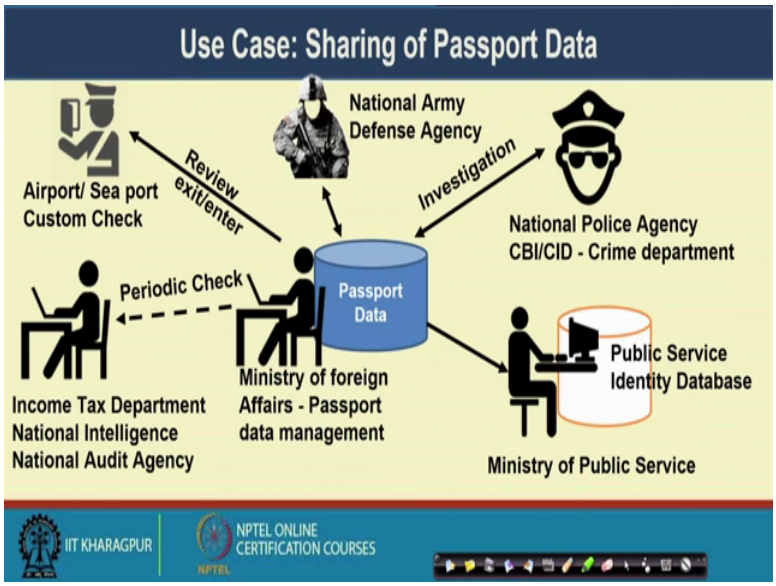
(Refer Slide Time: 21:15)



Well, the message that, I want to convey here that here the major problem is that data it is shared among multiple organization at different levels of government structure, when the data is shared among multiple organizations at different level of the government structure the data breaches the possibility of data breaches it increases at every level you can have data duplication. Say for example, whenever you are submitting your copy of the Aadhaar card or your Aadhaar number to some bank or to some mobile company you are actually making a duplication of the data.

Now, this data duplication gets increased and the data multiplicity get increased which actually, increases the possibility of the data breach. So, if that entire data is on a central storage and then if, you can make a architecture where everyone will be accessing the data via some common platform which is available to everyone through which everyone can validate whether those access are correct or not then possibly this kind of problems can be mitigated. So, that is why blockchain is coming to be a disruptive technology to support these different types of applications which are suitable for the Government parties.

(Refer Slide Time: 22:40)



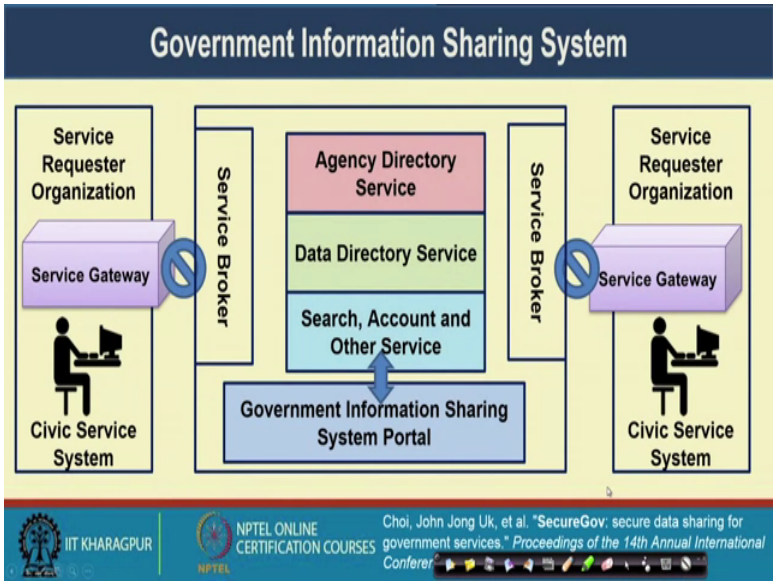
Let us see, an use case of your passport data. So, your Passport Data is ideally at the Ministry of foreign Affairs who are who are responsible for Passport data management. Now, there are different other organization in the picture who actually use your Passport Data. So, the Income Tax Department, the National Intelligence, the National Audit Agency, they can periodically check your passport data to find out that which countries you have visited and how much time you are there in those countries to look into the amount of money or the amount of assets that you possess and it is relationship with your a foreign visits. So, the Income Tax Department can look into your Passport Data to find it out then, your Airport or the Custom Check they look into your Passport Data to review the Airport exit or entry.

Then, the National Army or the Defense Agency they can look into the Passport Data to find out whether there is certain kind of National theft the Police Agency in Indian context the CBI or CID the Crime department they can look into the Passport Data for investigating certain cases then, you have this Public Service Identity Database like, say whenever you are going for a opening a bank account then, you need to give a proof of your identity there you submit a copy of your passport page. So, the data is also a copy of that data is also we do.

So, that this entire Passport Data it is being managed or it is been accessed by multiple government departments. Now if, something bad happens with your passport data then,

who is responsible for that actually, you do not know or it becomes, very difficult to proof someone that what has actually happened to that data.

(Refer Slide Time: 24:38)

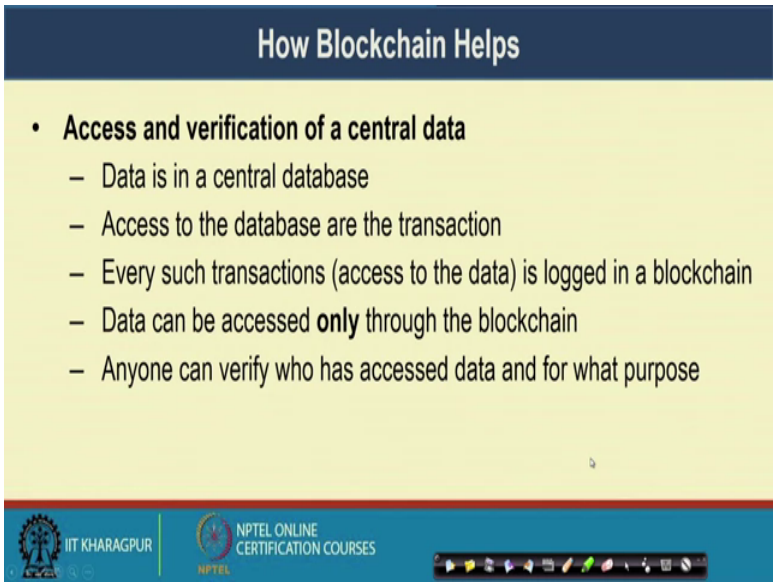


And here, block chain come into pictures. So, this is a kind of broad Government Information Sharing System which can be de centralized with the help of a block chain technology. So, I have just tried to give a schematic view which I have borrowed from one paper the reference is given at the bottom.

So, this architecture says that, you have certain Service Requester and other Service Requester who actually, request the service from your data collector through some Service Broker intermediate Service Broker who actually, help you to get access to the data say for example, for Aadhaar data the responsible service. So, for you can think of UIDAI responsible Service Broker who is helping to validate the individual Aadhaar data and then in the database you have multiple different type of data and the services, you have Agent Directory Service the Data Directory Service, the Search Account or other different type of Services and some portal through which you access the entire data.

Now, if this access to the data gets decentralized and if it is performed on the top of a block chain then it becomes easier to find out that who has actually, access this particular data. So, that we can look into more details and you can make up proven and start tracking of how my data is being accessed by multiple parties.

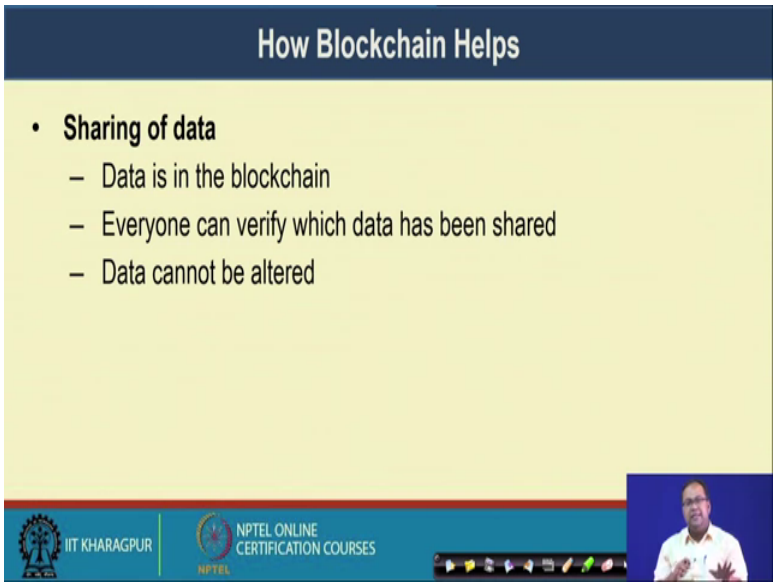
(Refer Slide Time: 26:14)



So, how blockchain helps here? So, one aspect is the access and verification of central data. So, your data is in a central database and access to the database you represent it in the form of a transaction every such transactions that is logged into a blockchain the concept that I have explained earlier, like all the data access you first log it on the block chain. So, you first say that I am going to access this data for this purpose which is written as a transaction then, different nodes in the network they will validate that whether you are authenticated enough or you are responsible or whether you can have access to that particular data or service. And, if they agree then you put that information to the log and access the data and that way the verification is done through the consensus algorithm and the log is being maintained under a blockchain which you cannot alter later on.

So, you will not be able to claim later on that I have not made this particular transaction because everyone in the network through the consensus protocol they have, already validated that you are the authenticated person who is initiating the transaction and you have put the transaction in the transaction log which anyone can see. So, anyone can verify who has accessed data and for what purpose.

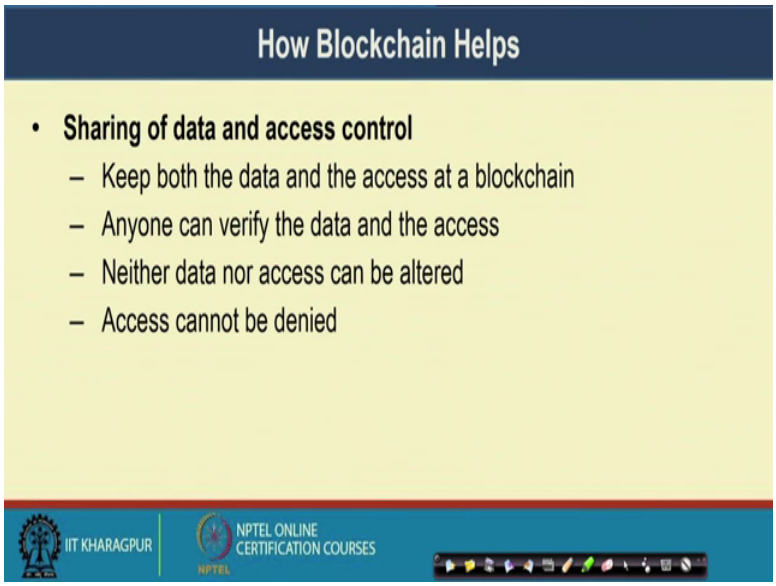
(Refer Slide Time: 27:48)



The second form where blockchain can help is the sharing of data. Now, instead of putting the access in the form of transaction in the blockchain you put the data in the blockchain it itself.

So, in that case you can always see that which particular data has been shared with others and once you share certain data that data cannot be altered. So, this kind of model is very useful for your say your supply chain management system where, the data is basically the demand and supply at different locations and that can be put inside a block chain. The third model is sharing of data as well as access control.

(Refer Slide Time: 28:28)



So, you combined the other two approaches together. So, you keep both the data and the access at a blockchain. So, anyone can verify the data as well as who has accessed that data. Now, neither data nor the access that can be altered later on and the access cannot be denied. So, you get a tamper proof technology to maintain your data as well as make a access control on top of that architecture.

(Refer Slide Time: 28:57)

Few use cases. So, where government is actually, involving in block chain based applications. So, in Russia the state run back Sberbank they partner to it Russia's Federal

Antimonopoly Service phase to implement document transfer and storage via blockchain. So, this was a news that published December 2017.

(Refer Slide Time: 29:23)

Then, in South Korea Dayli Financial Group which is house of Korean fintech startups, they are working on creating different blockchain based ecosystem they called it as ICON which will allow different government departments, universities, hospitals, banks etcetera to interact without any third party networks. So, you can have a blockchain environment on which they can share their data and provide service to the people.

(Refer Slide Time: 29:54)

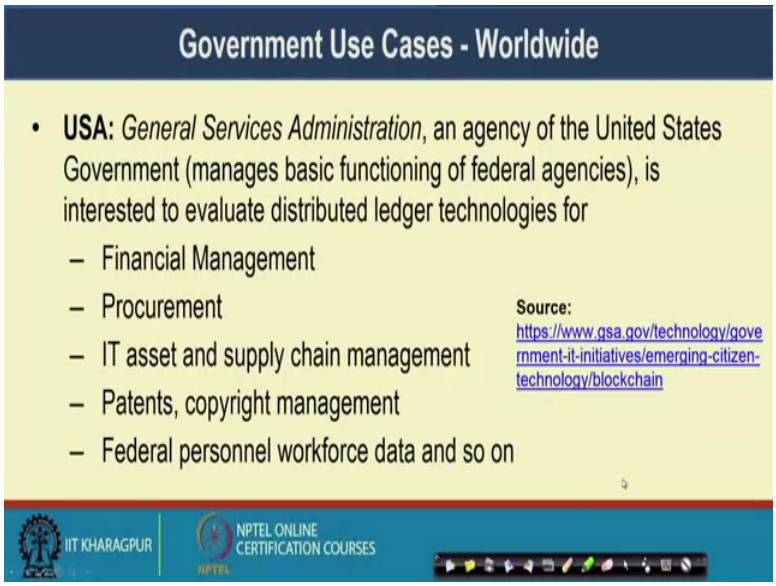
Then in Singapore, Singapore Government was pioneer in developing blockchain based application. So, they have started a project called Ubin. So, in this Ubin project they have started to explore the use of this distributed ledger technology for clearing and settlement of payment and securities. So, like the for domestic inter-bank payments they are looking into the feasibility of distributed ledger technology for using this Ubin. It is like that you want to issue and transfer funds among participate provide loan to certain participants for that all these access information they will be put in a blockchain that can be later verified by the auditors easily.

(Refer Slide Time: 30:43)

In India there was a recent development so, it is particular news was very very new. So, the news was in February 22, 2018 when it got published. So, in India the government is trying to develop something called a India Chain which is a trial solution for utilizing the blockchain technology for digitization and verification of educational degree certificates. So, it is like that, there are a lot of fraud on educational degree certificate. So, the degree certificate should be put on a blockchain platform and that can be easily verified by different department who wants to verify them.

Or there will also be have certain kind of access logs to find out that who actually, access download educational certificates for a particular person and authorization can also be guaranteed on top of this architecture. So, they have India has taken this initiative.

(Refer Slide Time: 31:49)



And, the last on USA so, in USA blockchain was a big impact. So, the Government has started to look into the blockchain technology from different aspects. One aspect is this General Service Administration of GSA which is an agency of the United State Government. It manages the basic functioning of federal agencies. They are interested to evaluated the distributed ledger technologies.

So, they have made a call for proposal for getting multiple suggestion about how the blockchain technology can be applied for the Financial Management, procurement, IT asset and supply chain management, patents and copyright management. Then the Federal personal workforce data management, in this different aspects of blockchain technology. So, this gives you a overall view about how government can utilize this blockchain platform to secure the data as well as to ensure the access and auditing of information at the government level.

In the next lecture we will look into certain use cases of this and we will also look into one practical example where the government was successfully able to develop electronic platform to facilitate multiple services through this blockchain concept. So, we will discuss this details in the next class.

Thank you for attending the class for today.