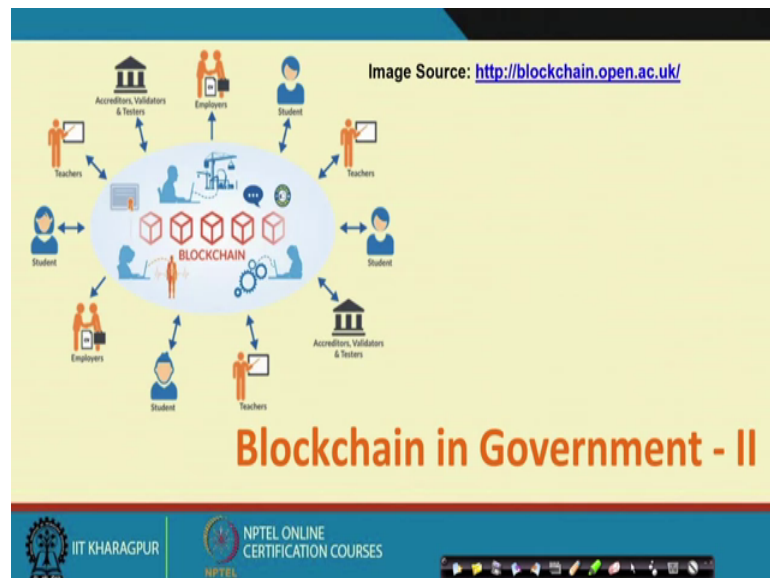


Blockchains Architecture, Design and Use Cases
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

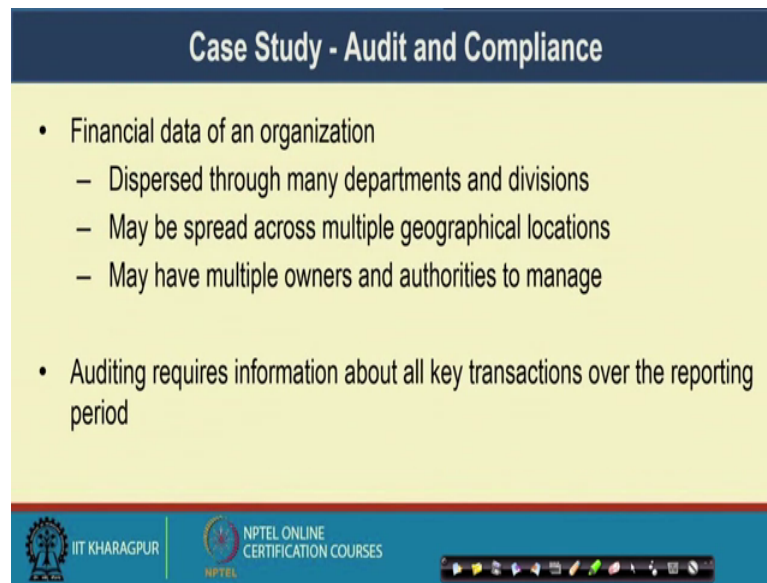
Lecture – 40
Blockchain in Government – II (Use Cases)

So, welcome back to the course on Blockchain. In the last class we have, looked into a broad overview about how Blockchain technology can be useful for managing data and access to the data at a government level. So, today we will look into certain use cases of data.

(Refer Slide Time: 00:36)



(Refer Slide Time: 00:37)



The slide features a dark blue header with the title 'Case Study - Audit and Compliance' in white. The main content area has a light yellow background and contains two bullet points. The first bullet point is 'Financial data of an organization', followed by three sub-bullets: 'Dispersed through many departments and divisions', 'May be spread across multiple geographical locations', and 'May have multiple owners and authorities to manage'. The second bullet point is 'Auditing requires information about all key transactions over the reporting period'. At the bottom, there is a blue footer with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a navigation bar.

- Financial data of an organization
 - Dispersed through many departments and divisions
 - May be spread across multiple geographical locations
 - May have multiple owners and authorities to manage
- Auditing requires information about all key transactions over the reporting period

So, let us, start with a few case studies. So, the first case that we are looking into is using the blockchain technology for audit and complaints. So, this Financial data it is a huge vulnerable data for an organization and interestingly the financial data whenever, you are going to collect it from organization that need to be audited periodically at the end of financial year.

So, this financial data actually, it comes from multiple sub divisions under organizations. So, normally it happens that you just think of large company which wants to give tax income tax their income tax at the end of the financial year and they have to show their audit that that was the total amount of income over the financial year.

The total amount of expenditure over the financial year and what total profit that they have gain based on which we have to submit the tax, the government tax. Now, the Government auditor their task is to verify that whatever the claim this particular institution or the organization it is making that particular claim is actually a valid claim and there is no falsification in that data.

Now, the question comes that, if you just look into the entire auditing purpose which is applied now a days. So, this auditing procedure it is very complex and the auditors they have to manually check every purchase and every big purchase and the different expenditures which are being reported by organization or by a company details and try to

find out that whether there is certain kind of inconsistencies in the information that they are sharing over all.

So, in this aspect, blockchain can play a good role. We will see that how blockchain can be utilized in for this purpose. But, the trouble come into picture because if, you in an organization which is divided into multiple such sub division. So, whenever some financial matter comes, the institution or the organization the top financial authority of the organization. They share the money or the profit or the fund among multiple subdivisions then, there are financial authority are the subdivisions.

They again can share a distribute the fund into the lower level or they can spend certain funds themselves. And for the auditing purpose the logs start coming from the lower level. So, the lower level or the bottommost level of the organization, they submit their audit logs to their parent organization or the parent division.

They validate the audit logs and then send it again to their parent organization that way this entire organizational architecture it forms, some kind of tree and through which this funds propagates from top to bottom or as this audit log propagates from bottom to top.

So, the challenge again may come that sometime this individual organizations or different divisions of an organization they may spread across multiple geographic domains. And say for example, if you think about the top IT companies like say Microsoft Google, Facebook whatever you name for they are spread into across multiple countries. And the auditing rules the financial rules are different countries are actually different.

So, how this companies are actually going to manage this entire financial data for auditing and the Compliance purpose? So, you may have multiple owners and authorities to manage these data. So, this auditing requires information about all the key transaction which have happened over the reporting time.

So, as I mentioned, this auditing is a difficult task because you need to gather this entire data and perform the auditing at the different level then combine them together and find the Auditing at the organization level. So, let us see that how blockchain can make this entire process simplified well.

(Refer Slide Time: 05:22)

The slide is titled "Audit and Compliance" and contains the following text:

- What if the data is stored in a central server?
 - The problem of a central server - what if the server gets hacked?
 - Who will manage the server? The administrator of the server may not have the power to view the data
 - But the administrator can tamper the data if compromised
- What is the validity of data provided by different divisions?
 - What if the voice from two divisions do not match?

A hand-drawn diagram on the right side of the slide shows a central server icon connected to several smaller boxes representing different divisions or departments. A blue circle highlights the central server, and another blue circle highlights one of the division boxes.

The slide footer includes the IIT KHARAGPUR logo, the NPTEL ONLINE CERTIFICATION COURSES logo, and a small video inset of a speaker.

So, before, we going to blockchain let us see that what if, we store the data in a centralized server? So, if you store the data in a centralized server first of all, you have the problem of a central server. So, if that central server gets hacked all your data are gone . Next question comes that, who will manage the server? it may happen that the administrator of that server the administrator is or sometime the administrator maybe a group of people they are not authorized or they do not have the power to view the data, but it may always happen that the administrator can tamper the data, you can restrict the few of the data by applying certain kind of security mechanism like encryption of data and so on.

So, that only the authorized persons or authorized agent can look into the data, but you do not have any control where the data is being stored. So, sometime I think you have heard of that, people have destroyed certain logs or certain entries just to make it difficult for the life of the auditor difficult to find out that what particular problem has been happened over this data. So, if the administrators are compromised administrator can always tamper the data.

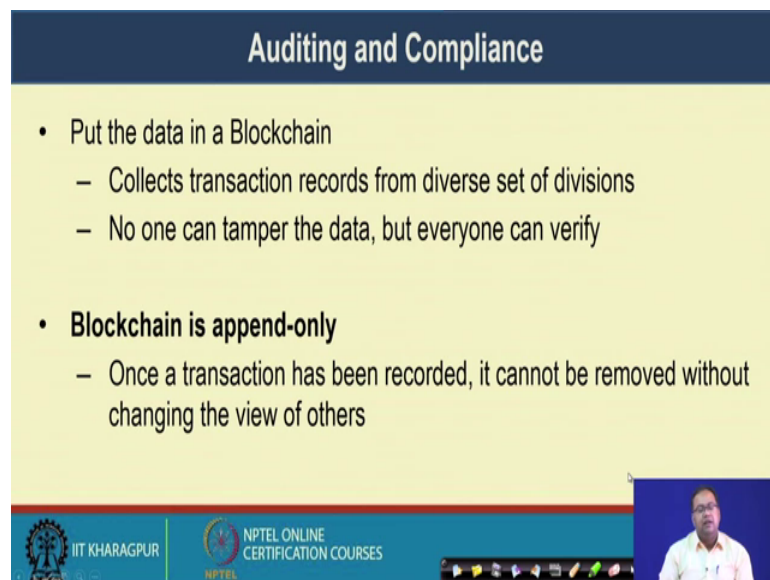
So, that way putting something on a central server is the is not always safe for you, you will never be able to guarantee the absolute safety of that data. Then another question comes, with this kind of auditing purpose that what is the validity of the data which is provided by different divisions?

So, it is like that, if you think of the entire organization is in a kind of tree structure and at every level you are so, at every level you are doing individual auditing. And whatever auditing report is coming from this lower level the auditor at this level then, relay on the audit data which is coming from the lower level.

Now, what if the auditor which is which there at this level, the auditor it itself is compromised. So, that way it becomes difficult even, for this middle level auditor or the top level auditor to find out that something bad has happened with that this data.

So, even someone who is there in the part of the system they may get compromised that, we have to assume on a on a real environment or on a real scenario.

(Refer Slide Time: 08:11)



The slide is titled "Auditing and Compliance" and contains the following content:

- Put the data in a Blockchain
 - Collects transaction records from diverse set of divisions
 - No one can tamper the data, but everyone can verify
- **Blockchain is append-only**
 - Once a transaction has been recorded, it cannot be removed without changing the view of others

The slide also features logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES at the bottom, along with a small video inset of a speaker.

So, here comes, the blockchain. So, you put the data in a Blockchain. So, the blockchain it collects all the transaction records from diverse set of divisions. Now, on top of blockchain you can apply the privacy policy or you can apply the concept of channels. So, here I am utilizing a term which Praveen has explained you in the context of Hyper ledger Fabric.

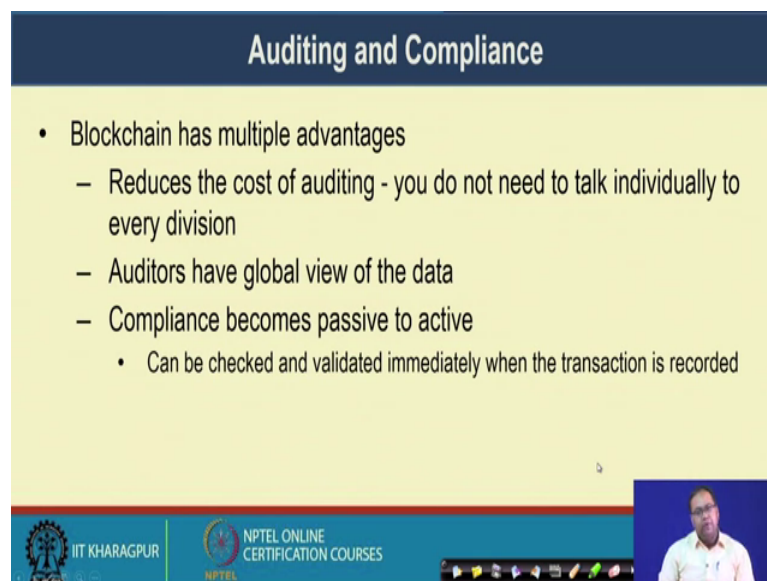
So, what blockchain you have this concept of channels, were the information which is, shared in one channel it remain private to only the users of that channel. So, that way, by creating multiple channels you can have access control over the data like you can ensure that, only this valid personal or the authorized personal they will have access to the data

and no one else will have access to the data or they will not be able to view that data by utilizing multiple channels all together. But, you can prove that what data is there over the entire blockchain and that entire data is tamper proof. Now, the copy of the blockchain the good thing here is that the copy of the blockchain is there on individual parties.

So, no one will be able to tamper the data or destroy it is local database to entirely falsify the system or make that system difficult to prove that certain bad has happened over the system. So, what was the problem we keeping data in central server? So, if the administrator was compromised; so, the administrator can delete the data delete that portion of the data and make the life of the auditor difficult to prove that certain bad has happened.

So, there was no way to prove that certain bad has happened but, with this blockchain because no one has control over the entire blockchain that are the entire technology is a decentralized technology no one will be able to delete that data once that data has been written the blockchain platform. And this append only feature of Blockchain, it gives this power to the entire system to prove that what happened to individual transactions and making auditing of the transactions becomes much easier.

(Refer Slide Time: 10:39)



The slide is titled "Auditing and Compliance" and lists the following advantages of blockchain:

- Blockchain has multiple advantages
 - Reduces the cost of auditing - you do not need to talk individually to every division
 - Auditors have global view of the data
 - Compliance becomes passive to active
 - Can be checked and validated immediately when the transaction is recorded

The slide also features logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a small video inset of a speaker in the bottom right corner.

So, we have multiple advantages here first of all, it reduces the cost of auditing you do not need to talk individually to every division and you do not require the auditor at every

division the top level auditor it can simply look into all the transactions happened there and find out whether something bad has happened or not. So, the auditors they have the global view of the data. Now, second thing the compliance it becomes passive to active this is one important achievement by utilizing the block blockchain platform.

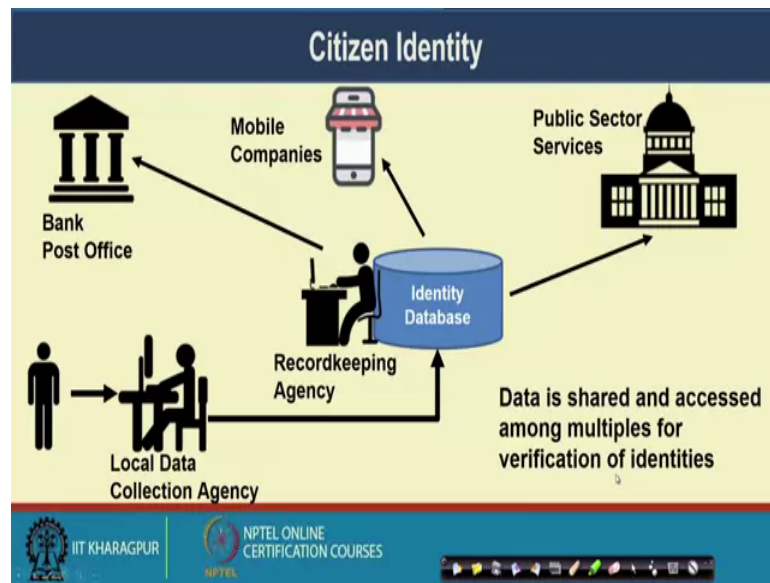
So, the auditors can write certain small quotes on top of this blockchain certain small scripts like, the smart contracts to automatically validate that whether, certain transactions are complying with the existing transaction or existing fund availability or not.

So, even before the transaction has happened or the transaction has been initiated you can check this compliance report you can check the compliance by writing the smart contracts under blockchain platform. That gives the additional power and because of which people claim that blockchain is a disruptive technology that can change that has the power to change this entire financial management system for auditing and compliance check.

So, after you have purchase something the auditor need not to check for the compliance even, before the purchase has happened the smart contract it itself can check the compliance and remember that the smart contracts is it itself a publicly available court. So, anyone can see that what is their detail in the smart contracts and they can validate whether the smart contracts is actually doing the correct thing or not. So, you cannot insert a smart contract as a malware or a yeah, like a as a as a as a malware or a virus inside the blockchain architecture because everyone can validate that code and that particular script is open to all.

So, that script will automatically execute and validate the system has having compliance the new transaction that is coming it is having compliance with the old transactions and already having the fund which is, which is there with individual subdivisions or the divisions of an organization,. The second use case which is having lot of debate now a days is looking into the citizen identity.

(Refer Slide Time: 13:08)



So, Aadhaar has the debate from this platform like, whenever you have the citizen identity data or the Aadhaar data that particular identity data that is being accessed by multiple independent organizations.

So, you have the individual persons who are getting their data record. So, you have this Local Data Collection you can see who are recording the data and then transferring the data to the Identity Database then you have the Recordkeeping Agency the Recordkeeping Agency is ensuring the security of this Database, but this particular data is actually accessed by multiple organization.

So, I have just tried to take an example of the Aadhaar data and the different organizations who are currently accessing my Aadhaar data. So, the banks or the post office have your Aadhaar data the mobile companies they are taking your Aadhaar data to validate that you are authorized person for having a Indian scene, for getting a Public Sector Services you have to register your Aadhaar details.

To validate that you are a citizen of a country and you are authorized to get that particular service. So, this entire data it is shared and accessed among multiples for verification of identities. Now, as an individual this individual it does not have any information about with whom the data has been shared or who are currently accessing my data.

(Refer Slide Time: 14:44)



The slide is titled "Citizen Identity" and contains the following content:

- Control the access through a Blockchain
 - Blockchain has information about who has accessed my data
 - I can verify how my data has been accessed
 - I can verify what part of my data has been accessed
 - Everyone can verify how the overall data is getting accessed
 - **“Access auditing”**

At the bottom of the slide, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a small video feed of a presenter.

Now, if I put this entire thing, in a blockchain or if, we control the entire access to a blockchain. So, this blockchain can have the information about who has accessed my data; I as an individual I can verify that, how my data has been accessed; I can verify that, what part of my data has been accessed.

So, if you look into the identity data the identity data have multiple fields. It has your name it has your identity, it has your mobile number it has your address.

So, if a mobile agency accesses your Aadhaar data you can find out from this blockchain that, which part of the data has been looked by the mobile agency or even you can write some smart contracts there which will not disclose your entire Aadhaar data rather, it will just take the data from the mobile. It will validate that data with the data which is available with the Aadhaar database and it will simply reply back with an yes or no.

So, that way as an individual as a citizen of the system you can find out that who has accessed your data and for a what purpose they have accessed your data. And you can you can also verify that who are different entities in the overall system who are having access over the entire Aadhaar data.

So, you can have something called a “Access auditing” of the system. So, you can find out that who are accessing the data and for what purpose they are accessing data what part of the data is being accessed in this entire procedure.

(Refer Slide Time: 16:22)

The slide is titled "Blockchain for Defense" in a dark blue header. Below the header, on a light yellow background, are the following bullet points:

- Multi-organizational information flow
 - Tracking of information origin, flow and destination
 - Asset tracking
 - Certification of peoples and machines
 - ...

Below the text, there are three images representing military assets: a group of soldiers in camouflage gear labeled "Army", a grey naval ship labeled "Navy", and a grey fighter jet labeled "Air Force". The labels are written in blue cursive. At the bottom of the slide, there is a blue footer with the IIT Kharagpur logo and the text "NPTEL ONLINE CERTIFICATION COURSES". A Windows taskbar is visible at the very bottom of the slide.

The third use case that, I am going to talk about is from the Defense perspective. Now, this defense it is a truly Multi-organizational system where you require Multi-organization information flow.

So, if you look into the Defense architecture of a conflate has three broad systems. It has it is own army it has the Navy and it has the Air Force. Now, this individual three organization or three subdivision of defense, they have their own policies, their own regulation for sharing the data or sharing the information.

Now, with this Multi- organization information flow in a defense, you can track the information origin the flow and destination. So, if you remember the byzantine general problem and which can happen in a different scenario and if, you are utilize in a blockchain with this consensus mechanism to find out that what instruction has been passed from army to navy or form navy to air force, everyone can see that and everyone can validate the origin of the information and the correctness of the information.

Then, the asset tracking whenever the military assets are transferred from different organization of the entire defense then the certification of the peoples and machines that can be done you by utilizing the blockchain technology.

(Refer Slide Time: 17:56)

The slide features a dark blue header with the title 'Defense Secure Messaging and Transaction Platform' in white. The main content area has a light yellow background and contains a bulleted list. At the bottom, there is a blue footer with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a standard video player control bar.

- Defense cyber security relies on secrecy of information and trust among individuals
 - Both are difficult to ensure in a real environment
- Needs to ensure that
 - Only the privileged information has been accessed
 - Information logs has not been tampered
 - Provenance tracking of information origin and flow

So, in general these defense secure messaging and transaction, platform it can utilize this concept of blockchain technology. So, this defense cyber security it relies on the secrecy of information and the trust among individual.

So, in general whatever information is coming from army to Navy, the Navy commanders get tracks the information which is coming from the army commander. Now, if that army commander is compromised that is a big threat to the entire country. Now, ensuring this kind of security or the secrecy of information and the trust both are difficult to ensure in a real environment. So, we need to ensure that only the privilege information has been accessed.

So, no one is accessing some information which is not intended for them. Information logs which are there they are not been tampered over time and Provenance tracking of information origin of flow. So, from where, the information has actually originated and how the information has flown over the entire systems. So, this entire team can be mapped on a services which is provided by a blockchain platform. So, again just like the earlier case you put everything in a blockchain whenever certain information is flowing you first put in a blockchain and then make a flow of the information

So, you have a transaction log and through that transaction log anyone can validate the origin of the transactions and a movement of the transaction over the entire system.

(Refer Slide Time: 19:32)

The slide features a map of Estonia with a blue, black, and white color scheme. To the right of the map, a bulleted list provides key statistics. Below the map, the word 'Estonia' is written in red, followed by the text 'A country in northern Europe'. The slide footer includes the IIT Kharagpur and NPTEL logos, along with a small video inset of a presenter.

Let Us See a Success Story

- Area 45,227 KM²
- Population (2011) 1,294,455
- Population Density 28/km²
- GDP (2018) \$43.567 Billion

Estonia
A country in northern Europe

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Well. Now, let us see a success story where, blockchain has been utilized not only the blockchain several other digital or e-governance concept has been utilized. So, we are talking about small country called Estonia.

So, Estonia is A country in northern Europe if you look into the demography of that particular country it has a Area of 45,227 Kilometer square. According to 2011 census, the population of some 1,294,455; so, the population density you see it is pretty low.

It is 28 per square Kilo meter and a GDP of the country as per the 2018 data. It is 43.567 Billion dollar.

(Refer Slide Time: 20:27)

The slide is titled "e-Estonia" and features a list of benefits. The text is as follows:

- Digital ID card and decentralized distributed system
- Multiple benefits Check <https://e-estonia.com/>
 - File taxes within 5 minutes
 - Sign a contract electronically
 - Register a business within 30 minutes
 - i-Voting
 - You can become a e-Citizen!

The slide also includes logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES at the bottom, and a small video inset of a speaker in the bottom right corner.

So, Estonia they have launched a platform called e-Estonia in e-Estonia you can have, digital ID card and the de centralized distribution system of the information among the people of Estonia.

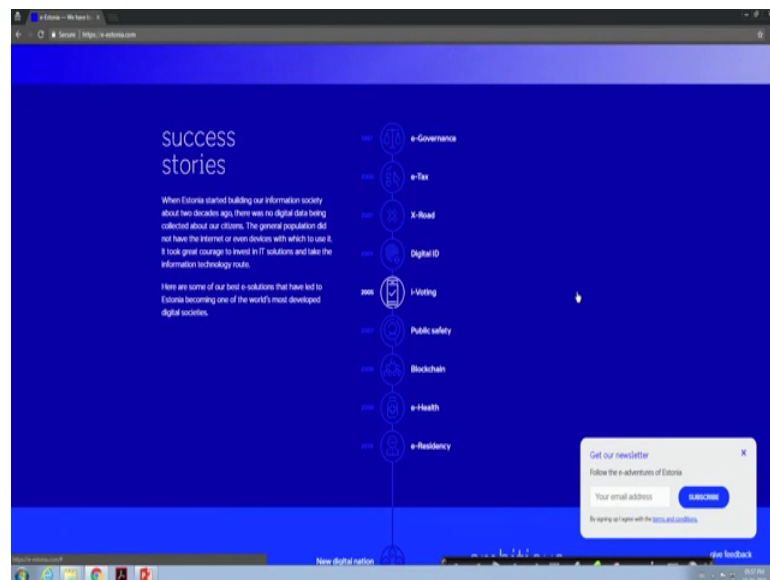
So, it supports multiple services there like you can file the taxes within 5 minutes and that can get validated because, all the information is over that distributed digital platform. You can sign a contract electronically; you can register a business again within some 30 minutes everything is done electronically over that platform. You can become a e-Citizen of Estonia by subscribing to that particular platform and you can participate in i-Voting. So, vote over the internet.

(Refer Slide Time: 21:18)



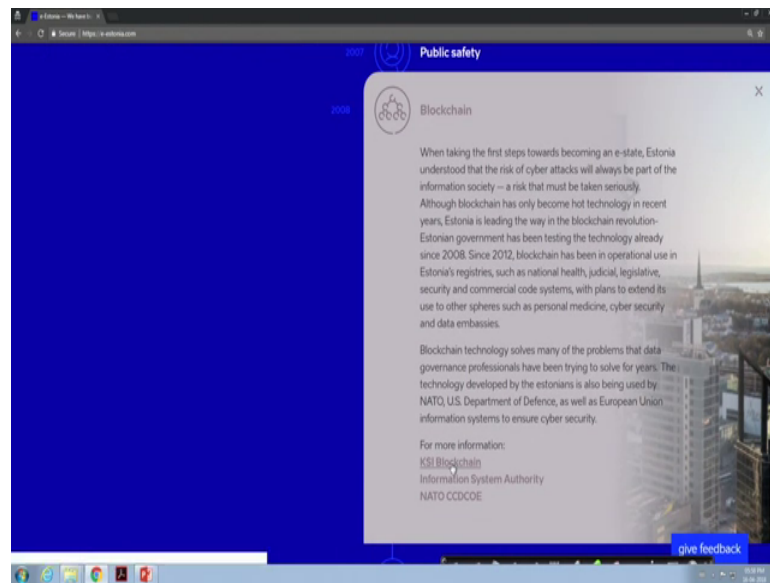
So, let us (Refer time: 21:18) of e-Estonia. So, here is the site for e-Estonia; so, where it can find out the different services provided by e-Estonia. So, the tagline is very nice that we have built a digital society and so can you.

(Refer Slide Time: 21:40)



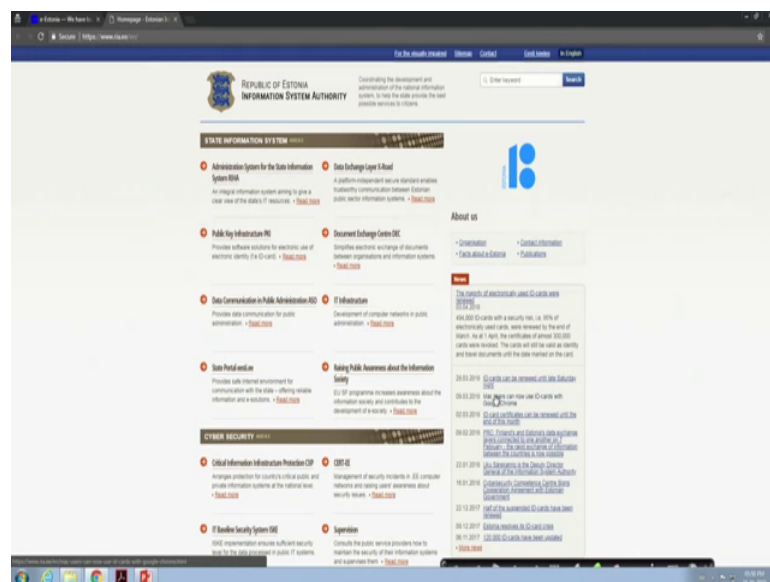
So, let us look into the services which are being provided by Estonia and which are basically successful for Estonian perspective like this e-governance, e-tax. So, let me just increase the font. So, these e-governance, e-tax, x-road, digital ID, i-Voting, public safety blockchain; do, here they have utilize the blockchain for many application.

(Refer Slide Time: 22:12)



So, here there is a details that, the type of services that they have utilized over the blockchain platform. Say it is the information system authority where they have utilized the information system for developing a blockchain based architecture.

(Refer Slide Time: 22:28)



So, here you can see that, different kind of a information system that they have utilized using Blockchain.

So, the entire state information system that was that was uploaded over the blockchain platforms. So, the administrative system the data exchanges, even, the public key

infrastructure, the document exchange. So, for all this things they have utilized blockchain based platform.

(Refer Slide Time: 23:07)



Then, this e-health e-residency and many other ambitious futures like that there trying to build up on this e-Estonia platform and many of these services; they are utilizing the concept of public domain blockchain technology. So, you can just browse through this website and you can look into the different aspect on which there utilizing different e-governance technique and different type of services over this kind of a blockchain platform.

So, this is a nice success story where a government organization it has utilizes the blockchain platform to build up a nice applications and nice architecture. Where, you can perform many transactions or you can access different kind of database the medical records, the educational information in one click and you can ensure the safety of the information on top of that platform.

So, I request all of you to explore these, e-Estonia platform and look into the different services that, they have developed and also look into the details about how they have utilized this blockchain concept to develop multiple services for e-governance perspective. That will give you a broad idea about how you can utilize blockchain for building up services for a nation.

So, in today's class the, we have talked about few such applications and use cases where government can benefit from the utilization of blockchain platform. We will look into many of such other applications in details as we make progress. So, I hope that you have enjoyed this, lecture with this particular information about the success stories of blockchain in real platform which actually, make you a motivation that well.

Bit coin can be one application build up on blockchain platform and because of all these financial and the dconomic debate over bit coin even if, you keep aside bit coin from this is blockchain concept and if you focus on the blockchain itself you can build up a plenty of services over this platform.

So, we will come up, with few of or many other such applications in our subsequent lectures and we will look into the details of them.

So, thank you all, for attending the class today.