

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

Lecture – 01
Introduction to Blockchain – I (Basics)

Welcome to the course on Blockchain Architecture Design and Use Cases. So, this course will be taken by myself, Dr. Sandip Chakraborty from Computer Science and Engineering Department at Indian Institute of Technology, Kharagpur along with Dr. Praveen Jayachandran from IBM Research, India.

So, in this course we will cover a fundamental topic blockchain which is now it is very important and we see multiple use cases for this particular topic and this course is unique in the sense, like in this course we will cover important part of the industry aspects which will be mainly covered by Praveen and I will cover the fundamental theoretical concept behind blockchain. And together we will try to focus on multiple aspects of this particular technology.

(Refer Slide Time: 01:13)



The slide, titled "Course Instructors", features two portraits side-by-side. On the left is Sandip Chakraborty, wearing glasses and a dark jacket, with the text below identifying him as "Sandip Chakraborty, Department of CSE, IIT Kharagpur". On the right is Praveen Jayachandran, with a goatee and a light blue shirt, with the text below identifying him as "Praveen Jayachandran, IBM Research, India". The slide footer includes the IIT Kharagpur logo, the NPTEL Online Certification Courses logo, and a navigation bar with various icons.

So, as I have mentioned we two are the course instructor I am from IIT, Kharagpur and Praveen is from IBM Research. So, the first part of the course will be mostly taken by me which will cover the basics of blockchain and then Praveen will cover the industrial aspects of this particular technology, and how IBM is working on this technology to

expand its barrier over multiple application domains starting from various industrial aspects, governmental aspects as well as various aspects of supply chain management, financial sectors and so on.

(Refer Slide Time: 01:53)



The slide is titled "What We'll Cover in This Course" and lists the following topics:

- A history of blockchain – how the computation environment gradually evolved
- Blockchain – architecture, design and protocol
- Blockchain consensus protocols
- Security and Privacy aspects of Blockchain
- Various use cases – Finance, Supply Chain, Government
- Hyperledger Fabric – a platform for Blockchain development
- Research aspects

The slide footer includes the IIT KHARAGPUR logo, the NPTEL ONLINE CERTIFICATION COURSES logo, and a navigation bar with various icons.

So, this is a broad over view of the course that we will cover throughout this 30 hours of lecture. Initially I will give you for this week I will give you a brought overview of blockchain with a focus on the history how this technology came into practice.

And I hope that many of you know that this technology was actually came from the financial sector from the concept of cryptocurrency where its seen it has seen a tremendous application of blockchain technology along with multiple other concepts. So, in that particular direction I will start with how basic cryptocurrency protocols are implemented using blockchain and then how blockchain concept can be extended for multiple other domains. So, in the second week I will focus on the architecture design and protocol aspects of blockchain, the system aspect as well as the security aspects, then we will focus on the consensus protocols of blockchain which is particular system aspect and which makes this concept of blockchain really decentralized and internet scale.

Then we will cover the security and the privacy aspects of blockchain. After that Praveen will covered on multiple application use cases starting from financial sector, supply chain management, government aspects and at the same time Praveen will cover a part of hyperledger fabric which is a platform for a blockchain development using hyperledger

fabric platform you can develop multiple applications of blockchain. So, Praveen will give you many applications and use cases and show you that how you can develop a particular blockchain application using the concept of hyperledger fabric.

And finally, we will discuss on some advanced topic of blockchain, the current research aspects how the industries utilizing blockchain for multiple use cases.

(Refer Slide Time: 04:02)

What Is A Blockchain

- A decentralized **computation and information sharing platform** that enables **multiple authoritative domains**, who do not trust each other, to **cooperate, coordinate and collaborate** in a **rational decision making process**

Image courtesy: <https://blog.exchangeunion.com>

The slide features a network diagram with nodes represented by padlocks connected by lines, symbolizing a decentralized network. The slide is part of an NPTEL online certification course from IIT Kharagpur.

So, let us come to the basic concepts of blockchain starting from this definition, and throughout this first week of talk we will mostly focus on this definition and try to expand various keywords which are there inside this definition.

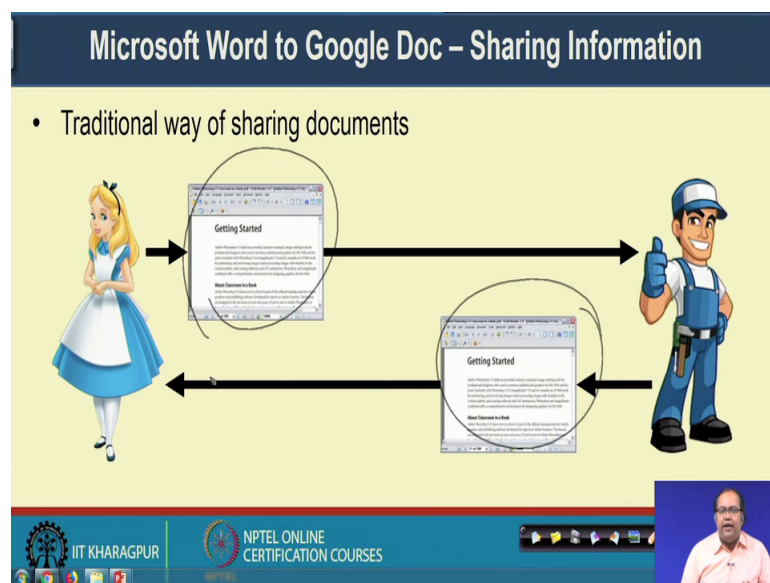
So, by definition blockchain is a decentralized computation and information sharing platform which enables multiple authoritative domains who do not trust each other to cooperate coordinate and collaborate in a rational decision making process. So, the keyword that we have in this particular definition is this decentralized that is an important aspect of blockchain, we will talk about that how this technology is decentralized and what is the utility of this particular technology when you use decentralized platform.

Then this computation and information sharing platform, so blockchain broadly you can think of it as a decentralized database which helps in cooperation between multiple authoritative domain. So, this terminology multiple authoritative domains it is the third

keyword. So, the technology is particularly useful when multiple parties or individual they want to cooperate it with each other, and they want to come to a common platform to share the information among themselves.

And another important aspect of blockchain is that whenever we are talking about multiple authoritative domains. This multiple authoritative domains they do not trust each other. So, this is an important aspect of blockchain that you can combine multiple authoritative domains who do not trust with each other and they can come to a common platform where they can cooperate, coordinate and collaborate in application development process at the business intelligence process. So, this is the broad definition of blockchain and let us know see a particular use case that how blockchain can be useful for developing applications.

(Refer Slide Time: 06:20)



So, if you look into the traditional way of sharing documents whenever we used to do it using Microsoft word say Alice wants to share some documents with Bob. So, what ideally Alice will do? Alice will just write down his content inside his or her own document. So, Alice will whatever Alice wants to write she will write it in her own document, then Alice will share that document to Bob and after that Bob will update the document with his content and share the document again to Alice. So, that was the traditional way of cooperation between Alice and Bob when they want to write some think in a shared document.

Now, in this particular architecture there are multiple disadvantages. The first disadvantage is that Alice and Bob they will not be able to simultaneously edit the document, that is a fundamental problem of this architecture that first Alice up to update her own content then she can share the document with Bob, and once Bob receives that content then only he will be able to update the content and share it back with Alice.

(Refer Slide Time: 07:39)

Microsoft Word to Google Doc - Sharing Information

- Shared Google doc - both the users can edit simultaneously

**The environment is still centralized.
Does centralized system harm?**

The slide features a central image of a Google Docs document interface. To the left is a cartoon illustration of Alice, and to the right is a cartoon illustration of Bob. Arrows point from Alice to the document and from the document to Bob. The slide includes logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES at the bottom.

Now, from this architecture we move towards the next architecture where we use this Google Doc or share Google Doc platform. So, in a shared Google Doc dot platform both Alice and Bob can write simultaneously or they can edit the document simultaneously. But with that this shared Google Doc document the problem is that this environment is still centralized.

Now, the question is that does centralized environment harm or what is the disadvantage that if we use a centralized environment for cooperation during this kind of information sharing platform. So, the major problem of a centralized system is that it works as a single point of failure.

(Refer Slide Time: 08:19)

Problems with a Centralized System

- **A single point of failure**
 - If you do not have sufficient bandwidth to load Google doc, you'll not be able to edit
 - What if the server crashes?

Image courtesy: <http://timkellogg.me/>

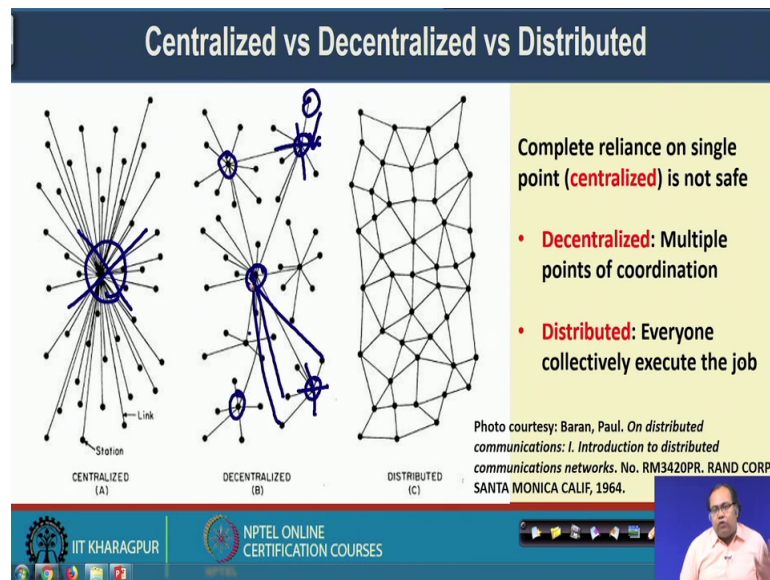
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Say if you do not have sufficient bandwidth to load the Google Doc, just consider this kind of scenario then you will not be able to do a edit on that particular document, you have to wait until you are able to connect to the internet and load the Google Doc platform

Now, another problem comes which problem is not there may be for Google Doc because Google has their dedicated server architecture or they made the server application failsafe. But if you are building your own application and you are writing that application or storing that application in a centralized computer and two people are connecting to that computer to get that information then the problem is what if the server or your computer crashes.

In that case the entire information get lost or even if you want to make it failsafe you want to keep it a backup you have to load the backup and only after loading the backup you will be able to process it further. So, that is the major point of this kind of centralized systems and that is why we want to move from a centralized platform to a distributed platform.

(Refer Slide Time: 09:25)



So, whenever we are moving from a centralized platform to a distributed platform we basically have broadly distributed system concepts people talk about 3 different architecture, one is called a centralized architecture, the second one is called the decentralized architecture and the third one is called a distributed architecture, architecture.

So, in case of a centralized architecture there is a central coordination system and every node connecting to central coordination system and whatever information they want to share the information will be shared by this central coordination system. And under this platform you have a problem like if this central coordination platform fails then all of these individual nodes they will get disconnected.

So, from the centralized system we will move towards a decentralized system. So, in this decentralized system you have few coordinators rather than a single coordinator and all these coordinator cooperative with each other and the individual nodes they are connected to this coordinator. So, in this particular architecture, if this particular node fails or multiple node fails then this coordinators can connect to another individual nodes can connect to another coordinator and can share the information and can or perform the operation using those or those available coordinators which are there.

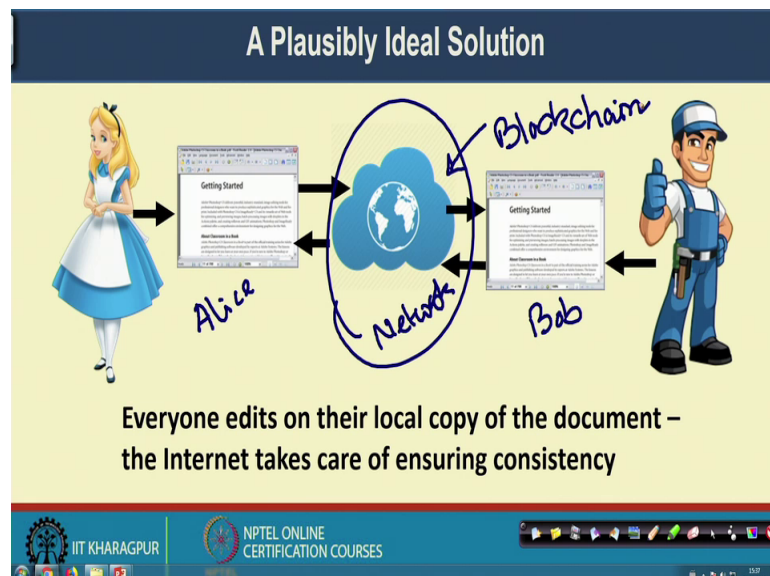
So, in this particular decentralized architecture you have the advantage that you can still tolerate multiple number of failures, until the network becomes disconnected. So

obviously, this architecture works on top of a network and because of multiple simultaneous failure if the network get partitioned or the network get disconnected then this individual nodes will not be able to cooperate with each other.

So, to solve this problem we move to the next architecture which we called the complete distributed architecture. So, in a complete distributed architecture you do not have this kind of centralized coordinator and all the nodes they participate in the computation or the information sharing process or in the application development where they coordinate with each other and collectively develop the application or collectively share the information among them self.

So, that are the relative advantages or disadvantages of a decentered platform and distributed platform over a centralized platform. And in our modern architecture what we want, that well centralized platforms are good, but they are not scalable they are not robust to failure. So, we want to move from a centralized architecture to a decentralized architecture or a distributed architecture. So, blockchain is a platform which helps you to support this kind of decentralized platform or a distributed platform where you can share the information among yourselves in a very custody manner.

(Refer Slide Time: 12:36)



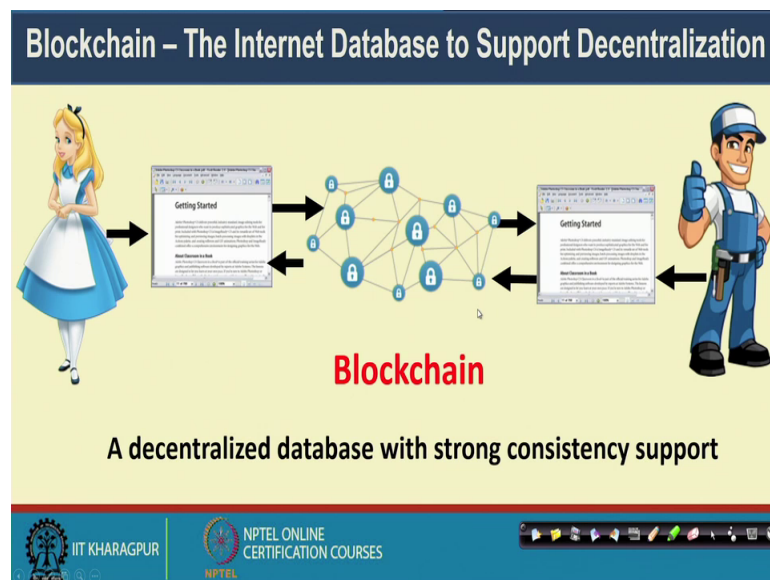
So, this is the ideal solution using blockchain. So, in a blockchain platform Alice has her own copy of the document and Bob has his own copy of the document. So, this copy belongs to Alice and this copy belongs to Bob, and they can simultaneously write to their

own document and here I have the network in between and the network has the task to ensure that the information consistencies maintained between the documents which Bob and Alice hold individually.

So, this is an ideal use case where you can use the blockchain platform. So, this blockchain platform comes in between. So, this blockchain platform which is pant over the network and it will help you to make this kind of coordination where Alice will keep her own copy of the document, Bob will keep his own copy of the document, they can independently write their personally personal copy and then the blockchain platform will ensure that the information that they are entering inside the document they are getting synchronised with each other and both with time both will be able to see the most updated copy or they will be able to update the over the most updated copy.

So, that is the advantage of a blockchain technology over a complete centralized or a centralized architecture where or architecture where you have a shared copy which is between which is shared between multiple parties.

(Refer Slide Time: 14:28)



So, this is an interesting and typical application of a blockchain. So, this blockchain comes in between, it replaces the network and the blockchain helps that both Alice and Bob will be able to simultaneously read or write the documents; And the advantage that I have mentioned that they do not need to rely on the internet or if a server crashes they do not depend on a server crash. So, by definition we can say that a blockchain is a

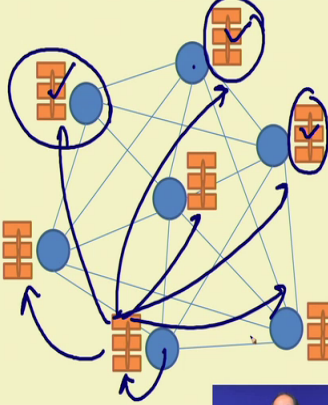
decentralized data based platform with strong consistency support. So, it is supporting that whatever information Bob or Alice is writing in the document individually they are getting synchronized over the network, ok.

So, now, let us look into a very simplified architecture of blockchain.

(Refer Slide Time: 15:15)

A Very Simplified Look of the Blockchain

- Every node maintains a **local copy** of the **global data-sheet**
- The system ensures consistency among the local copies
 - The local copies at every node is identical
 - The local copies are always updated based on the global information



The diagram illustrates a decentralized network of nodes (blue circles) connected by lines. Each node contains a local copy of the global data-sheet, represented by orange blocks. Some nodes have a checkmark, indicating they are updated or consistent. Arrows show the flow of information between nodes, ensuring consistency across the network.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

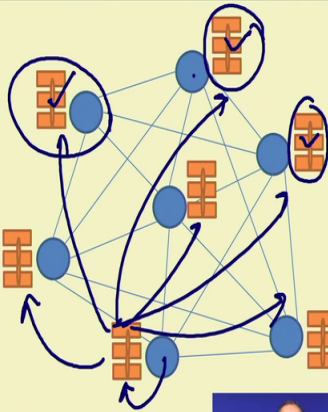
So, in a typical blockchain architecture every individual node they maintains a local copy of blockchain. So, here I have multiple nodes in the internet who are connected with each other, and everyone is maintaining a local copy of the global data sheet.

Now, the system task is to ensure that all this individual copies they are consistent with each other. Consistency here means that the local copies that every node has those copies are identical, and this copies are always updated based on the global information; that means, if this node wants to enter some information to this blockchain. So, this information will get updated to all the copy of the blockchain that every node possess. So, that is that is basically the architectural platform of blockchain which supports a strong consistency among the local replica local information that every node has.

(Refer Slide Time: 16:26)

A Very Simplified Look of the Blockchain

- We call this a **Public Ledger**
 - A database of “**historical information**” available to everyone
 - The “**historical information**” may be utilized for future computation
- **An Example:**
 - Say, the historical information are the banking transactions
 - The old transactions are used to validate the new transactions



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

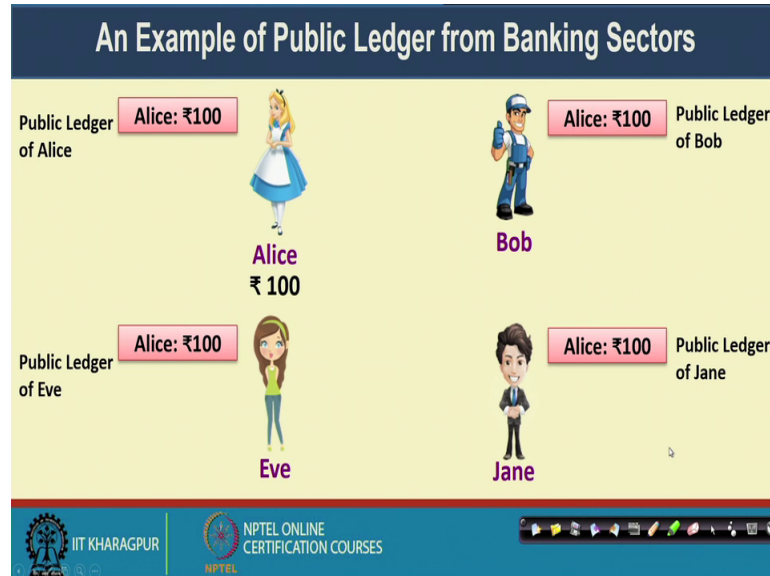
So, this local information we called this local information a public ledger. So, this is an term important term in the context of blockchain, the concept of public ledger. So, the public ledger is something like everyone possess his or her own copy of data. So, if you think of a data base system a data base is nothing but a collection of historical information which is available to everyone. So, public ledger is a work like a data base where it contains this kind of historical information which is available to inform everyone and this historical information can be utilized for future computation.

An example of public ledger can be like the banking transaction. Say you are keeping the banking transactions inside the public ledger and this whole transactions which are there they are basically used to validate the new transaction. Now, in a typical banking system what we do that we maintain a passbook and the bank work like a centralized authority which stores all our transaction information and whenever you are going to bank or you whenever you are making a transaction during that time bank validates everything with the centralized information that it has.

Now, in case of this public ledger we are moving form a centralized banking system to a decentralized backing system where every individual has their own copy of the global tractions which is synchronized and which is consistent and whenever you are trying to make a new transaction or someone else is trying to make a new transaction during that

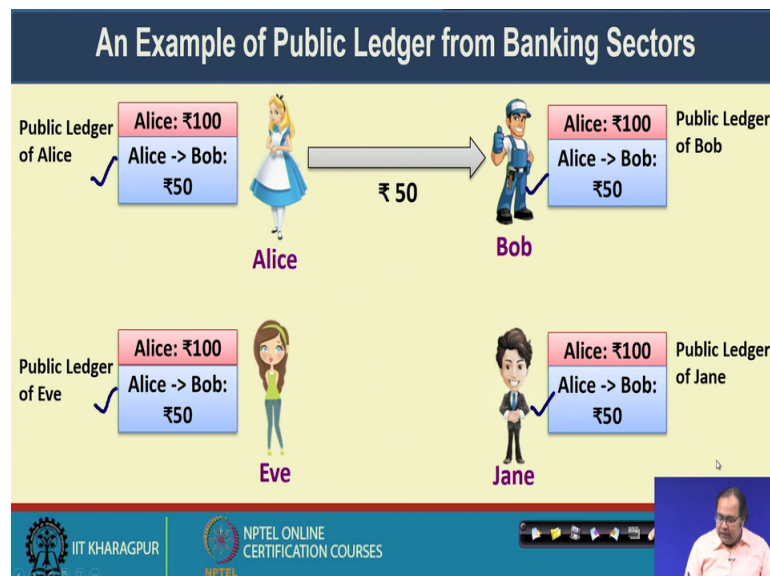
time that new transaction is validated against the old transactions that you have already there inside the public ledger.

(Refer Slide Time: 18:18)



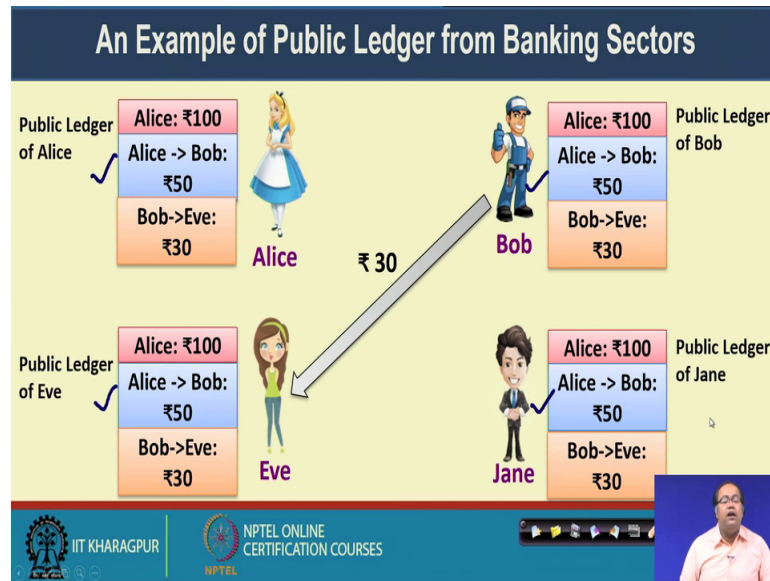
So, let us see an example of public ledger from banking sector. So, we have 4 participants here Alice, Bob, Eve, Jane. Now, assume that Alice wants to Alice initially has 100 rupees in her hand. So, the public ledger that is there, so the public ledger is available to Alice, Bob, Eve and Jane and the public ledger that they have it has the initial content or initial information that Alice has race 100 in her hand.

(Refer Slide Time: 18:57)



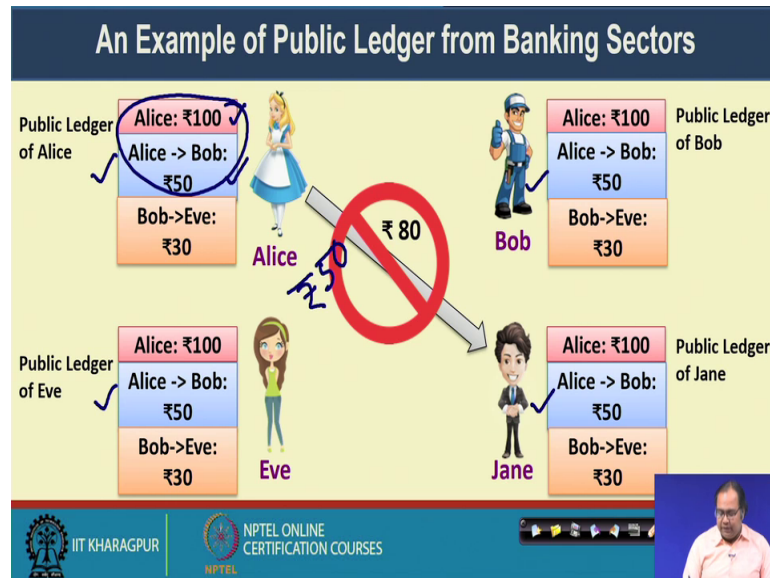
Now, say Alice wants to make a transaction of ₹ 40, rupees 40 to Bob. In this case we add up another transactions in the public ledger; that means, this information need to be updated to all the all the public ledger all copies of the public ledger that Alice has, Bob has, Eve has and Jane has. So, this particular transaction gets updated to all these copies of the public ledger.

(Refer Slide Time: 19:25)



Then say Bob wants to make another transaction of rupees 30 to Eve. So, this particular information is again updated in the public ledger; that means, the public ledger which is available to Alice, Bob, Eve and Jane and everyone basically contained the information of all the transactions and the local copy of that particular entire public ledger is available to all the parties who are there in the network.

(Refer Slide Time: 19:52)



Now, say Alice wants to make a transaction of rupees 80 to Jane. Now, by looking into this public ledger you can see that Alice initially had rupees 100 with her and then Alice made a transaction of rupees 50 to Bob. By combining this two transaction I can say that now Alice has only this 50 in her hand. So, if you are trying to make a transaction of rupees 80 that means, this particular transaction is not valid.

So, all the parties which are there in the network by looking into their public ledger they will be able to understand that this particular transaction is not valid. So, this particular transaction is blocked and this that is not added to the public ledger. So, in this particular way public ledger works in the context of a decentralized system.

(Refer Slide Time: 20:41)

Blockchains and Public Ledgers

- Blockchains work like a public ledger
- However, we need to ensure a number of different aspects
 - ✓ **Protocols for Commitment:** Ensure that every *valid transaction* from the clients are committed and included in the blockchain within a finite time.
 - ✓ **Consensus:** Ensure that the local copies are consistent and updated.
 - ✓ **Security:** The data needs to be *tamper proof*. Note that the clients may act maliciously or can be compromised.
 - ✓ **Privacy and Authenticity:** The data (or transactions) belong to various clients; privacy and authenticity needs to be ensured.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, blockchain the concept of blockchain you can think blockchain is nothing but a public ledger; however, whenever you are implementing such kind of blockchain by utilizing the concept of public ledger you need to ensure a number of different aspects, first the protocol for commitment.

So, the protocol for commitment means whenever someone is making a new transaction during that time you need to ensure that this particular transaction if it is valid, it will get committed to the existing public ledger or the existing blockchain otherwise that entry will not be there in the blockchain. So, there should be a mechanism for validity checking of every upcoming transactions from the clients and then based on that validity checking you will be able to either accept the transaction and include it in the existing blockchain or you can delete the transaction or discard the transaction.

Now, the second requirements is a consensus. Consensus is an important aspect in the in the context of blockchain. So, in case of blockchain as we have discussed that you have a local copy of the information available to every individual parties and there is no such central platform like a bank which will maintain the consistency of the transactions or the consistency of the information. So, that is why the consensus mechanism ensures that whatever local copy every individual party has they are consistent with each other that everyone has the most updated copy and a copy that they have individuals have they are identical or similar to each other.

The third important aspect is the security. That means, the data that you are inserting in a public ledger or inside the blockchain, now because this blockchain is distributed to individual parties everyone is maintaining their local copy of the blockchain. So, that person may change something in that local copy and broadcast that saying that see this is the updated information.

But the other nodes in the network they should be able to understand that whatever this person is broadcasting that is the false information or that is the tempered information the blockchain that that person is broadcasted that has false information and they should be able to discard that particular information. So, that way the security need to be ensured because you do not have some centralized authority like bank will be able to maintain the validity of the information rather in a decentralized way you have to ensure the validity.

And a final aspect is the privacy and authenticity. So, the data or the transactions which is their inside the blockchain it belong to various clients. So, it is coming from various clients and you are putting that information inside the blockchain and a copy of the blockchain is available to every parties and that is why the privacy and authenticity of the information need to be ensured.

(Refer Slide Time: 24:04)

Formal Definition of a Blockchain

- A Blockchain is "an **open distributed ledger** that can record transactions between two parties **efficiently** and in a **verifiable** and **permanent** way" (Iansiti, Lakhani 2017)
- The keywords: **Open** (accessible to all), **Distributed or Decentralized** (no single party control), **efficient** (fast and scalable), **verifiable** (everyone can check the validity of information), **permanent** (the information is persistent)

Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". *Harvard Business Review*. Harvard University.

The slide includes a video player interface at the bottom with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES. A small video inset shows a speaker in the bottom right corner. Handwritten annotations include a blue circle around 'open', a red circle around 'distributed ledger', a blue circle around 'efficiently', a blue circle around 'verifiable', a blue circle around 'permanent', and the handwritten text 'tamper-proof' with checkmarks.

So, if we look into the formal definition of blockchain, so the formal definition of blockchain is something like this. So, this definition I have taken from this particular

book by this is in data review report review report called The Truth About Blockchain by Marco, Iansiti and Karim Lakhani. They have published this article in January 2017 and there they have given nice definition of blockchain. So, according to them a blockchain is an open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.

So, again in this particular definition we see a number of keywords. So, understanding this kind of keywords is important. So, the first keyword is this open. So that means whatever information you are putting inside the blockchain that should be accessible to all. So, everyone will be able to observe and validate that particular information. So, that is the first requirement for blockchain.

The second one is distributed ledger. So, a blockchain is a distributed ledger; that means, you are keeping a copy of that public ledger to every individual parties who are there in the platform and their communicating with each other. So, that that is the concept of distributed. Now, the platform can be either distributed or decentralized based on your application.

The third keyword is efficiently. So, you need to ensure the efficiency of the information, efficiency of the protocol, so the protocol need to be fast and scalable. So, it should scale up with the number of client request as well as the number of participants in the network.

Then the next keyword is verifiable. Verifiable is again an important key keyword which says that everyone who are there in the network they should be able to check the validity of the information. So, that is termed mean by verifiable. And then a permanent, permanent means the information that you are entering inside the blockchain that information is persistent or sometime we call it as tamper proof.

So, tamper proof means that once you have inserted an information inside a blockchain then you will not be able to change that information or update that information in future time. So, if you want to update that transaction you have to insert a new transaction saying that the old transaction is invalid and that is the new transaction. But whatever has been already committed that committed transactions will never be able to rolled back or someone will not be able to change that particular transaction. So, these are the important properties of a blockchain environment.

So, with this I will conclude this first 30 minutes lecture where we have seen a broad overview of blockchain and we have seen that how you can utilize the decentralized platform for information sharing among multiple parties, and while doing that information sharing what are the different aspects that you have to look into. And in the next lecture we will look into that how we are utilizing this concept of blockchain and how the concept of blockchain gradually evolved starting from cryptocurrency and nowadays various industrial application. So, see you again in the next lecture.

Thank you.