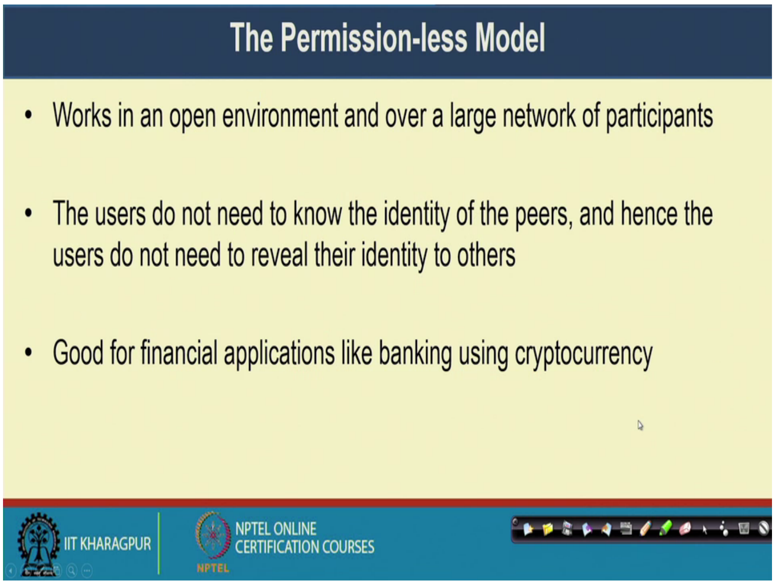
Blockchains Architecture, Design and Use Cases
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 04
Introduction to Blockchain – IV
(Blockchain Applications)

So, welcome to the fourth lecture of this blockchain course. So, today we will talk about this conceptualization of the blockchain architecture and some interesting fact inside this blockchain design, and we will look into a few application that can be realized using blockchain.

(Refer Slide Time: 00:41)



The Permission-less Model

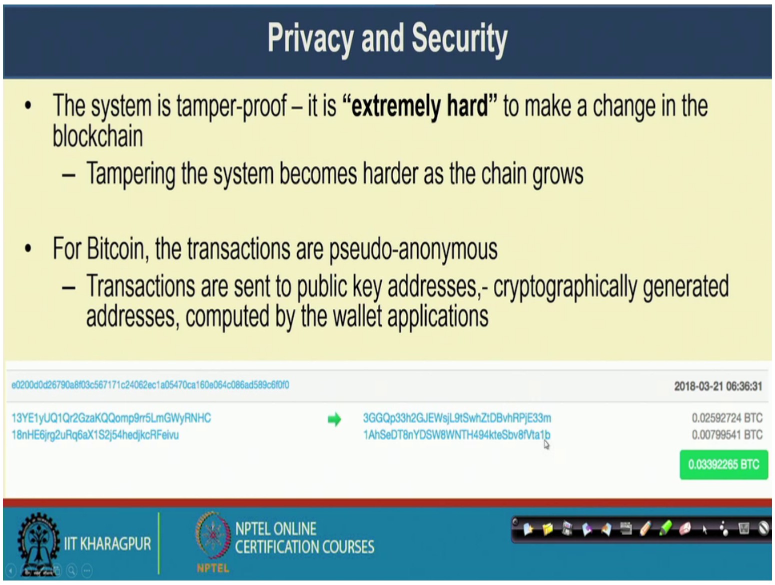
- Works in an open environment and over a large network of participants
- The users do not need to know the identity of the peers, and hence the users do not need to reveal their identity to others
- Good for financial applications like banking using cryptocurrency

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

So, in the last class we have discussed about this permission less model. So, we have discussed that a permission less model, it works in an open environment and over a large network of participants. So, where the participants do not need to reveal their own identity; so, the users do not need to reveal their own identity to other peers and hence the users also do not need to know the identity of the others. So, the entire protocol works on a challenge response fashion.

So, this kind of permission less model, they are kind of good for financial applications like cryptocurrency, where you want to develop a currency mechanism that will not be under control of any single participants and anyone in the network will be able to participate in the transactions by utilizing that currency.

(Refer Slide Time: 01:40)



Privacy and Security

- The system is tamper-proof – it is **"extremely hard"** to make a change in the blockchain
  - Tampering the system becomes harder as the chain grows
- For Bitcoin, the transactions are pseudo-anonymous
  - Transactions are sent to public key addresses,- cryptographically generated addresses, computed by the wallet applications

e0200d0d26790a8f03c567171c24062ec1a05470ca160e064c086ad589c6f0f0 2018-03-21 06:36:31

13YE1yUQ1Qr2GzaKQQomp9rr5LmGWyRNHC
18nHE6jrg2uRq6aX1S2j54hedjkcRFeivu
➡
3GGQp33h2GJEWsjL9tSwhZtDBvhRPjE33m 0.02592724 BTC
1AhSeDT8nYDSW8WNTH494kteSbv8fVta1b 0.00799541 BTC

0.03392265 BTC

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

NPTEL

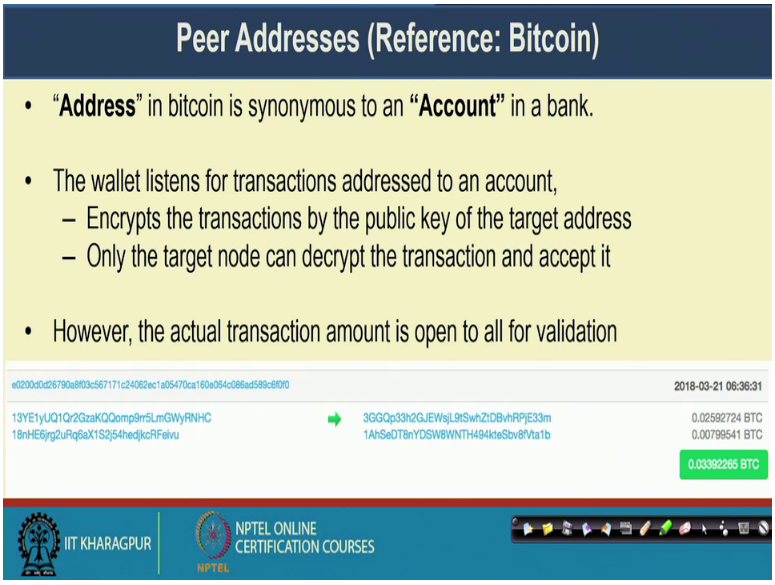
So, this kind of environment they provide certain level of privacy and security. As I have mentioned earlier that a system is tamper proof, it is extremely hard to make a change in the blockchain. But remember that it is not impossible based on the architecture that we have, it is always possible to change a to tamper the blockchain architecture, but it is extremely hard. So, with the current hardware devices that we have, it is it is nearly impossible to tamper a blockchain architecture.

Now, regarding privacy for Bitcoin, the transactions are pseudo anonymous that provides certain level of privacy not a complete privacy. So, in case of Bitcoin that a transaction which are send, they are sent using some public key addresses the concept of the public key and a private key we will discuss starting from the next week, while we go to the details of different cryptographic mechanism. So, which are utilized for a blockchain.

So, this broadly this public key addresses are cryptographically generated addresses, which are computed by the wallet applications. So, here in this example you can see that this particular things, they are the cryptographically generated addresses using this public key cryptography, and this addresses from this addresses you will not be able to understand who are the actual users.

So, you can just see that this user has transferred certain money, certain 0.0339 certain Bitcoin to this user, but who are those user users are in actual real network that you do not know that you will not be able to reveal. So, it provide certain level of privacy, but remember it does not guarantee the complete privacy, because you are still able to see the transactions; Although, you are not decode the users, but you are still able to see the transactions.

(Refer Slide Time: 03:43)



Peer Addresses (Reference: Bitcoin)

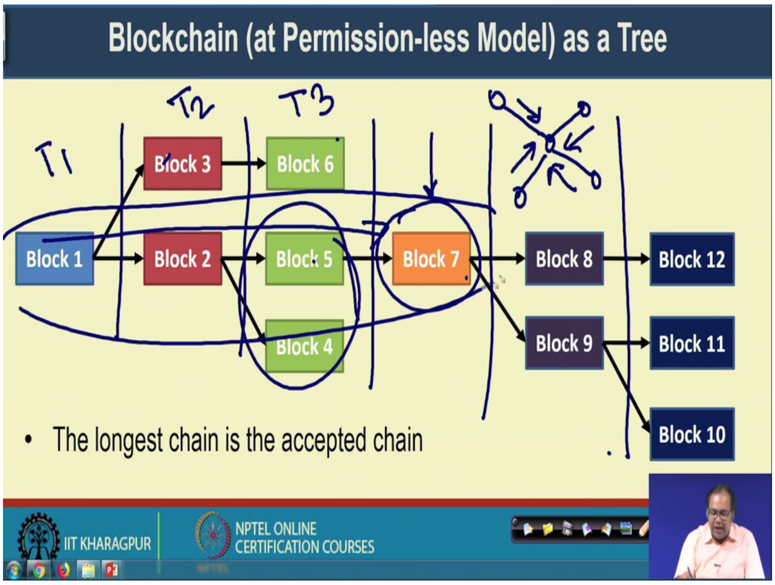
- "**Address**" in bitcoin is synonymous to an "**Account**" in a bank.
- The wallet listens for transactions addressed to an account,
  - Encrypts the transactions by the public key of the target address
  - Only the target node can decrypt the transaction and accept it
- However, the actual transaction amount is open to all for validation

e0200d0d26790a8f03c567171c24062ec1a05470ca160e064c086ad589c6f0f0			2018-03-21 06:36:31
13YE1yUQ1Qr2GzaKQQomp9rr5LmGWyRNHC 18nHE6jrg2uRq6aX1S2j54hedjkcRFeivu	➡	3GGQp33h2GJEWsjL9tSwhZtDBvhRPjE33m 1AhSeDT8nYDSW8WNTH494kteSbv8fVta1b	0.02592724 BTC 0.00799541 BTC
			0.03392265 BTC

So, this addresses in Bitcoin they are synchronous to an account in a bank. So, every address they uniquely identify a user. So, for every user one addresses associated with him or her. So, the wallet it listens for the transactions address to an account, and these transactions they are encrypted by the public key of the target address. So, only the target node can decrypt the transaction and accept it. That a target node can understand that this particular transactions is intended for myself and the wallet accept the transactions and publish that availability of this much amount of Bitcoin to its his or her wallet.

However, the actual transaction as I have mention, it is open to all for verification. So, Bitcoin makes this things public because anyone can verify the transaction. So, user IDs are constant. So, this ID once it is generated this will remain forever until you change the wallet or until you lose your wallet. So, whatever transactions that will be done by a same wallet, it will have this addresses. So, the addresses are unique based on that unique addresses you can validate the transaction, but you can cannot reveal or you cannot find out the actual identity of the corresponding user.

(Refer Slide Time: 05:07)



Blockchain (at Permission-less Model) as a Tree

- The longest chain is the accepted chain

Now, there is one interesting fact in blockchain mining procedure. So, in the blockchain mining if you remember that what we discussed, that multiple users they are simultaneously trying to mine a block; they are simultaneously trying to solve a mathematically challenging problem based on this challenge response architecture that I have discussed in the last class, and based on that they are trying to find out a block.

Now each of these blocks are generated in individual time instances. So, this is say T 1 at T 1 you have the block 1, now at T 2 again multiple users are trying to generate the blocks and assume that, 2 users have found out the block simultaneously or nearly at the same time. So, what will happen both will at this block 2 block 1.

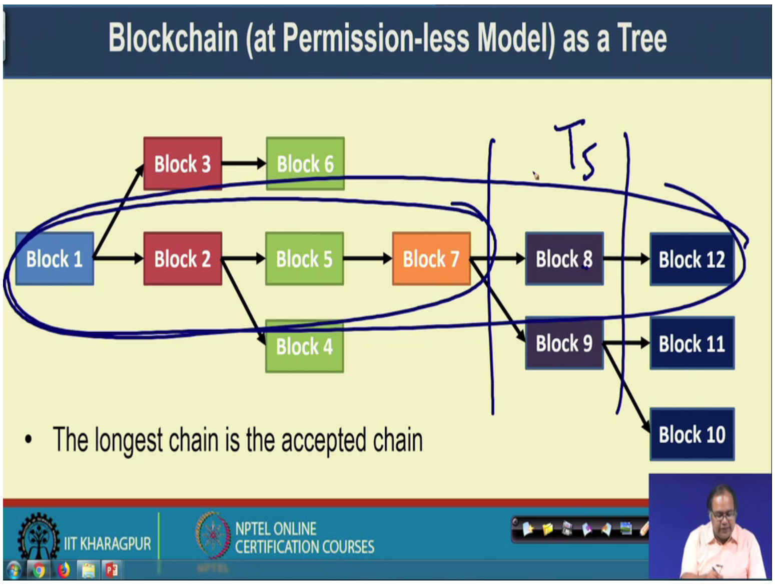
So, now I actually have 2 parts from block 1. From block 1 either I can go to block 3 or I can go to block 2 then at time 3 again, whenever the new transaction comes the users will try to again mine that the miners will try to mine that an at the new blocks. And at that time instance it may happen that 3 other users they are able to successfully find out the nonce, which will have the corresponding difficulty in the hash function they will able to get it at the same instance of time.

Now, if they are able to get it at the same instance of time. So, they are 3 other blocks and now this 2 users, they have this block as the previous block. So, they connect the block with this as the previous block another user is connects the block this one as the previous block. Now, what happens in case of a blockchain network that whenever you are adding up a new block to the blockchain, then you are broadcasting that updated blockchain to your neighbours

Now, a neighbour if you look into a peer to peer architecture, a particular neighbour can receive the block for from multiple other peers and whenever it finds out that well there are multiple copies of the blocks, which he or he or she has received then it accepts the block with the longest chain. So, it only accepts the longest chain. So, whenever say another user comes here, it assumes that this is the longest chain. So, the whenever the next block is mined that gat get added to block 5.

So, once block 7 gets added to block 5, then this particular chain becomes the longest chain. So, this particular chain becomes the longest chain, now the subsequent block will added to block 7 and that will not be added to block 6. So, again at this time instance say this is T 1 T 2 T 3 T 4 and T 5. So, at this time instance again 2 miners can mine the block simultaneously so, there can be 2 other blocks.

(Refer Slide Time: 07:53)



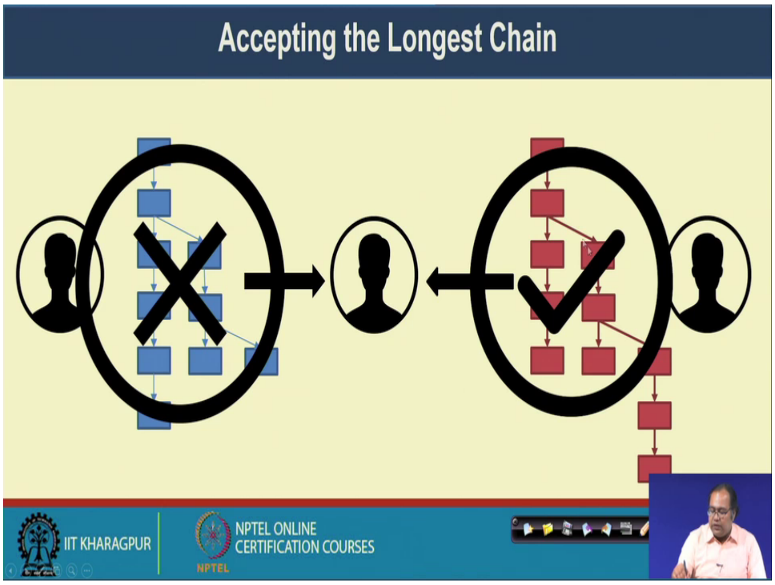
Blockchain (at Permission-less Model) as a Tree

- The longest chain is the accepted chain

So, that way in general a blockchain is not a chain rather a tree you can represent it as a directed tree and in that directed tree whatever be my longest chain, that is accepted as the current chain. And in sometime instance it may happen that you have 2 different chain both of them are having same length say for example, in this case this chain this chain and this chain all the 3 chains are of same length.

So, whenever a miner has this kind of option he randomly selects one of them one of them. And ideally what it happens then whenever people are propagating the updated block to the neighbours it is expected that some chains will get invalidate over invalidated over time. So, the exact procedure of invalidation again we will discuss when we will go to in depth make of in depth discussion of this mechanisms.

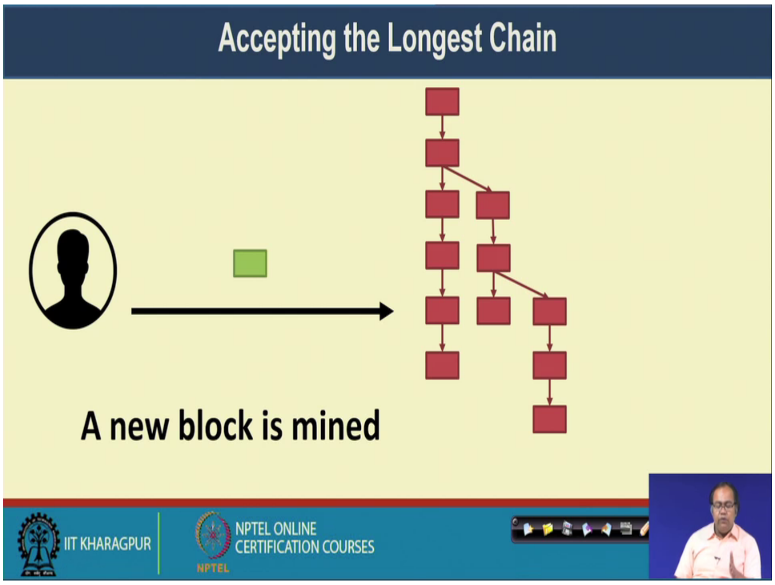
(Refer Slide Time: 08:56)



Accepting the Longest Chain

Now, that is the idea whenever a this user gets a two different blockchain two different versions of the blockchain, it always accepts the longest chain. So, this was the longest chain based on the current blockchain. So, it has a part length of 1 2 3 4 5 1 2 3 4 5 6 7 it has the length 6. So, it will accept that chain.

(Refer Slide Time: 09:20)

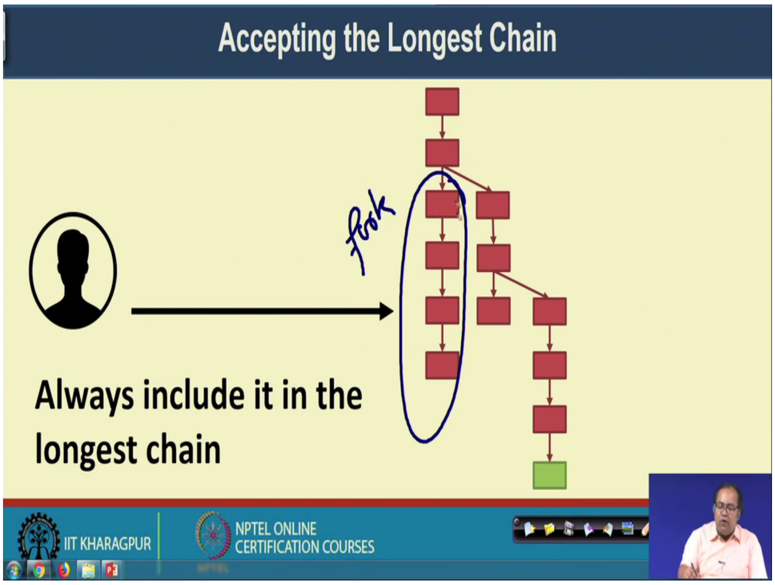


Accepting the Longest Chain

A new block is mined

Now, whenever a new block is mined during that time, that new block is always added to the longest chain.

(Refer Slide Time: 09:29)

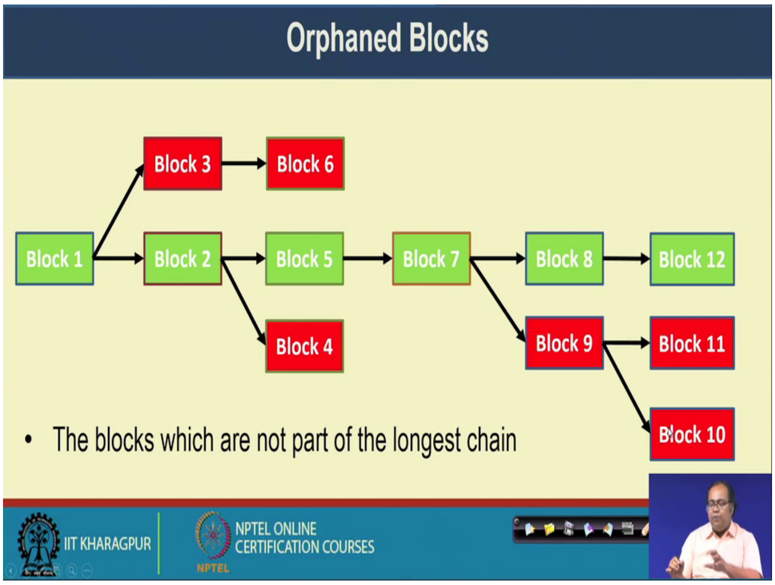


Accepting the Longest Chain

Always include it in the longest chain

So, whenever the new block is mined. So, this particular chain this particular chain is the longest chain. So, the new block will get added to this longest chain. So, that way whenever the blocks are getting propagated or multiple users are mining the data simultaneously and you have possibility of having multiple chain together. So, all this call things with taked a name from operating system and we say that a new chain has been forked, just taking into the concept of process from operating system is there new chain has been fork. But whenever a new chain gets if that is not the longest chain, that is not used any further always the longest chain is getting used to add of the new blocks to a existing blockchain.

(Refer Slide Time: 10:26)



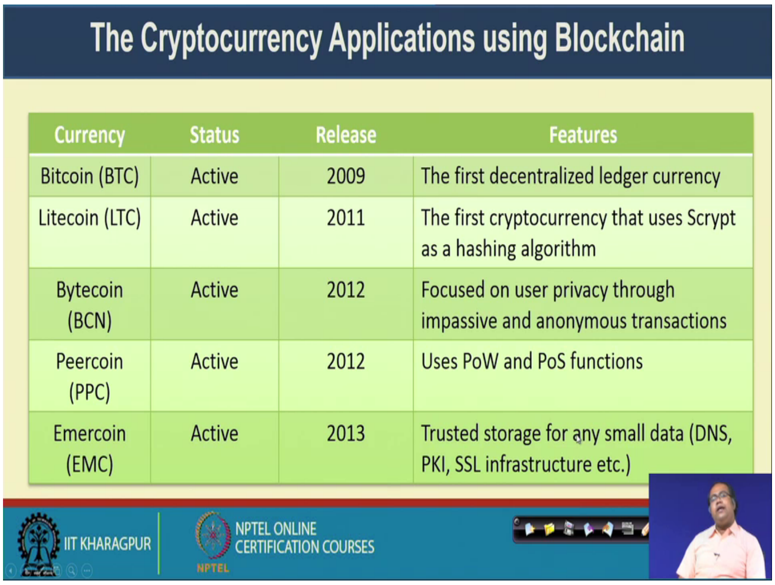
Orphaned Blocks

- The blocks which are not part of the longest chain

So, the other blocks which are there we call those blocks as the orphaned blocks. So, those blocks are not part of the longest chain. So, here this green chain is the longest chain. So, all the blocks in the green chain they are considered as the valid blocks and all other blocks, they eventually becomes orphaned blocks although in this case this also becomes the longest chain. So, you can you can consider this chain as well.

So, one of the chain from root to leaf whichever with the longest chain or if there are multiple chains, then out of the multiple chains one of the chain you consider as the main chain and other chains the blocks in the other chains, they will be considered as the orphaned blocks.

(Refer Slide Time: 11:07)



The Cryptocurrency Applications using Blockchain

Currency	Status	Release	Features
Bitcoin (BTC)	Active	2009	The first decentralized ledger currency
Litecoin (LTC)	Active	2011	The first cryptocurrency that uses Scrypt as a hashing algorithm
Bytecoin (BCN)	Active	2012	Focused on user privacy through impassive and anonymous transactions
Peercoin (PPC)	Active	2012	Uses PoW and PoS functions
Emercoin (EMC)	Active	2013	Trusted storage for any small data (DNS, PKI, SSL infrastructure etc.)

Now, let us look into few applications of blockchain, first we look into multiple cryptocurrency application. So, once the Bitcoin was developed in 2009 by Satoshi Nakamoto, which was the first decentralized ledger currency which had taken the concept of blockchain as its backbone.

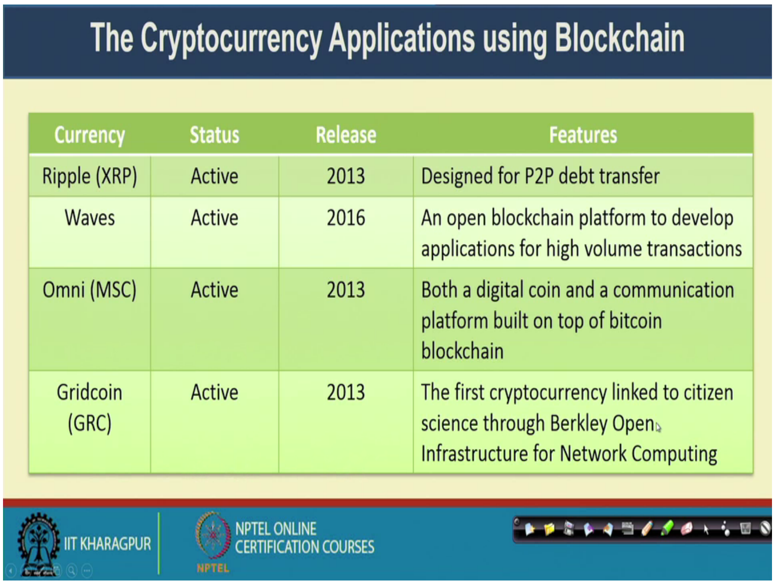
Multiple other such cryptocurrency mechanism came into practice and people have developed multiple types different type of mining and consensus algorithms, which have been part of their individual currencies. So, in 2011 we had the another cryptocurrency call Litecoin, which used a concept hashing algorithm call script, which is a lightweight hashing algorithm that have been utilized in litecoin.

Then in 2012 there is another cryptocurrency call bytecoin. So, the bytecoin it focused on user privacy through impassive and anonymous transactions. So, in case of your standard Bitcoin all the transactions are visible, but in that case they have a way to they have designed the way to hide the transaction, but still a mechanism to validate the transactions.

Then in peercoin which came in 2012, they used another consensus algorithm along with proof of work, which is called the proof of stake. So, the details of the proof of stake we will discuss while will concentrate on different kind of consensus algorithm. So, this peercoin it has taken P o S proof of stack as its mining algorithm.

Then in 2013 there was this emercoin, emercoin it developed an architecture to store small data which had can be utilized for the purpose of domain name system validation, public key infrastructure, SSL infrastructure to implement this kind of system, which requires a small database and for them this emercoin it provide data trusted storage architecture.

(Refer Slide Time: 13:09)



The Cryptocurrency Applications using Blockchain

Currency	Status	Release	Features
Ripple (XRP)	Active	2013	Designed for P2P debt transfer
Waves	Active	2016	An open blockchain platform to develop applications for high volume transactions
Omni (MSC)	Active	2013	Both a digital coin and a communication platform built on top of bitcoin blockchain
Gridcoin (GRC)	Active	2013	The first cryptocurrency linked to citizen science through Berkley Open Infrastructure for Network Computing

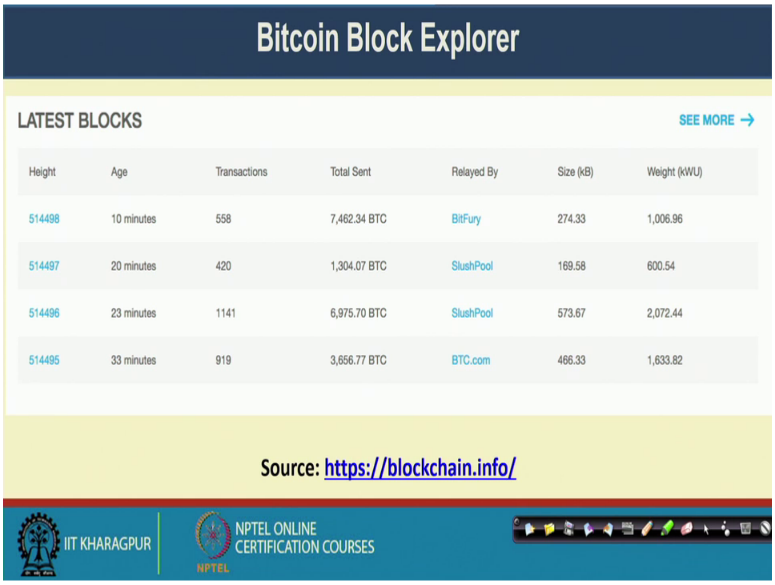
Then we had something called ripple which is a cryptocurrency, which was designed for peer to peer debt transfer. In 2016 we had seen waves which is an open blockchain platform to develop applications for high volume transactions, it supported higher throughput or significantly higher throughput compared to bitcoin, but it has a limitation like it cannot support a large number of nodes in the network, that is in that ride of which will explore later on.

Then there was a currency called Omni which came in 13, which used both as a digital coin and at the same time a communication platform, which was built on top of the Bitcoin blockchain and then 13 there was gridcoin the gridcoin was the first cryptocurrency, which is linked to citizen science.

So, citizen science are interesting application which is similar to that crowd funding application that I have mention, while talking about this concept of smart contract, where a group of people comes together and collectively they complete some task. So, this kind of environment in Berkley open infrastructure network computing they termed it as citizen science; so, this gridcoin that was utilized to support citizen science platform over a decentralized architecture.

So, these are some of the cryptocurrency applications which are developed over years, there are multiple other applications people are exploring on people have already developed and those are the basic advantage of those applications are that they are completely build on a decentralized platform, where you do not require a centralized storage architecture, but yet you can support multiple security and privacy then this kind of consensus this kind of properties over the system.

(Refer Slide Time: 15:02)



Bitcoin Block Explorer

LATEST BLOCKS

SEE MORE →

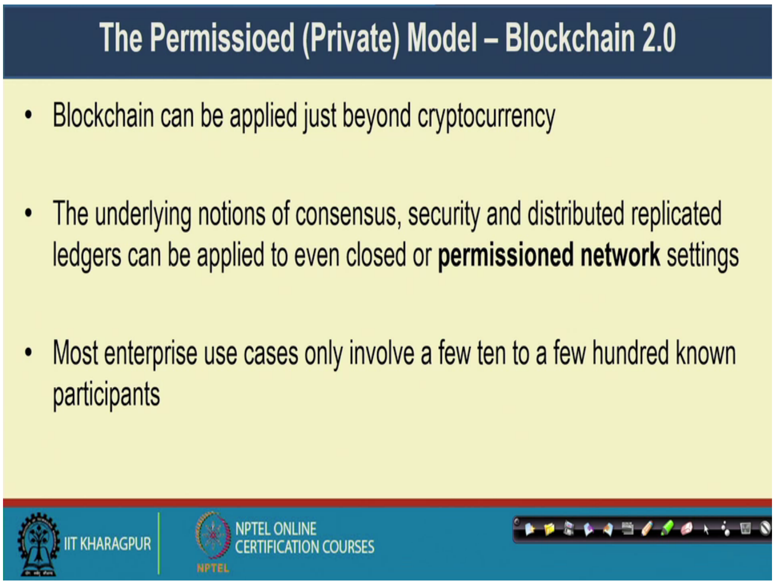
Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
514498	10 minutes	558	7,462.34 BTC	BitFury	274.33	1,006.96
514497	20 minutes	420	1,304.07 BTC	SlushPool	169.58	600.54
514496	23 minutes	1141	6,975.70 BTC	SlushPool	573.67	2,072.44
514495	33 minutes	919	3,656.77 BTC	BTC.com	466.33	1,633.82

Source: https://blockchain.info/

So, there is a interesting site that I have shown your earlier the Bitcoin block explorer. So, if you go to decide blockchain dot info, you can see the current blockchain which is behind the Bitcoin architecture. So, this snapshot I have taken during that time that was the height of the block. So, that was the yeah this was the height of the block 514498 and you can see that how much at what time that block was the get added.

So, from this block to this block it took 10 minutes, then this block to this block it took 3 minutes. So, at what time the block was mined and block was added to the network. Now all of this blocks may not be the part of the main chain main Bitcoin blockchain, but it may be some blocks are maybe the orphan blocks. So, by going to this blockchain dot info you can see, which are the which are the blocks which are part of the main chain and which are the blocks which are orphan blocks.

(Refer Slide Time: 16:14)



The Permissioed (Private) Model – Blockchain 2.0

- Blockchain can be applied just beyond cryptocurrency
- The underlying notions of consensus, security and distributed replicated ledgers can be applied to even closed or **permissioned network** settings
- Most enterprise use cases only involve a few ten to a few hundred known participants

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL

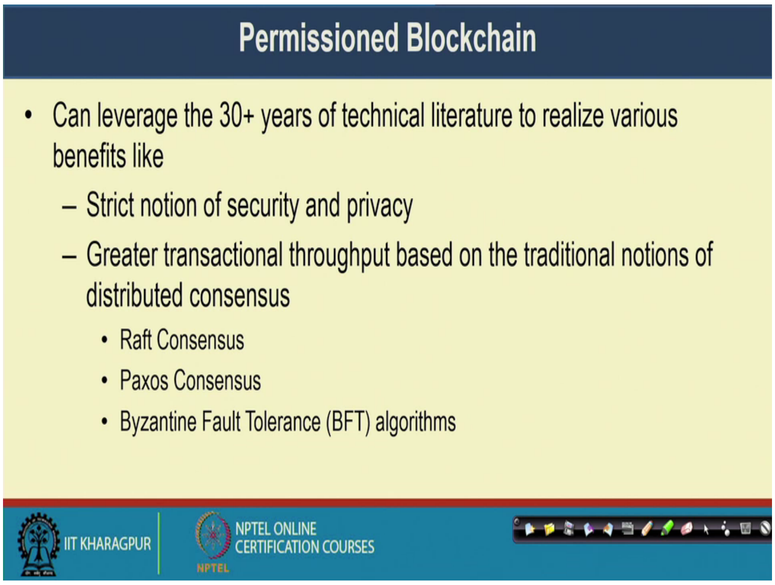
Now, in blockchain 2 we are little moving from this concept of permission less model to something called a permission model or a private model. So, in case of a permission model or a private model; so, this concept of blockchain the industry people they explore that is concept of blockchain, it can be applied beyond cryptocurrency. So, this underline notion of consensus security distributed replicated ledgers, they can also be applied to many kind of closed or permissioned network settings.

And interestingly most enterprises use cases most enterprises use cases, they consider this kind of closed environment or a permission environment where you have some few 10 to few 100 number of known participants, who are participating in a consensus procedure and or who are participating in that application, they want to share some information among themselves or they are collectively designing some kind of applications which will perform some predefined task.

So, from there we have the that concept of a permission model of blockchain, which came as a part of a blockchain version 2.

Now, in permission blockchain the interesting first is that the users or known a priori because your environment is close.

(Refer Slide Time: 17:29)



Permissioned Blockchain

- Can leverage the 30+ years of technical literature to realize various benefits like
  - Strict notion of security and privacy
  - Greater transactional throughput based on the traditional notions of distributed consensus
    - Raft Consensus
    - Paxos Consensus
    - Byzantine Fault Tolerance (BFT) algorithms

IIT KHARAGPUR

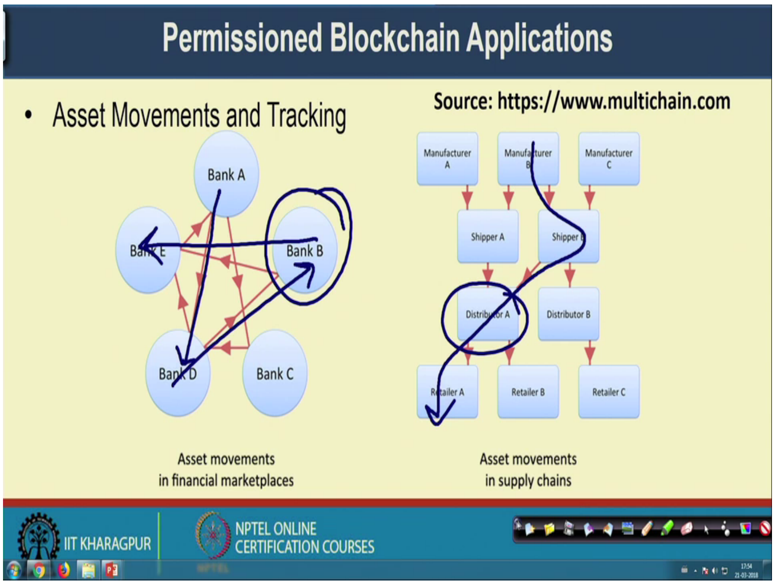
NPTEL ONLINE CERTIFICATION COURSES

Now, when your environment is close you may not require an consensus algorithm based on challenge response, which has its own disadvantages like it takes a significant amount of time to commit a block in the existing blockchain, because the consensus takes a significant amount of time and you have a re restriction on the size of the block.

So, in case of permission blockchain, you can leverage the existing distributed system consensus algorithm, which was developed in the last 30 plus years and those kind of algorithms it provide the stricter notion of security and privacy. And this supports greater transactional throughput based on the traditional consensus algorithm like this raft consensus, paxos, byzantine, fault tolerant consensus all this different kind of consensus algorithms will study later.

But this type of consensus algorithms, they provide significantly higher transaction throughput compared to the standard proof of work mechanism, which is a challenge response is mechanism and which is incorporated in Bitcoin architecture.

(Refer Slide Time: 18:45)



Permissioned Blockchain Applications

- Asset Movements and Tracking

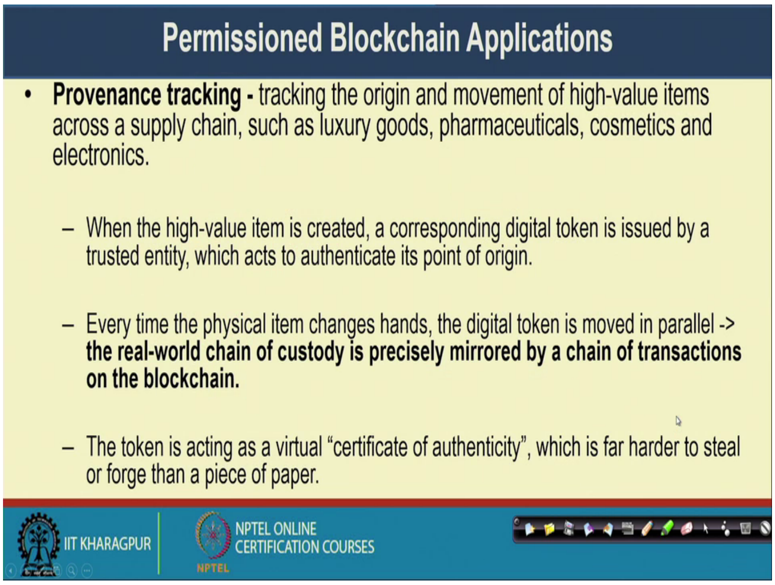
Source: https://www.multichain.com

Now, this kind of permission blockchain they have multiple application. So, one application can be in the direction of asset movings of tracking. So, here are 2 examples see in one examples, the assets are moving from multiple banking branches, say there kind of secured secured assets like the money which is moving from multiple banks or even the branches of multiple banks and you want to track, that what is the movement.

So, when it is moved from say bank A to bank D, then bank D to bank B, then bank B to bank E you want to monitor or you want to keep track of that. And you want to keep track of that in such a way so, that bank B cannot deny in a later time that it has not received that particular asset. Another application of this kind of asset movement can in the supply chain, where you have multiple manufacturers and the manufacturers sending the asset to the shipper.

The shipper is sending the asset to the distributor and the distributor is sending the asset to the retailer and you want to track the path that how a particular asset has been moved from manufacturer to shipper to which distributor to which retailer, and in such away in a secure way that distributor A will not be able to deny later on that he or she has not received that particular asset.

(Refer Slide Time: 20:14)



Permissioned Blockchain Applications

- **Provenance tracking** - tracking the origin and movement of high-value items across a supply chain, such as luxury goods, pharmaceuticals, cosmetics and electronics.
  - When the high-value item is created, a corresponding digital token is issued by a trusted entity, which acts to authenticate its point of origin.
  - Every time the physical item changes hands, the digital token is moved in parallel -> **the real-world chain of custody is precisely mirrored by a chain of transactions on the blockchain.**
  - The token is acting as a virtual "certificate of authenticity", which is far harder to steal or forge than a piece of paper.

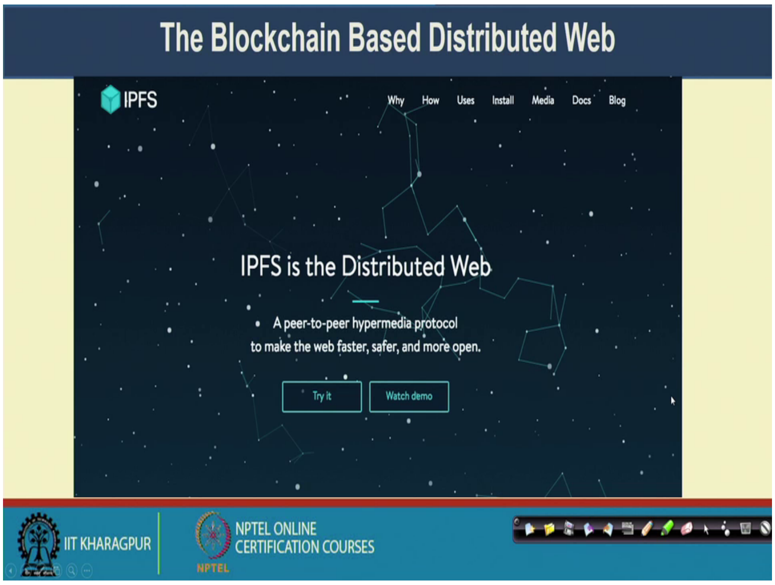
So, that way there are multiple applications and in this kind of particular application we can rely on the blockchain environment to design a nice solution like the provenance tracking, where you want to proof that a particular distributor or a particular person or intermediary has indeed received the asset. So, you are trying to track the origin and the movement of such high valued items, in a supply chain like say the luxury goods, the pharmaceuticals, the cosmetics, the electronics like that.

Now, how you can realize that in the blockchain? Like when the high value items is created, a corresponding digital token that can be issued by a trusted entity because here we are considering closed environment. So, all the supply chain all the stakeholders in the supply chain environments there known a priori. So, they can get this kind of digital token, which acts to authenticate its point of origin that mean the asset has originated at that point.

Now, every time the physical item changes the hands or changes its locate location, the digital token is moved in parallel. So, the real world change of custody, you can precisely mirror it inside a chain of transactions on the blockchain. So, as and when the asset moves from one supplier to one distributor to the next distributor, you can basically put a corresponding token in the blockchain and that particular chain that particular series of transactions, will tell you that how the assets has actually been moved. And because the information has been stored inside the blockchain no one will be able to deny it later on that, he or she has not actually received that particular asset or he or she has not forwarded the asset to another party.

So, this token it is acting like a certificate of authenticity, which is far harder to steal or forge than a piece of paper. So, if you are writing something on a piece of paper, it is easier to forge that compare to if you are putting it inside the blockchain and again the good thing here is that you do not have a centralized environment, that you can you do not need to rely on a centralized architecture to implement this kind of concept.

(Refer Slide Time: 22:25)



The Blockchain Based Distributed Web

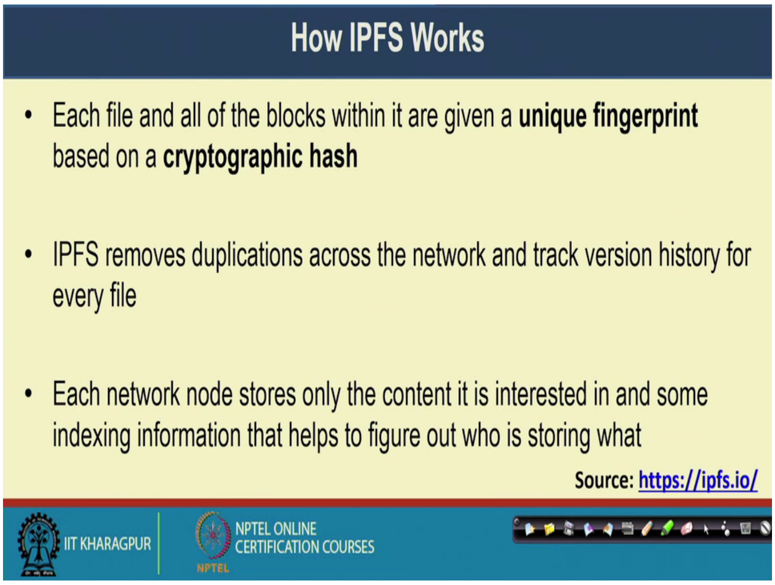
IPFS is the Distributed Web

A peer-to-peer hypermedia protocol to make the web faster, safer, and more open.

Now, another interesting application of this blockchain is, the implementation of a distributed way. So, there is this concept of call interplanetary file system. So, interplanetary file system actually implements the distributed wave architecture, where it combines the small storage elements or the small storage which is available in or individual devices, and by combining the small storages which is available to different users, you can actually construct a large storage. And the idea here is that whatever data I have in my storage possibly or in most of the time, that particular data is also available to multiple other users.

Now, if you can connect all those users together, then what you can possibly do that well the original data remains to only one users and for other users, you do not need to store that data what you can do? You can just keep a pointer that this data is available to this particular user. Now to make it failsafe, you can just keep some multiple replica of that data to few other users. So, that way this IPFS it can provides high availability of service whereas, avoiding the replication of the data or the replication of the files over multiple users.

(Refer Slide Time: 23:47)



How IPFS Works

- Each file and all of the blocks within it are given a **unique fingerprint** based on a **cryptographic hash**
- IPFS removes duplications across the network and track version history for every file
- Each network node stores only the content it is interested in and some indexing information that helps to figure out who is storing what

Source: https://ipfs.io/

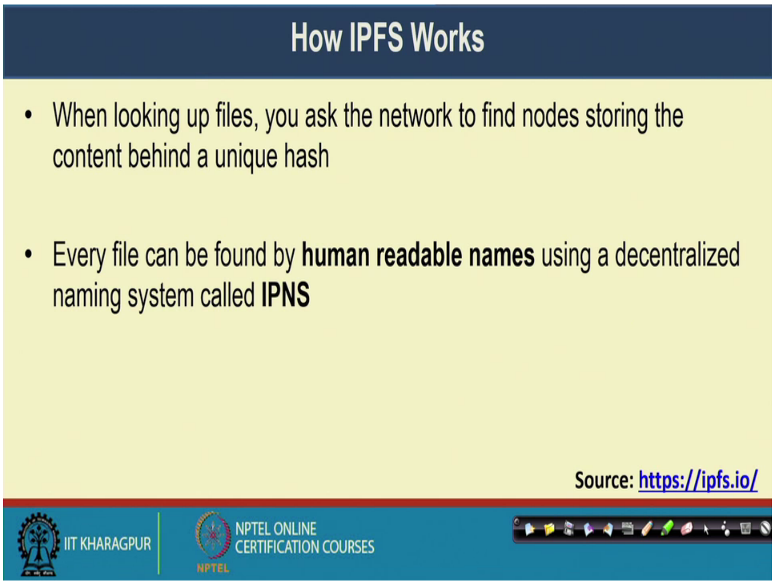
IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

So, this way this IPFS works. So, you can go to this site ipfs dot io when that is the opens project. So, you can just explore that are you can play with this IPFS tool. So, in IPFS each file and all of the blocks within it, they are given a in unique fingerprint through which you can identify a specific file or a specific block inside the file, which is based on the cryptographic hash function.

Now, IPFS it removes the duplication across the network to save the storage space and track version history for every file that if a file has been changed. So, it makes another replica of that file. So, that if some users wants the old version of the file he or she will be able to steal access the old version of the file. And each network node it stores only the content it is interested in and some indexing information that helps to figure out that who is storing what.

(Refer Slide Time: 24:42)



How IPFS Works

- When looking up files, you ask the network to find nodes storing the content behind a unique hash
- Every file can be found by **human readable names** using a decentralized naming system called **IPNS**

Source: https://ipfs.io/

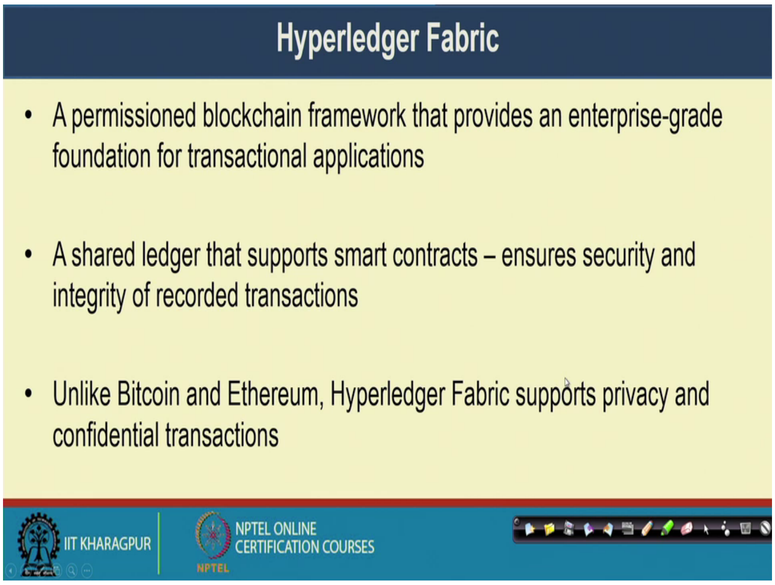
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL

So, when you are making a look up on the files. So, you ask the network to find nodes which are storing the content, behind that unique hash. So, every file is now have a unique hash function by using the unique hash function, you can make a look up that which user hash that current file. And every file that can be found by human readable names, that that IPFS also implement it using a decentralized naming system call IPNS interplanetary naming system.

So, what it does? This IPNS maps the names the human readable names to the corresponding hash entity. So, you can even such with that your human readable name. So, that way this indexing information, this indexing information is basically store inside the blockchain and what is the advantages of that? Say if you are if you are owning a file if a some file is you have some file. So, that information is there in the blockchain and everyone has that copy of the blockchain.

Now, later on you cannot deny that you do not own that file. So, that way IPFS ensures the availability of the file even in the presence of failure and it provides a secured way or a authentic way, to search the file over the internet.

(Refer Slide Time: 26:04)



Hyperledger Fabric

- A permissioned blockchain framework that provides an enterprise-grade foundation for transactional applications
- A shared ledger that supports smart contracts – ensures security and integrity of recorded transactions
- Unlike Bitcoin and Ethereum, Hyperledger Fabric supports privacy and confidential transactions

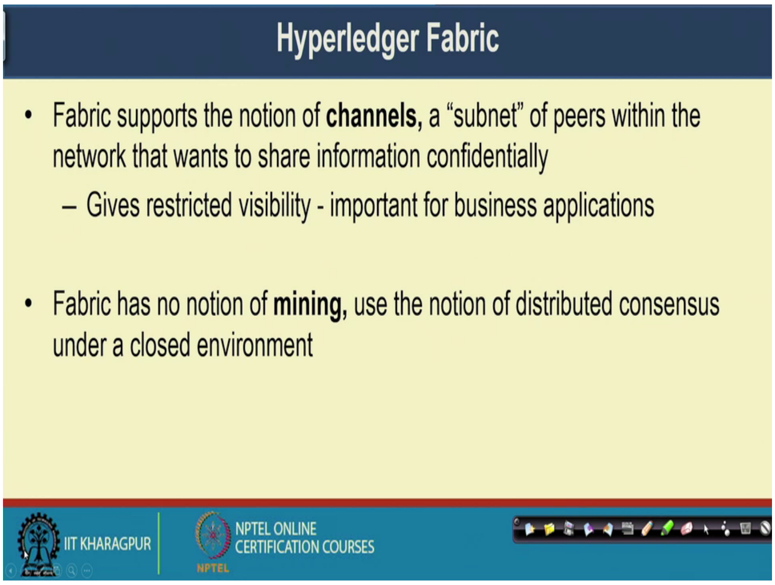
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL

Then there is one interesting platform to implement this kind of permission model of blockchain and this kind of permission model of blockchain, which is nowadays very important for the industry perspective to implement different kind of business application. So, a permission blockchain framework, it provides an enterprise grade foundation for transactional application. So, hyperledger fabric is a permission blockchain framework. So, it contains a shared ledger with support smart contracts and ensure security and integrity of the recorded transactions.

Now, this concept of the hyperledger fabric platform is little different from Bitcoin and ethereum. Ethereum is another platform for implementing blockchain application using. So, using ethereum platform you can implement decentralized applications or they are called as dapps. So, you can implement your own dapps using a ethereum platform.

So, the concept of hyperledger fabric list little different from Bitcoin and ethereum, in comparison with Bitcoin and ethereum hyperledger fabric it support strong privacy and confidentiality of the transactions which is not supported in case of Bitcoin or ethereum.

(Refer Slide Time: 27:27)



Hyperledger Fabric

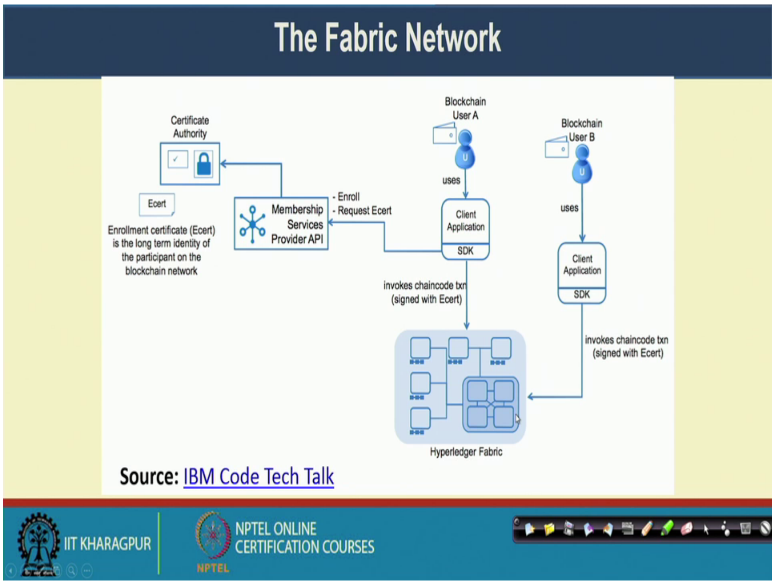
- Fabric supports the notion of **channels**, a “subnet” of peers within the network that wants to share information confidentially
  - Gives restricted visibility - important for business applications
- Fabric has no notion of **mining**, use the notion of distributed consensus under a closed environment

So, another interesting feature of hyperledger fabric it is that it supports the notion of channels. Channel you can think of it is a subnet of peers within the network who wants to share the information confidentially. So, that is important for the business perfective in case of business perfective, everyone should not have the same feasibility of the data. Some group of users or some group of peers has one level of feasibility some other group of peer has some other level of feasibility.

Say one group of people can see some 10 files, another group of people can see some 20 other files. So, using this concept of channel inside hyperledger fabric, you can implement this kind of architecture where you can provide or you can support this kind of partial visibility or restricted visibility, which is very important for business applications or for the smart contract applications.

Now, from the consensus perspective, because it is an closed environment or it is a permission environment. So, fabric does not have any notion of mining rather it is used a notion of this standard distributed consensus algorithm under a closed environment.

(Refer Slide Time: 28:40)



The Fabric Network

Certificate Authority
Ecert
Enrollment certificate (Ecert) is the long term identity of the participant on the blockchain network
Membership Services Provider API
- Enroll
- Request Ecert
Blockchain User A
uses
Client Application
SDK
invokes chaincode txn (signed with Ecert)
Blockchain User B
uses
Client Application
SDK
invokes chaincode txn (signed with Ecert)
Hyperledger Fabric
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

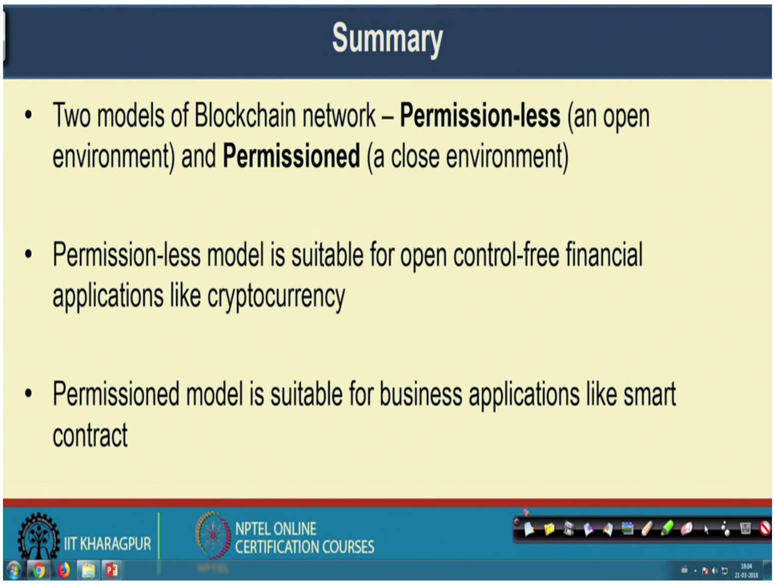
Source: IBM Code Tech Talk

So, this is typically of fabric network architecture. So, in a fabric network say you have this blockchain users. So, the block chains users take of first take a membership from a certification authority, which makes the environment that as closed. So, whenever a blockchain user. If it do not have a certificate at that time whenever it is participating in this blockchain application, it can contact with the certification authority and get a certificate by enrolling his name, that way you are making the environment closed and then it can invoke there is something called chaincode transaction.

So, this chaincode transaction, it implements the basic blockchain architecture in case of a permission model or in case of a closed model. So, they can invoke the chaincode transaction and put the transaction inside this blockchain platform which is maintain by fabric.

So, in later classes Praveen will give you the detail design and architecture of this fabric platform with some applications and coding that how you can implement your own application over the fabric platform. So, as you will progress on this course, we will go to the details of this blockchain fabric platform as a hands on new case.

(Refer Slide Time: 30:05)



Summary

- Two models of Blockchain network – **Permission-less** (an open environment) and **Permissioned** (a close environment)
- Permission-less model is suitable for open control-free financial applications like cryptocurrency
- Permissioned model is suitable for business applications like smart contract

So, in summary so, you have seen that there are two models of blockchain network, one is the permission less model for open environment and another one is the permission model, which is for a closed environment. Now, this permission less model it is suitable for open control free financial applications like cryptocurrency whereas, this kind of permission model which is suitable for business application like smart contract.

So, that is so, that is all for this week. So, in this week in summary you have discussed about the basic notion of blockchain and what are the different technical aspects, that we need to study to understand the functionality of the blockchain. So, I have given you a brief overview or a bird’s eye view of how the blockchain environment actually works, and what are the different applications both in the permission environment as well as in permission less environment, that you can realize using the blockchain architecture or the blockchain environment.

So, in the next set of classes we will go to the detail of this different mechanisms. So, we will start looking into the basic cryptography functionalities which are useful for implementing a blockchain architecture, at the same time we will look into the mining algorithms and the consensus algorithms in further details. And we will look into that what are the different ways people are exploring this blockchain system to make its more scalable or more useful for different kind of government as well as the industrial applications.

So, we will meet again in the next classes so.

Thank you.