

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

Lecture – 02
Introduction to Blockchain – II
(Historical Perspective)

Welcome back to the second lecture on Blockchain Architecture Design and Use Cases. So, in this particular lecture, we will look into the historical perspective of blockchain and how this concept of blockchain evolved over time and utilised in to different applications.

(Refer Slide Time: 00:39)

The Fundamentals

- **Cryptographically Secured Hash Functions**
 - **Hash Functions:** Map any sized data to a fixed size; Example $H(x) = x \% n$ where x and n are integers and $\%$ is the modular (remainder after division by n) operations. x can be of any arbitrary length, but $H(x)$ is within the range $[0, n-1]$.
 - **Cryptographically Secured:**
 - **One way**, given a x , we can compute $H(x)$, but given a $H(x)$, no deterministic algorithm can compute x
 - ✓ For two different x_1 and x_2 , $H(x_1)$ and $H(x_2)$ should be different

Handwritten notes:
 $x_1 \neq x_2$
 $H(x_1) \neq H(x_2)$
 $x_1 = x_2$
 $H(x_1) = H(x_2)$

Diagram: A box containing two circles, representing a hash function.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, basic fundamental which is very useful in context of blockchain so, the concept is cryptographically secured hash function. So, hash function is a function that map any sized data to a fixed size. So, for example, if you define hash function like $H(x) = x \text{ modulo } n$, where x and n are integers and this modulo is the modular operation; that means, remainder after division by n . So, if we define a hash function like this way; that means, in this case you can see that whatever be the value of x the value of $H(x)$ will be in between 0 and $n - 1$. So, this type of functions we call it a kind of hash function.

Now, one advantage of this hash function such that, we call them they are one way function; that means, given a x and n you can compute $H(x)$. But if $H(x)$ is given then you

cannot say that what is the corresponding value of x , you cannot say it uniquely. So, that is the property of a hash function and this concept of hash function is widely used in the concept of blockchain or indeed blockchain is nothing, but on data structure which is built upon this concept of hash function.

Now, this hash function concept of hash function is used widely in cryptographic context and then we call this kind of hash function as cryptographically secured hash function. Now, the properties of this cryptographically secured hash function is step first function is one way; that means, given a x you can compute $H(x)$, but given $H(x)$ you cannot compute x with any deterministic algorithm.

And the second property is that for any two different x_1 and x_2 , this H of x_1 and x_2 should be different; that means, if x_1 equal to x_2 then you should have a H of x_1 equal to x_2 for two different data set, but if x_1 not equal to x_2 then H of x_1 should not be equal to H of x_2 . So, this kind of hash function we call it as cryptographically secured hash functions.


(Refer Slide Time: 03:06)

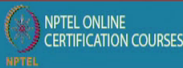
Cryptographic Hash Functions


- Examples: MD5, SHA256
- X is called the **message** and $H(X)$ is called the **message digest**
- A small change in the data results in a significant change in the output – called the **avalanche effect**

Input	cryptographic hash function	Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 468B FB7D CB22 823C ACC7 6CD1 90B1 EB6E 3ABC
The red fox jumps over the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEF2 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 48F4 1799 7D88 BCF8 92B9 6A6C

Image source: Wikipedia







Now, this kind of cryptographically secured hash function they have another important property which is called avalanche effect. So, what is an avalanche effect? So, avalanche effect is something like this. So, whenever we are defining a cryptographically secured hash function or sometime we will call it as cryptographic hash function.

So, this x is called the message and $H(x)$ is called a message digest. And an example of cryptographically secured hash function is MD5 or SHA-256. In next week class we will discuss about the details of this MD5 and SHA-256 the algorithms behind them. But the avalanche property of this cryptographically secured hash function or cryptography hash function is as follows, say given an input whenever you are computing the digest, if you make some little change in the input you will see significant change in the digest.

Say for example, whenever the input is fox this is the digest, whenever you make the input as the red fox jumps over the blue dog, you get this one as the digest. Now, from here to here you make a small change that the earlier one was that the red fox jumps over the blue dog.

Now, you make it the red fox jumps over the blue dog; that means, from over you are making a change at over, then you can see that there is a significant change between the message digest. So, the message digest are completely different. By looking into this message digest you cannot say that the original input was similar. Then from over you if you make it over you will see completely different message digest again by looking into this message digest we will not be able to say that the original input takes to accept.

Similarly over if you make it over again completely different message digest. So, this particular effect in cryptographically secured hash function it is known as avalanche effect; and avalanche effect ensures that just by looking into the digest it is nearly impossible to guess what was the input or even it is nearly impossible to guess that whether 2 inputs were similar by the just by looking whether 2 digest are similar or not. So, that is an important aspect for the blockchain context I will discuss why that is so.

(Refer Slide Time: 05:37)

Cryptographically Secured Chain of Blocks

- The first use - **time-stamp a digital document** (Harber and Stornetta, 1991)
 - A sequence of timestamps $[TS_1, TS_2, TS_3, \dots]$ denoting when the document is created or edited.
 - Whenever a client access a document, construct a block consisting of the sequence number of access, client ID, timestamp, a hash value from the previous request; and the entire thing is hashed to connect it to the previous blocks.

Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". *Journal of Cryptology*. 3 (2): 99–111

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So let us now go back a little bit about history that the use of this kind of cryptographically secured hash function in chains or blocks from where the concept of blockchain gradually evolved. So, the first use of this concept of cryptographically secured chain or blocks it came in 1991 in a paper by Harber and Stornetta. So, they have developed an mechanism for time stamping a digital documents. So, you have a digital document and that document is edited by multiple person purpose peoples time to time.

So, one person has first created the document, then person 2 has edited the document, then person 3 has edited the document and you want to maintain a list of time stamp when the document has been first created followed by when the document was edited in a subsequent way, but in a secure way.

So, such that no people will be able to make a change in the time stamp value. That is important from the document purpose because many of the time you want to see when document was last edited or if some people claim that I have not make any editing in the document you want to see that whether that person has actually make an edited editing in the document or not.

So, to solve this particular problem Harber and Stornetta they have used this concept of chain of blocks they have not palm this as a blockchain, but the concept is similar to (Refer time: 07:00) blockchain. So, what they did? So, they have taken a parameters like the initial number the initial say in what order the people have accessed. So, it has started

from 0 1 2 3, then corresponding change value the constructs. So, that block is something like that whenever client access a document you construct a block like this which contains the sequence number sequence number of access, this C1 C2 C3 C4 at the client I D where access the block then the corresponding time stamp value, the time stamp value and the hash value from the previous request. So, this is important.

So, initially you have some hash value H 0 and whenever your having this block information you have this information, you make a hash of this enter information and get this value H 1.

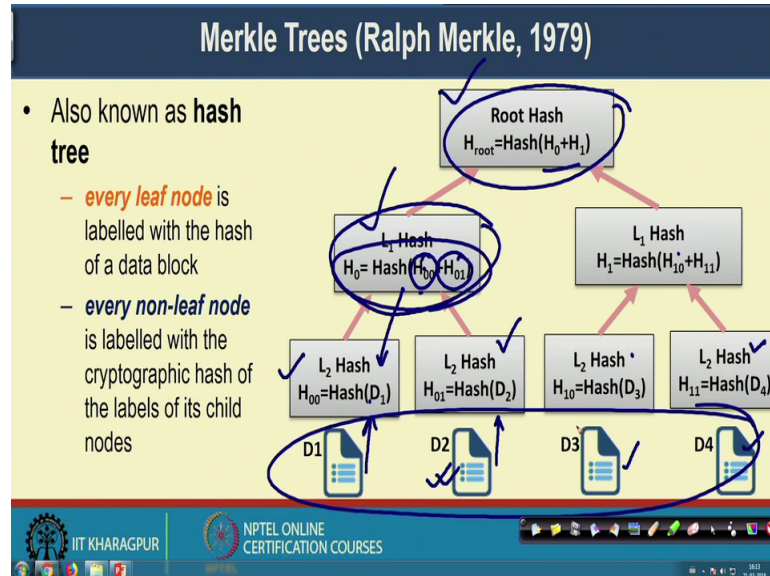
Now, this value of H 1 will be used in the next case, when the client 2 will access or make an editing in the document. Then again by taking this values; that means, that the sequence number the client who has made by editing the time stamp and hash value of the previous one, you again generate a hash values which is H 2 and this H 2 will be a used in the next iteration when client 3 will access the document or make an editing in the document. Then from here you generate H 3 and this H 3 will be used when client 4 will make some editing in the document. Now in the advantage of this hash chain is that if you want to make same change in the time stamp value.

Say for example, if you want to make change in time stamp 1; that means, you have to change the value of H 2 H 3 H 4 all the subsequent hash values and people will able to observe that all this values have been changed for example, client 2 will be able change that his hash values that has been changed, and that way they will be able to detect that someone is trying to tampering the document, tampering the timestamp value which is there; So, that way this concept of this concept of chain of blocks by connecting them by the hash function, that was used to cryptographically securing the timestamp value of a digital document.

So, this particular architecture looks like something similar to blockchain, where you have multiple blocks of data and this blocks of data are connected by hash value. So, here this second block it is connected with the first block by this H 1, then block 2 it is connected to it block 1 by this hash value, then block 3 it is connected to it block 4 it is connected to block 3 by this hash value. So, that way this individual hash values are helping to connect the blocks one after another and making the block as tamper proof.

That was the first use of this concept of the chain of blocks which was an earlier version blockchain in securing this digital document.

(Refer Slide Time: 10:20)



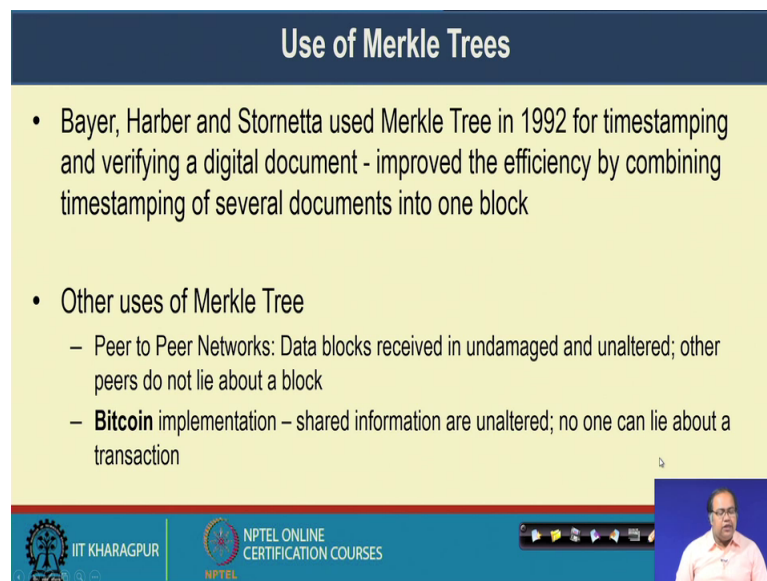
Now, the next concept another concept which is widely used which what is the foundation for blockchain concept it is called the markle tree. So, what is a markle tree let me explain it with this example. So, markle tree is a tree structure, where the leaf nodes they will contain the hash of the document and every individual individual node or intermediate node, they will contain the hash of the combination of the left child under a right child.

So, this is an example of a markle tree. So, the leaf node it contains the hash of the content of this document. So, this leaf node contain the hash of D 1, this leaf node contains the hash of D 2, this leaf node contains the hash of D 3 this leaf node contains the hash of D 4 and then this level 1, the intermediate node it contains the hash of these 800; that means, the hash value of D 1 plus the hash value of D 2 and the and their combined hash value then at root level.

So, this is a example of a binary markle tree in root level, the root contains the combined hash of its left child and a right child. That means, if you are making any change in this document, that change will get reflected in this hash value this hash value as well as this hash value.

Now, if you want to secure a number of documents together so, here assume that you want to secure all these 4 documents together, then you have the advantage that you can propagate this root value. So, the root value if there is any change in any one of these 4 documents, then that change will get reflected in the root value and that way that way you have the advantage that, you can collectively secure a number of documents together by using this concept of merkle tree.

(Refer Slide Time: 12:27)



Use of Merkle Trees

- Bayer, Haber and Stornetta used Merkle Tree in 1992 for timestamping and verifying a digital document - improved the efficiency by combining timestamping of several documents into one block
- Other uses of Merkle Tree
 - Peer to Peer Networks: Data blocks received in undamaged and unaltered; other peers do not lie about a block
 - **Bitcoin** implementation – shared information are unaltered; no one can lie about a transaction

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, this concept of merkle tree was actually used in 1992 by extending the work where the earlier people in 1991 they have developed a chain kind of architecture to secure the time stamp values in a digital document and their here in 1992, Bayer Herber and Stornetta they have developed a mechanism where, they have used a merkle tree to secure the time stamp values for a number of documents for set of documents.

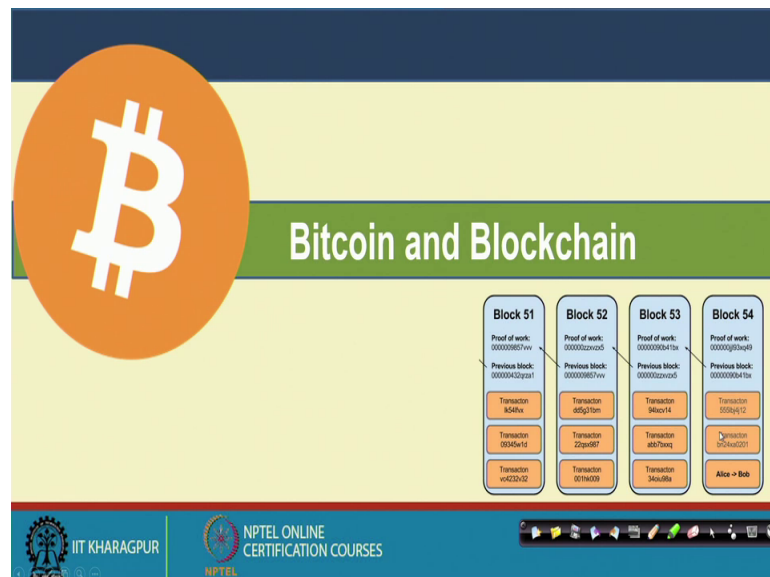
Now, there can be other uses of merkle tree like in a peer to peer network whenever you are sharing a set of data blocks you want to ensure that the data blocks are received in a unmanaged and a unaltered way. So, and other peers they are not lying about a block like they are sharing a block, but that block is not a updated block.

So, in that case if you share the root hash of the merkle tree, which is called as the merkle root; if you share the merkle root the merkle root ensures that non of the documents has been altered. Another use full of the merkle tree is the implementation of

the Bitcoin, which is the most popular cryptocurrency which actually worked as the foundation of this concept of this bit bit blockchain.

So, in case of bit can also you want to find out that the shared information which is there, that information's are unaltered and no one is lying about some old transaction. So, there also you can construct a merkle tree of all the transactions together and if same one is just denying one particular transaction, your merkle root will change and by looking into the merkle root you will able to validate that whether the set of transactions have been transmitted form one node to another node in a unaltered way or not.

(Refer Slide Time: 14:08)



Now, as Bitcoin worked as the foundation behind this white spilt popularity of blockchain concept, let us look into the of concept Bitcoin in a later on I will have a detail discussion about bit coin methodology.

(Refer Slide Time: 14:25)

What is Bitcoin?

- Bitcoin is a **completely decentralized, peer-to-peer, permissionless** cryptocurrency put forth in 2009
 - **Completely decentralized:** no central party for ordering or recording anything
 - **Peer-to-peer:** software that runs on machines of all stakeholders to form the system
 - **Permissionless:** no identity; no need to sign up anywhere to use; no access control – anyone can participate in any role

* Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008)
(<https://bitcoin.org/bitcoin.pdf>)

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, Bitcoin it is a complete decentralised peer to peer and permission less cryptocurrency which was put forth in a 2009 in a white paper by Satoshi Nakamoto in this paper, “Bitcoin: A peer-to-peer electronic cash system”, it was a white paper were Satoshi Nakamoto first proposed the concept of digital cryptocurrency. So, the basic philosophy behind this Bitcoin architecture is that, first of all it is completely decentralised; that means, there cannot be any central party for ordering or recording or controlling your currency just like bank or government.

So, that was actually the concept which came from few mathematician and the philosopher that, that why my money will be controlled by a bank or a government agency, which is a centralised authority. So, I do not want my asset to be controlled by any centralized authority that was a debatable philosophy.

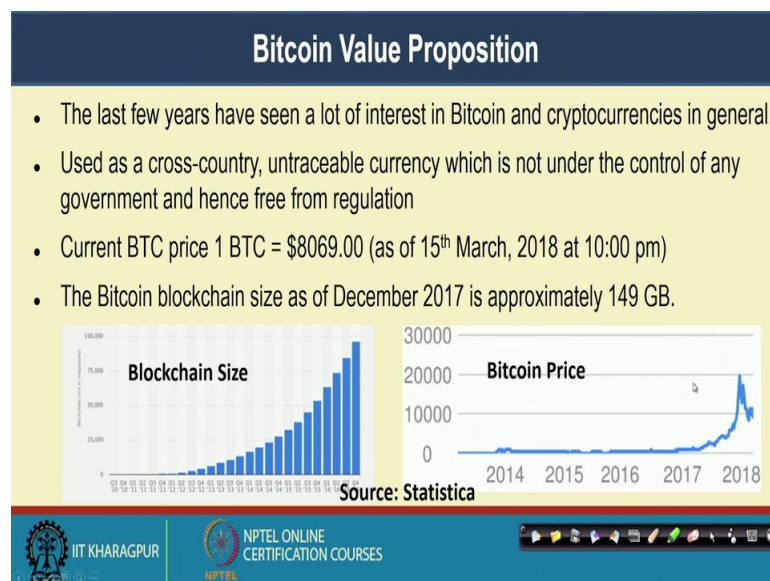
So, we are not going to that particular philosophy, but that philosophy that actually give this cryptocurrency and Satoshi Nakamoto through this Bitcoin paper he as given given practical inflammation of a digital currency or crypto currency, which is completely decentralised where no central authority like a bank or a government will have control over the currency.

The second property is the peer to peer that means the software the Bitcoin software it runs on the machines of all the stakeholders to form the system; that means, you do not have a central system with which all the peers are connected rather you have a complete

decentralized system where individual peers are connected with each other and they share the information among themselves. And third important philosophy behind is Bitcoin idea is that that it is permission less; that means, you does not any identity you do not require any identity to join Bitcoin network. Anyone can join the Bitcoin network and perform a transaction.

So, this gives raise to an very important and interesting question, that whenever you are allowing multiple parties join in our network to join in your financial transaction system, how will you ensure the security of the system because the persons who are joining because you are not authenticating them. So, they can be malicious or they can perform malicious activity. So, you have to develop system which will sustain in the presence of such kind of malicious attack. So, that was the interesting concept which was put forward in this Bitcoin architecture.

(Refer Slide Time: 17:02)



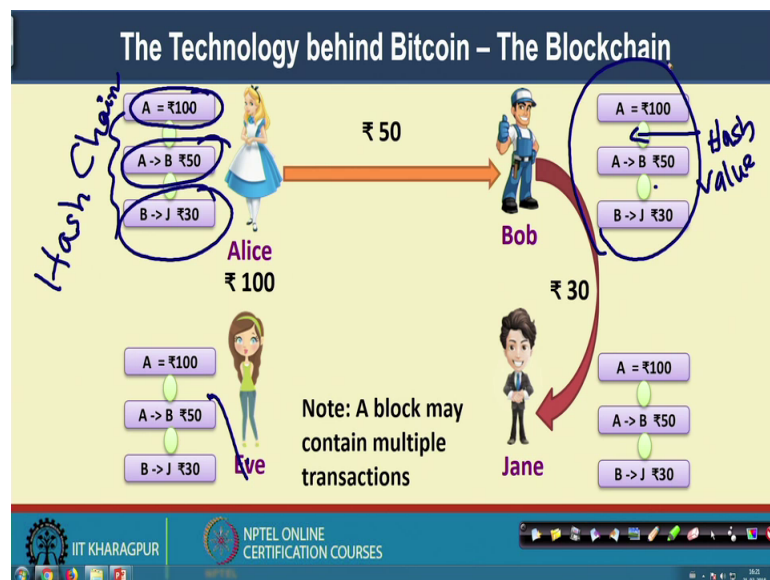
So, just a kind of a statistical information about Bitcoin that in last few years we have seen a lot of interest in Bitcoin and cryptocurrencies in general. So, it is used as a cross country untraceable currency, because there is no government control or the centralised control. Then the current Bitcoin price I have just recorded it in on 15th March 2018 at 10 pm and the value is fluctuating significantly over days.

So, if you look it today in Google you will possibly find out something different. So, on that day the currency one Bitcoin was some 8069 dollar, the price was 8069 dollar and if

you look in to the Bitcoin price increased that it reached on around 20,000 dollar in the earlier of in the last of last year and first month of this year and then right now, we are just observing deep in the price. And if you look into the blockchain size or blockchain worked as the backbone of this Bitcoin architecture.

So, if you look into the black blockchain as of December 2017, it is approximately around 149 GB. So, the size of the blockchain is actually growing exponentially. So, if you look into this left side graph, in the left side graph you will see that the growth of this blockchain size which actually stores the information of Bitcoin it is growing exponentially.

(Refer Slide Time: 18:32)



So, the technology behind Bitcoin is the blockchain. So, the way I have discussed in the last class about the public ledger the same thing is applied here.

Now, we are storing this transaction information in a block. So, every block contains the transaction information, those are the first block here contains the value that Alice poses; that means, there is a 100 with her, then she makes the transaction of this 50 to Bob. So, the next block contains that particular transaction, now Bob transacts say rupees 32 Jane.

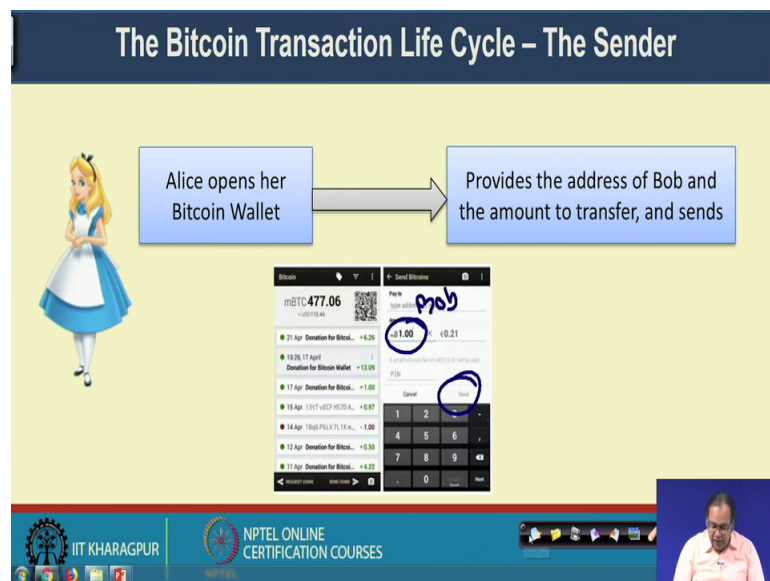
So, that is the third transaction and all these transactions are connected with each other though this concept of hash chain, I will discuss it sometime later lectures that what is the hash chain.

So, the concept that I discussed earlier in the context of digital documents that similar kind of architecture, where individually individual blocks are connected by a hash value. So, this circles are nothing, but a hash value, which is connecting the individual blocks together. So, that way this entire blockchain is coming into practise and the concept of decentralisation come into practise that, the copy of the blockchain is available to every individual party.

So, Alice has her copy of the blockchain Bob has his copy of the blockchain, Jane has his copy of the blockchain and Eve has her copy of the blockchain. So, every individual parties posses their own copy of the blockchain and whenever there is a transaction those transactions are get included in the existing blockchain.

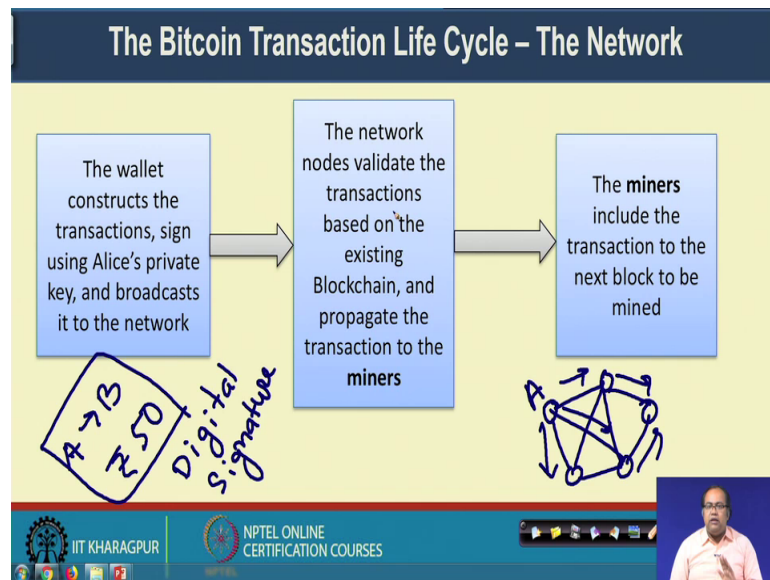
Now, one notice here that in this example I have shown one transaction in one block, but in reality there can be multiple transactions in single block, indeed there can be more than thousand transactions in single block.

(Refer Slide Time: 20:25)



So, let us look into the Bitcoin transaction life cycle, whenever Alice want to send some money to Bob, how it actually works. So, initially Alice see opens her Bitcoin wallet and provide the address of Bob and amount to transfer and same step. So, this is an example Bitcoin wallet. So, Alice gives the address of Bob here and then provides the money to transfer and then he press the send button. So, once you press the send button.

(Refer Slide Time: 21:03)

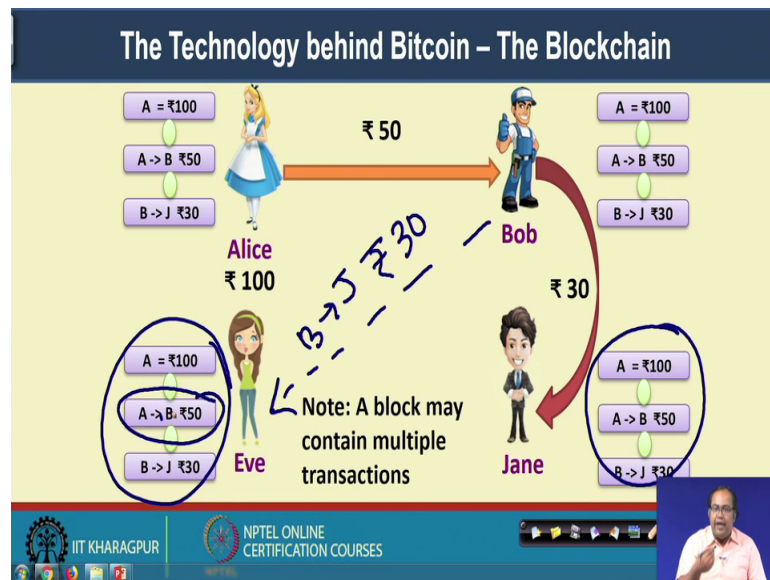


Then the wallet it constructs the transaction. So, so it makes transactions like say Alice to Bob of rupees 50, a transaction like that and this transaction is signed using Alice's private key. So, this concept of signing so, this is the concept of digitally signing a document. So, we call it as digital signature. So, by applying the digital signature techniques I will discuss the concept of digital signature later on by applying the digital signature technique so, Alice.

So, that wallet it signs the transaction made by Alice and broadcast it over the network. So, as you look know that this enter note network is the kind of peer to peer network everyone is connected to it others to some means say this is Alice. So, Alice wallet it makes or it broadcasts this transaction over the network. So, all the nodes in the network or at list majority of the nodes in the network, receives that particular transaction.

Now, this network node they validate the transaction based on the existing blockchain. Now that is another interesting fact about blockchain. So, in this slide we have see that this blockchain individual blockchain, they contains the all the transaction records. So, whenever Bob is sending this transaction of rupees 30 to Jane and this information is broadcasted to all the node.

(Refer Slide Time: 22:49)

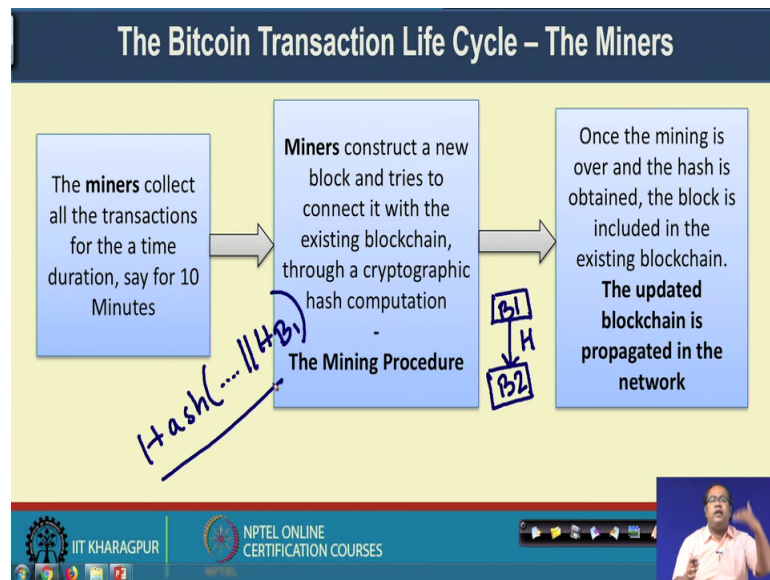


So, the information also reaches to if that Bob has made a the transaction to Jane of rupees 30. By looking into this blockchain Jane if can verify that whether this particular transaction is a valid transaction or not. So, she finds out that well Bob has received this 50 form Alice. So, currently Bob has rests 50 with him. So, Bob is legitimate to make a transaction of rupees 30 to Jane. So, this transaction is a valid transaction.

So, that way by looking into the exiting blockchain you can validate whether the transaction is a legitimate transaction or not. Now, once this transaction is validated, then this transaction are propagated to special some special node call miners and the task of the miner is to include the transaction to the next block will be mined.

That means, the task of the miner is collecting all the transactions from the client which was there for say last 10 minutes and their task is to construct a new block and then apply a mechanism called mining, I will discuss the mining mechanism later on apply the mechanism of mining to connect that block with the existing blockchain.

(Refer Slide Time: 24:10)



So now, we are coming to the minors. So, the miner they collect all the transactions all the transactions for a time duration say for 10 minutes and the miners they construct a new block and tries to connect it with the existing blockchain through some kind of cryptographic hash computation.

So, in a blockchain concept as I have mentioned earlier that every block is connected to the next block through some cryptographic hash function say this is B 1 and this is B 2. So, B 1 is connected to B 2 with some hash function and ideally what is there just to give you an hint that, whenever your computing this hash function for B 2 this hash function will contain some parameter along with the hash value, which was there for B 1. So, that way this B 1 it connects the next block B 2 and the task of the miner is to solve this hash problem in a difficult to it.

So, this hash problem which is given to the miners, it is a computationally difficult problem and that computation is difficult problem every miner needs to solve and one of the miner or sometime more than one miner they solve that problem and they are able to connect that block with the existing blockchain. So, the this is again I am saying that this is broad overview of the entire methodology, the details methodology I will discuss later on this is just a kind of introduction to you about how the whole system works.

And once this mining is complete then the hash is obtained and the block is included in the existing blockchain and this updated blockchain is propagated in the network. That

means, every nodes every participating node in the network, they receives the copy of this updated blockchain.

(Refer Slide Time: 26:07)

The Bitcoin Transaction Life Cycle – The Receiver

Bob opens his Bitcoin Wallet and refreshes, the blockchain gets updated

The transaction reflects at Bob's wallet

A → B
₹30

currency	rate	balance	date	description
USD	708.41	337952.50		
USD (default)	0.24	112.44		
UYU	6.17	2964.04		
UZS	593.90	283222.42		
VET	1.50	713.64	April 21, 15:18	18CK5A1gajRK K5C7yVST X79L Uzbh...
VND	5112.73	243909.32		
VUV	25.04	11946.69		

mBTC 477.06

18CK5A1gajRK K5C7yVST X79L Uzbh...

18CK5A1gajRK K5C7yVST X79L Uzbh... +13.09

18CK5A1gajRK K5C7yVST X79L Uzbh... +1.00

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSES

And once they receive the copy of the updated blockchain then Bob also receives that copy of the updated blockchain and once Bob receives that copy of the updated blockchain. So, best or by looking into the blockchain be Bob can find out well inside that updated block there is a transaction from Alice to Bob of say it is 30. So, Bob can view this transaction and once Bob is able to give this transaction, Bob can update this value to it is to his wallet so, the current value of Bitcoin that has been transferred from Alice to Bob that gets reflected to the wallet of Bob.

So, this transaction gets reflected to Bob and Bob can validate the transaction. So, this way the entire Bitcoin transaction works that whenever Alice wants to make a transaction of rupees 30 to Bob, and at the back bone the blockchain ensures that this particular transaction is a legitimate transaction or it is valid transaction. So, every individual user or individual node in the network they maintain their local copy of the blockchain and as you understand that, you need a complicated mechanism to ensure that all this local copies which are available to the individual nodes they are indeed the updated copy or the legitimate copy.

So, and or they are the kind of valid copy. So, once every node trans that well have a valid copy of the blockchain and they receives a new transaction. So, they can validate

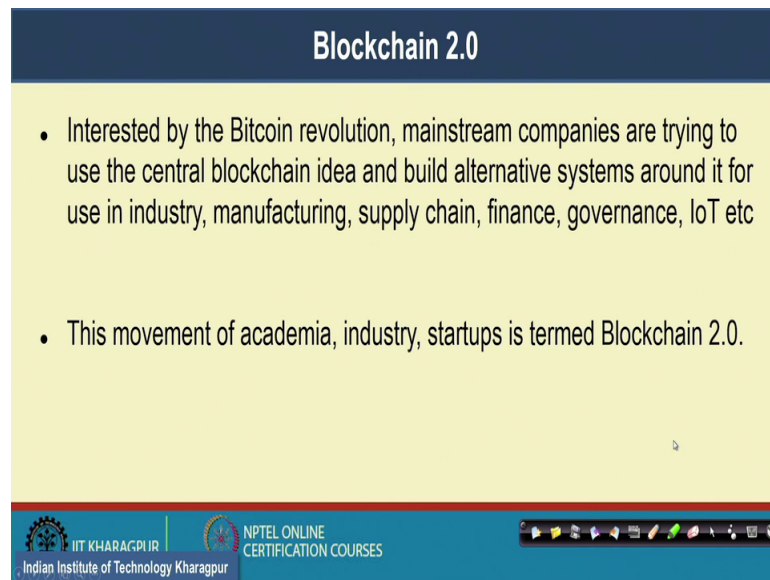
that new transaction against this copy of the blockchain and then the miners they collect all such transaction which are the valid transaction and miners also have a the capability to check the validity of a transaction. So, once the minor checks the validity of the transaction, then the miner can apply this mining process where they solve upcomputationally difficult cryptographic problem, where their task is to compute a hash function, but not a very simple hash function rather a difficult hash function and that difficulty level basically governs the complexity of the system.

So, once the miners solves that particular hash function, using this hash function the new block is added to the existing block. And that way the blockchain size of the blockchain gradually increases. So, as the transaction comes in new blocks are generated and blocks are added to the blockchain and this updated the copy of blockchain is propagated to the all the users.

And every user can see that whether there is any transaction which is intended for themself inside a block, and if there is any transaction which is intended for themself inside the block, they can include that transaction in the in their wallet. So, that way the transactions are performed with the help of a blockchain.

So, you can see that there is no such centralised authority like bank, which is controlling this entire transaction rather this enter transaction is controlled in complete distributed to a and there are many nice properties or interesting properties in this mechanism that will discuss in subsequent classes.

(Refer Slide Time: 29:32)



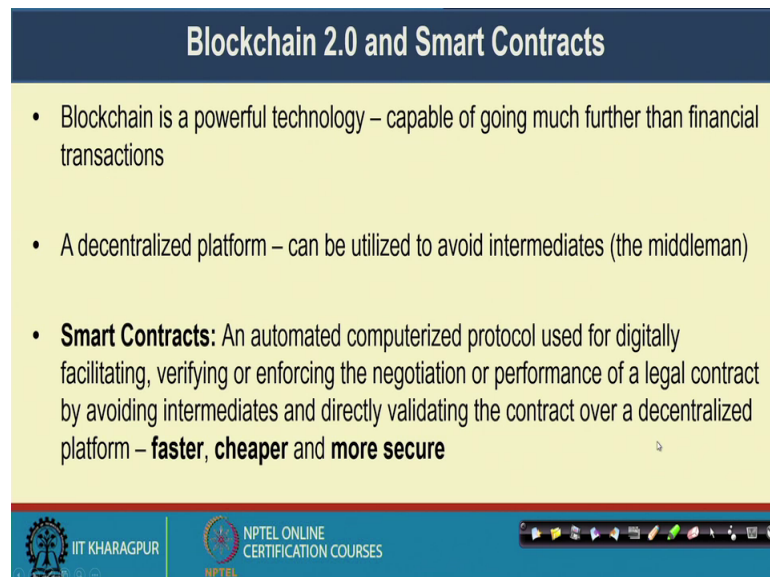
Blockchain 2.0

- Interested by the Bitcoin revolution, mainstream companies are trying to use the central blockchain idea and build alternative systems around it for use in industry, manufacturing, supply chain, finance, governance, IoT etc
- This movement of academia, industry, startups is termed Blockchain 2.0.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES
Indian Institute of Technology Kharagpur

So, based on this blockchain concept blockchain initial concept, there was this concept of blockchain 2, which was based on this bitcoin revolution. So, the concept of blockchain gradually applied to multiple other sectors like the academy industry and many of the start ups it is termed as blockchain 2.

(Refer Slide Time: 30:00)



Blockchain 2.0 and Smart Contracts

- Blockchain is a powerful technology – capable of going much further than financial transactions
- A decentralized platform – can be utilized to avoid intermediaries (the middleman)
- **Smart Contracts:** An automated computerized protocol used for digitally facilitating, verifying or enforcing the negotiation or performance of a legal contract by avoiding intermediaries and directly validating the contract over a decentralized platform – **faster, cheaper and more secure**

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES
NPTEL

And this concept of blockchain 2 that was extended for another interesting application, which is known as smart contract; So, a smart contract is that a smart contract basically provide a decentralized platform, which can be utilised to avoid the intermediarity in a in

a contract. When 2 persons are coming to a contract we have something like a legal advisory who is basically controlling this kind of contracts. So, there are some kind of middle man. So, with the help of this kind of blockchain environment, you can avoid the intermediaries or the middle mans.

So, this concept we is known as the smart contracts. So, this smart contracts provides on faster cheaper and more secure way for executing the contracts in a decentralised environment. So, in the next class will go to the details of this smart contracts in details, and we will look into that how you can develop applications using blockchain which will facilitate the use of smart contracts. So, we will discuss again during the next class, about this smart contact technology by utilising the blockchain environment so.

Thank you.