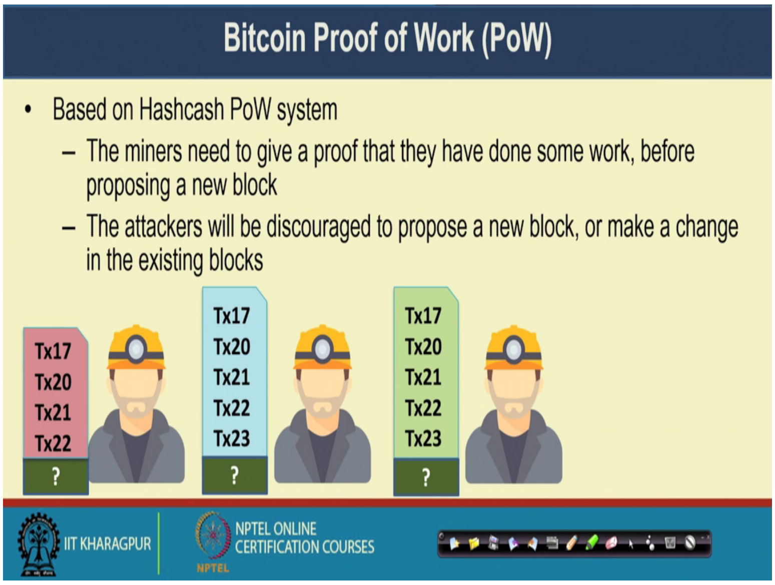
Blockchains Architecture, Design and Use Cases
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 12
Consensus in Bitcoin – II (Pow and Beyond)

Welcome back to the course on Blockchain Architecture Design and use cases. So, in the last class will have seen about the basic proof of work mechanism in hashcash. And today we will looking to that how bitcoin hashcash extends that, how the bitcoin proof of work extends the hashcash proof of work base system. And develop methodology to protect the blockchain by applying a distributed consensus mechanism. And along with that we will also look into several other consensus algorithms, which are being applied on a permission less model of blockchain, which are most similar to bitcoin based architecture and how they utilize the concept of consensus to ensure a secure tamper proof blockchain?

(Refer Slide Time: 01:15)



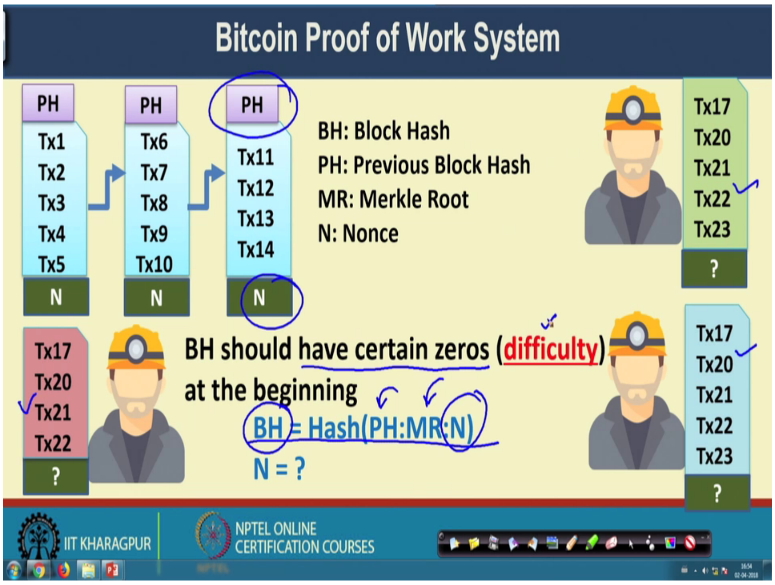
Bitcoin Proof of Work (PoW)

- Based on Hashcash PoW system
  - The miners need to give a proof that they have done some work, before proposing a new block
  - The attackers will be discouraged to propose a new block, or make a change in the existing blocks

So, this bitcoin proof of work it is based on hashcash proof of work system. So, the minors who are the special notes in bitcoin network who participate in the consensus procedure, they need to give a proof that they have done some work before proposing a new block.

So, if they can successfully complete that work then they are able to submit that block as a part of the existence existing longest chain of the block chain. Now, the attacker they will be in general discourage to propose a new block or make a change in the existing block, because they have to do the entire work of the blockchain, which is computationally difficult in a in a generic environment.

(Refer Slide Time: 02:00)



Bitcoin Proof of Work System

BH: Block Hash
PH: Previous Block Hash
MR: Merkle Root
N: Nonce

BH should have certain zeros (difficulty) at the beginning

$BH = Hash(PH:MR:N)$

$N = ?$

So, this is the methodology for bitcoin proof of work system. So, in case of bitcoin proof of work system, you have an existing blockchain. So, if you remember the basic blockchain architecture, in the basic blockchain architecture, every block is connected to the previous block with the hash value. So, here this PH is the hash value of the previous block. So, we have this the previous hash value and one nonce value, which is included in every block.

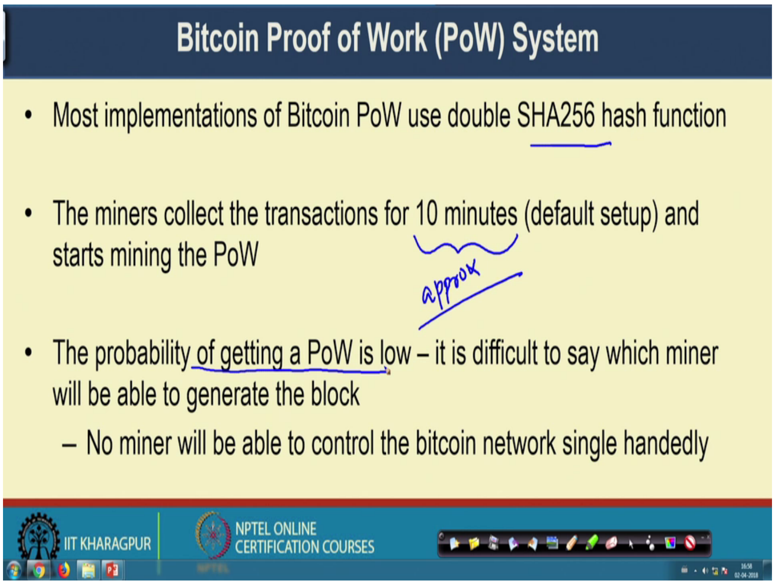
So, we need to encode or we need to include is one of these existing 3 proposed blocks with the existing blockchain. So, every minor they will try to find out a nonce value, which will satisfy certain hash equation. So, this is the hash equation that they have to perform.

So, you have the previous block hash along with you have the merkle root of the transaction. So, if you remember that all the transactions are arranged in the form of merkle tree, which is again a hash based architecture under root of the merkle tree contents the root hash, which we call as the merkle root. So, it includes the merkle root and along with a nonce value. Now, these blocks hash value it has a given challenge. So, the challenge is that you have to ensure certain number of zeros at the prefix, just like we have did in the hashcash based system.

So, this is termed as the difficulty of the system now the minors they will try with different values of nonce. So, they will try with different values of nonce to find out that for which hash value or they have to find out a certain block hash value, which has or which satisfies the difficulty given difficulty that is certain number of zeros at the prefix of the hash value. Now, every individual minor they will independently try to find out this nonce value and the minor who will be able to first find out the nonce value for his own block his or her own block, then he or she will be able to include that block as a part of the blockchain as a part of the existing blockchain.

So, this is the proof of work based system, which is utilized in bitcoin to ensure the consensus by utilizing challenge response base systems, here the challenge is that by changing the nonce value you have to find out hash with certain difficulty level; that means, to it is certain number of zeros at the beginning or better to stay a maximum number of zeros at the prefix, sorry minimum number of zeros at the prefix not maximum and that is the challenge which is imposed by the bitcoin network, can every minor need to solve that problem to find out the corresponding hash function.

(Refer Slide Time: 05:13)



Bitcoin Proof of Work (PoW) System

- Most implementations of Bitcoin PoW use double SHA256 hash function
- The miners collect the transactions for 10 minutes (default setup) and starts mining the PoW

approx

- The probability of getting a PoW is low – it is difficult to say which miner will be able to generate the block
  - No miner will be able to control the bitcoin network single handedly

So, most implementation of Bitcoin proof of work it utilizes SHA 256 bit hash function, which is a 256 bit hash function the minors they collect the transactions for approximately 10 minutes which is the default set up.

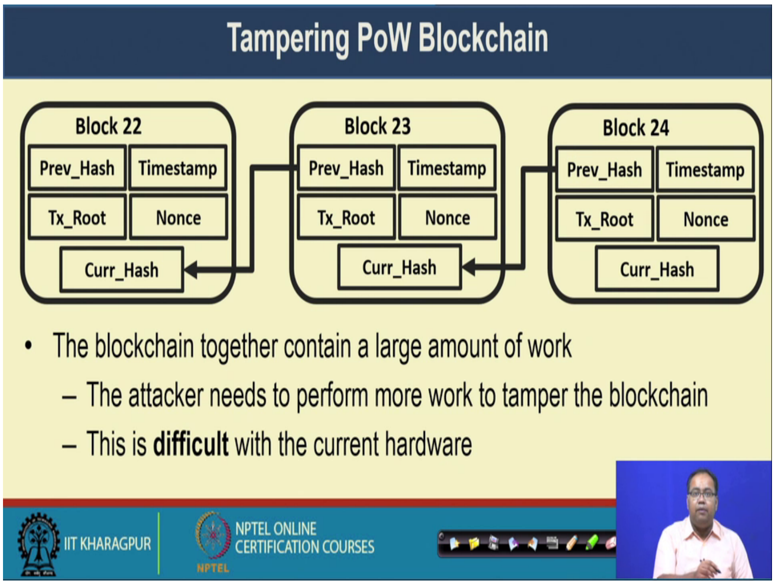
So, it waits for certain duration and a looks for all the transactions, which are coming within that duration. So, this is again a kind of approximate duration. So, this duration comes from the fact that the, at what periodicity the minor should mine a new block?.So, those the different steps will look into later.

So, ideally they wait for certain duration approximately 10 minutes and look for all the incoming transactions and to within that duration, if they get an updated blockchain then they find out that which transactions have already been included in the block, and by excluding those transactions, which are already been included in the existing blockchain they take the next the new set of transactions to propose a new block and starts the mining procedure; that means, start finding out the corresponding hash value.

Now, the probability of getting a proof of work is low. So, because the probability is low it is difficult to say who is minor will be able to generate the block. So, you have multiple minors who are simultaneously trying to generate a block and one of the minors out of those the hundreds or 1000 minors, who they are in the bitcoin network one of them will generate the block, and that way because this probability was low no minors will be able to control the bitcoin network single handedly.

So, it will it will not happen ideally it will not happen that no minors will be able to generate the all the blocks in the bitcoin network. So, that that level of randomization is supported by the bitcoin consensus protocol, which is the proof of work system. So, 1.2 note here that sometime in some literature this bitcoin proof of work mechanism, it is also termed as an nakamoto consensus based on with the proposal came from Satoshi Nakamoto some people also term it as nakamoto consensus ok. So, let us see that why bitcoin proof of work mechanism is tamper proof.

(Refer Slide Time: 07:49)



Tampering PoW Blockchain

Block 22

Prev_Hash | Timestamp

Tx_Root | Nonce

Curr_Hash

Block 23

Prev_Hash | Timestamp

Tx_Root | Nonce

Curr_Hash

Block 24

Prev_Hash | Timestamp

Tx_Root | Nonce

Curr_Hash

- The blockchain together contain a large amount of work
  - The attacker needs to perform more work to tamper the blockchain
  - This is **difficult** with the current hardware

So, this is the broad architecture of a block. So, in every block as we have learnt till now that every individual node they have to find out the nonce and this so, that this current has the hash for this block it satisfies certain difficulty like the minimum number of zeros that should be there in the prefix.

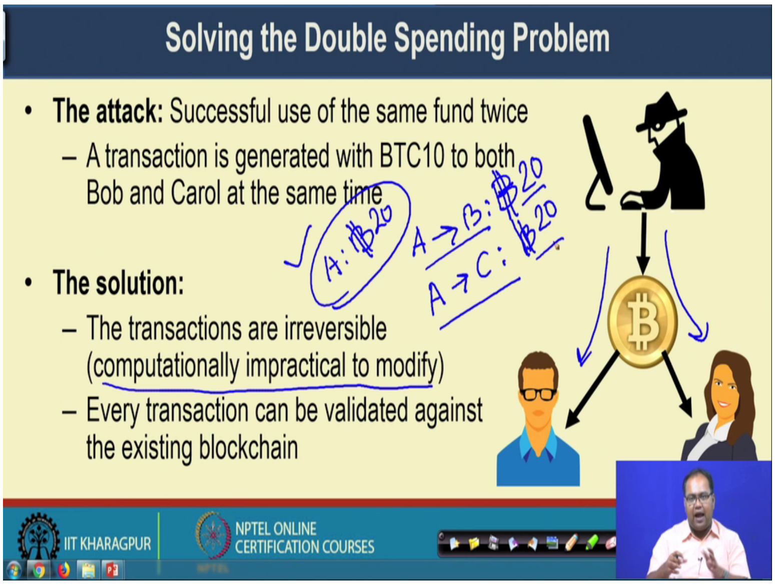
So, this hash value the current hash value of one block it is included as a part of the previous block. So, these things we have seen earlier. So, that way if some attacker wants to make some changes in one block, then they have to actually do the collective work or better to say we have to do more work more work compared to the collective work of all the blocks in the chain. So, every block in the chain it has been obtained by doing some work by individual minors. So, where the minors are where the minors are found out the nonce value based on the difficulty level.

So, the attacker have to do a collective work, which is more than the total collective work of all the blocks in the in the current blockchain. So, that way this is difficult with the current address. So, note the term that making an attack or tampering the current blockchain is difficult with the current hardware, but remember that it is not impossible.

So, if the attacker can do the work with by investing a huge hardware, which can compute the hash very fast and it will be able to change all the in hash values of all the blocks in the longest chain, then the attacker may be able to make a change in the blockchain or tempered the blockchain, but although it is computationally feasible, but there are 2 aspect first of all the time required to do that work ideally it should be significantly high, if the minor invest huge amount of hardware to do the things. Then the total amount of investment that the attacker is doing to launch this attack that should be; obviously, less than the gain that he or she will get by performing this attack.

So, that way ideally people think of that although this is not deterministically tamper proof it is always possible to tamper the blockchain with a very fast hardware in the future, but ideally people believe that data curve will be discouraged to launch an attack on the blockchain network. Because, they have to do more work compared to the collective work of all the blocks in the longest chain.

(Refer Slide Time: 10:57)



Solving the Double Spending Problem

- **The attack:** Successful use of the same fund twice
  - A transaction is generated with BTC10 to both Bob and Carol at the same time
- **The solution:**
  - The transactions are irreversible (computationally impractical to modify)
  - Every transaction can be validated against the existing blockchain

Where so, this proof of work also solves a problem in any digital crypto currency which will known as double spending problem or these double spending can also work like a attack some time.

So, the double spending means the successful use of the same fund twice. So, the attacker is trying to transfer the same bitcoin to 2 different person almost at the same instance of time. So, the attacker can launch a transaction A to B with certain bitcoin with certain say bitcoin 20 and then the attacker launches another transaction to see with the same bitcoin 20 and here the attacker say has only 20 bitcoin with him or her.

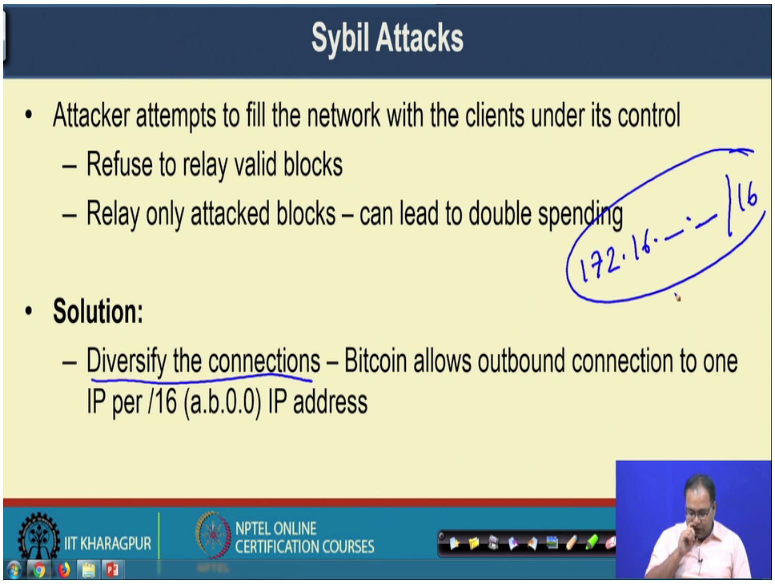
So, that way this kind of attack is known as the double spending attack in the digital currency literature. So, bitcoin by utilizing this proof of work mechanism it also solves the double spending problem, because the transactions that we are putting in the block they are irreversible or at least they are computationally impractical to modify we are we are not saying that it is impossible to modify, but as I have mentioned that the attacker have to do a significant amount of work or that are they have to do the work more than the collective work of the blockchain. And that way it is computational impractical and that is why that attacker will not be encourage to launch this kind of attacker.

So, that way whatever transactions which have been already submitted in the block they are kind of permanent transactions. So, they are kind of permanent transactions means you can think of them as the permanent ledger and whenever some new transaction comes, you can always validate that whether the new transaction confirm with the existing transactions which are there in the blockchain.

So, that way if this initial transaction has already committed in the blockchain from where you can find out that attacker has only 20 bitcoin wiki mod hard, and if the attacker is going to issue 2 different transactions of bitcoin 20, which has not possible like if we the attacker is going to launch a kind of double spending attack. So, the minors or the nodes in the bitcoin network can verify that and they can actually block such kind of double spending to happen over the bitcoin network.

So, that way by making the entire system kind of tamper proof the proof of work mechanism ensures that a double spending does not happen, in case of a blockchain network.

(Refer Slide Time: 13:53)



Sybil Attacks

- Attacker attempts to fill the network with the clients under its control
  - Refuse to relay valid blocks
  - Relay only attacked blocks – can lead to double spending
- **Solution:**
  - Diversify the connections – Bitcoin allows outbound connection to one IP per /16 (a.b.0.0) IP address

Well there can be certain type of attack which can happen on a proof of work based system and one popular attack that people are trying to perform is the Sybil attack. So, in case of Sybil attack the attacker attempts to fill the network with the clients under his control.

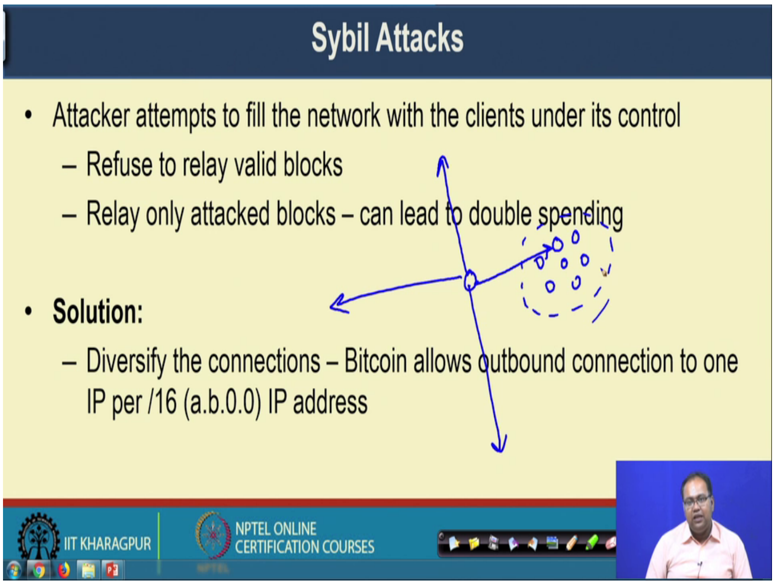
So, if the attacker can feel the network with clients under his control than the attacker can actually control or get the monopoly over the network and this plants can do different kind of actions based on the instruction from the attacker, they can refuse to relay the valid blocks, they can only relay the blocks which are generated by the attackers those blocks can lead to double spending.

So, that way that in the Sybil attack the attacker can include multiple such nodes in the network, who can collectively compromise the proof of work mechanism. Now to solve this problem the bitcoin network it apply a solution technique where it diversify the connections. So, the bitcoin only allows the outbound connection to 1 I P per slash 16 I P address.

So, if you have say I P address series of say something like 172 dot 16 dot something dot something slash 16. So, in this entire network you can have at most one here. So, that way if you diversify the network it is expected that if the attacker generates multiples that false minors, the attacker will generated them within the same network.

So, they will be clustered within same net same subnet. So, that is the expectation and with these expectation people find it that will Sybil attack may be possible, but if you diversify the outgoing connection that whenever you are forwarding the block you forward the block to multiple nodes rather than a cluster of nodes in the same network.

(Refer Slide Time: 15:54)



Sybil Attacks

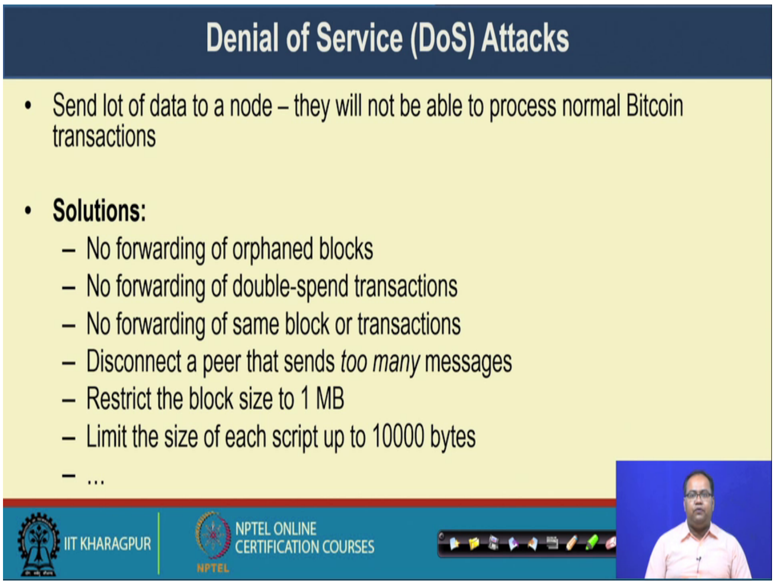
- Attacker attempts to fill the network with the clients under its control
  - Refuse to relay valid blocks
  - Relay only attacked blocks – can lead to double spending
- **Solution:**
  - Diversify the connections – Bitcoin allows outbound connection to one IP per /16 (a.b.0.0) IP address

So, the entire idea is something like that say you are forwarding a block and all these blocks all these nodes, belong to a single cluster. So, in that case you just make a connection to one of the node in this connection where you will forward the block. And then you can have multiple orders other peers where you can forward the block or forward the valid transaction.

So, in that case it will not happened that you are connected your peers are only from the attack nodes and they are not collectively relaying your transaction. So, that way blockchain expects or blockchain makes the Sybil attack hard to implement on a distributed network, but remember that all though this solution makes it hard to launch a Sybil attack, but it does not make it impossible. It is always possible to launch multiple attackers at multiple subnets and then collectively controlled them and then launched attack in a distributed way.

But, launching those kind of attack is much difficult in a real network.

(Refer Slide Time: 17:00)



Denial of Service (DoS) Attacks

- Send lot of data to a node – they will not be able to process normal Bitcoin transactions
- **Solutions:**
  - No forwarding of orphaned blocks
  - No forwarding of double-spend transactions
  - No forwarding of same block or transactions
  - Disconnect a peer that sends *too many* messages
  - Restrict the block size to 1 MB
  - Limit the size of each script up to 10000 bytes
  - ...

So, the next type of attack which can happen on a proof of work based system it is the denial of service based attack. So, in denial of service attack based attackers in a lot of data to a particular node and if you are sending a lot of data to a particular node, the node will not be able to process the normal bitcoin transactions.

So, that is the typical denial of service attack which can be happen on a proof of work base system and to solve this kind of denial of service attack bitcoin has a set of rules like you do not forward or can block off and block means the block, which have been fault from the main chain. So, if a block does not belong to the main chain, which is the longest blockchain you do not forward those blocks, then do not forward the double spend transactions, if you have found out that a transaction has already been forwarded.

So, you do not forward the transactions further, then do not forward the same block or transactions twice, then disconnect peer that send too many messages if as which we are a send too many of messages too many of transaction they would and then you disconnect that particular peer. Then you restrict the block size to 1 MB. So, restrict in the block size has an implication on solving the denial of service problem, if you have a larger block in a larger block you can put more transactions and the larger blocks become difficult to verify by the common normal nodes.

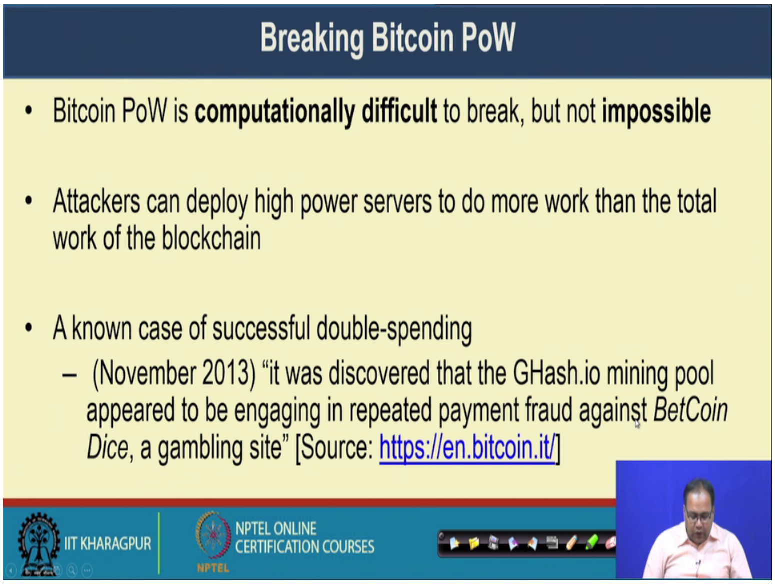
So, the normal bitcoin nodes which are there if they are getting a large block it may be difficult for them to verify the large block.

So, that way if you are restricting the size of the block it becomes easier to forward the block too many peers in the network. So, that is why the standard bitcoin network as proposed by Satoshi Nakamoto, it blocks or restricts the block size to something like 1 MB and nowadays with the current bitcoin version it can go upto 8 MB, then limit the size of the bitcoin script.

So, we have discussed earlier the concept of bitcoins scripting language where you provide the instruction that how to validate or how to match the input of a transaction to output off the next transaction or how to how to match the output of a transaction to the input of the next transaction. So, this bitcoin script there is certain limitation under bitcoin script that you limit the size of it bitcoin script to something like 10,000 bytes.

So, do not have a bitcoin script the more than that if you have a larger bitcoin script that is most susceptible to attack. So, do not forward transaction which has this kind of a largest scripts. So, by taking there are certain other measure there is huge list of measures that bitcoin network takes to solve denial of service attack over the proof of work base systems, but now let us look that whether it is possible to break the bitcoin proof of work or not.

(Refer Slide Time: 20:00)



Breaking Bitcoin PoW

- Bitcoin PoW is **computationally difficult** to break, but not **impossible**
- Attackers can deploy high power servers to do more work than the total work of the blockchain
- A known case of successful double-spending
  - (November 2013) "it was discovered that the GHash.io mining pool appeared to be engaging in repeated payment fraud against *BetCoin Dice*, a gambling site" [Source: https://en.bitcoin.it/]

So, as we have mentioned earlier that bitcoin proof of work is computationally difficult to break, that is the important term it is computationally difficult to break, but it is not impossible to break the proof of work based system.

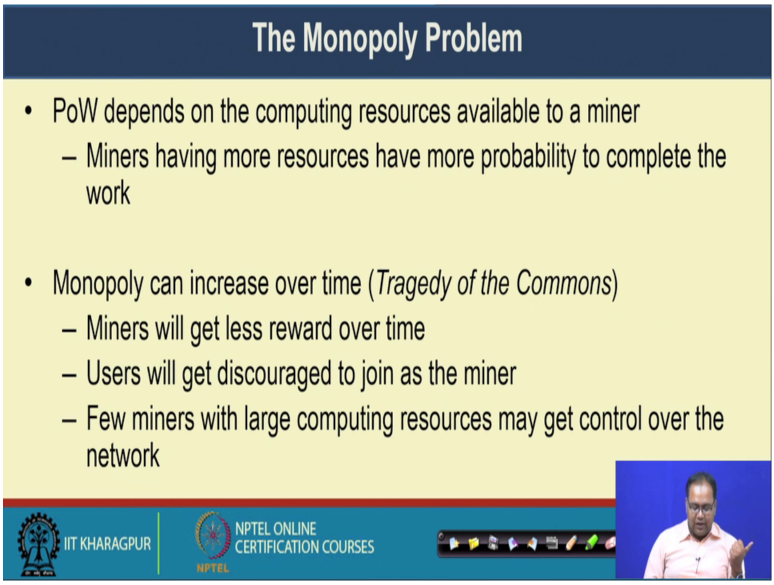
Ah. So, the attackers can always deploy high power severs or by deploying those high power server they can do more work than the total work of the blockchain and that way they can tamper the entire blockchain network. So, that is an one example one known case of successful double spending, which came from mining pool called g hash dot i o. So, this concept of mining pool will discuss latter on the mining pool means a state of minors coming together collectively and they are trying to mine a new block. So, that we called as a mining pool stop this g hash dot i o mining pool, it was discovered in November 2013 that G Hash dot i o mining pool they appeared to be engaging in repeated payment fraud against betcoin dice, which is a gambling website.

So, that kind of double, spending that has happened over there. So, he has that are you they were able to launch a double spending attack over the bitcoin network. So, that is the one problem and that problem particularly comes, because of something called the monopoly problem in the proof of work base system. So, this proof of work if you look into the proof of work based system proof of work depends on the computing resource available to a minor.

So, if a minor can pause a huge amount of computational resource, then the minor has then there is a possibility that a minor can control the entire network. Because, he has some huge hardware some huge server like, if you server or something like that where, if we can parallel do the computation of the hashing and by doing parallel computation of the hashing and later on will see that there are specialized hardware available for doing the bitcoin mining, by applying those kind of parallel hashing or by deploying huge servers for bitcoin mining and an attacker or a minor can gain control over the network. So, it may happen that a minor can gradually do or generate lots of blocks in the current blockchain.

Now, if huge number of blocks in the blockchain goes to a single minor, then his minor has the ability to control the entire flow of transactions in the blockchain. So, this particular problem we call as the monopoly problem in bitcoin network.

(Refer Slide Time: 22:50)



The Monopoly Problem

- PoW depends on the computing resources available to a miner
  - Miners having more resources have more probability to complete the work
- Monopoly can increase over time (*Tragedy of the Commons*)
  - Miners will get less reward over time
  - Users will get discouraged to join as the miner
  - Few miners with large computing resources may get control over the network

.

Where the minors have a more resources or more probability to complete the work, and there is a statistical theory called tragedy of the common. So, this tragedy of the commons theory, which says; which is from the economic perspective from the economic perspective it says that such kind of monopoly can increase overtime. So, why such kind of monopoly can increase over time?

So, if you remember the rewarding system whenever the minor mines and new block they get start and certain reward, but to limit the total amount of bitcoin in blocks in the economic system, we make a restriction about what is the total number of bitcoin that can be generated out of the mining procedure.

So, whenever we limit the total number of bitcoin that can be generated out of the mining procedure with time the amount of reward, that will be given to the to the miners that will drop, because the amount of bitcoin that can be generated that is also gradually dropping to make it saturated. So, because of that whenever the minors will get less reward over time so, the users will get discourage to participate or to join as a minor.

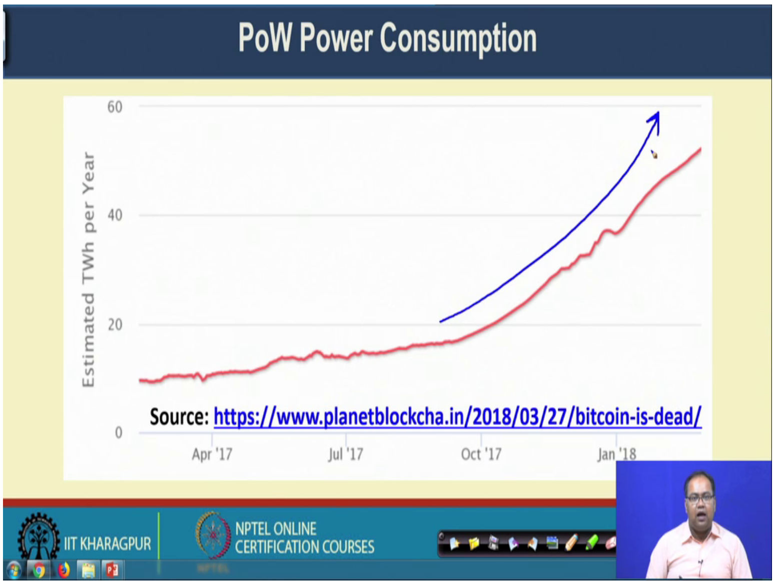
Now, if the user get discourage to join as a minor, then a few minors with large computing resources they may get control over the entire network.

So, that is a practical problem, which is not in they are in today’s bitcoin network, but with time it is expected that this kind of problem may arise, where because of the shortage of reward which is coming from the mining procedure only the minors who are having huge computation power they are only participating in the mining procedure. And indeed nowadays we are in a time when we have already started seeing this kind of phenomenon.

Now, a days you cannot participate in mining procedure just twitter general purpose CPU, if you if you if you just install the bitcoin mining software in the general in a general purpose CPU hardly you will see that you are you have you are able to generate a new block.

So, in that way only the minors with huge amount of computing resources over the time they will get control over the bitcoin network. So, this particular problem we call as the monopoly problem, which is a short coming of the proof of work based system.

(Refer Slide Time: 25:16)



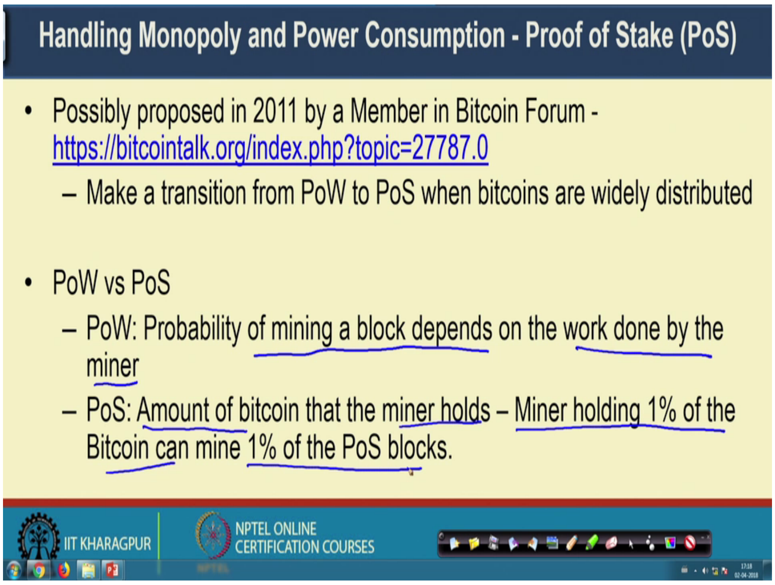
PoW Power Consumption

Source: https://www.planetblockcha.in/2018/03/27/bitcoin-is-dead/

Another problem of this proof of work based system is the power consumption. So, this proof of work based system, it relies on the amount of power which is being consumed, because you are whenever you are deploying huge amount of computational resources in the network, it is expected that those computational resources are actually consuming the huge amount of the power to generate those hash functions.

So, that way here this start typically shows the amount of power conjunctions with the bitcoin network. So, you can see that with time there is a kind of exponential growth in the power consumption due to bitcoin mining.

(Refer Slide Time: 26:00)



Handling Monopoly and Power Consumption - Proof of Stake (PoS)

- Possibly proposed in 2011 by a Member in Bitcoin Forum - https://bitcointalk.org/index.php?topic=27787.0
  - Make a transition from PoW to PoS when bitcoins are widely distributed
- PoW vs PoS
  - PoW: Probability of mining a block depends on the work done by the miner
  - PoS: Amount of bitcoin that the miner holds – Miner holding 1% of the Bitcoin can mine 1% of the PoS blocks.

So, to reduce this 2 problem to handle monopoly and the power conjunction in a proof of work base system different other consensus mechanism came into practice one popular is this proof of stake mechanism. So, this proof of stake mechanism it is possibly propose into 2011 by a member in the bitcoin forum. So, the idea was that you make a general transition from a proof of work base system to a proof of stake based system, when the bitcoins are getting widely distributed.

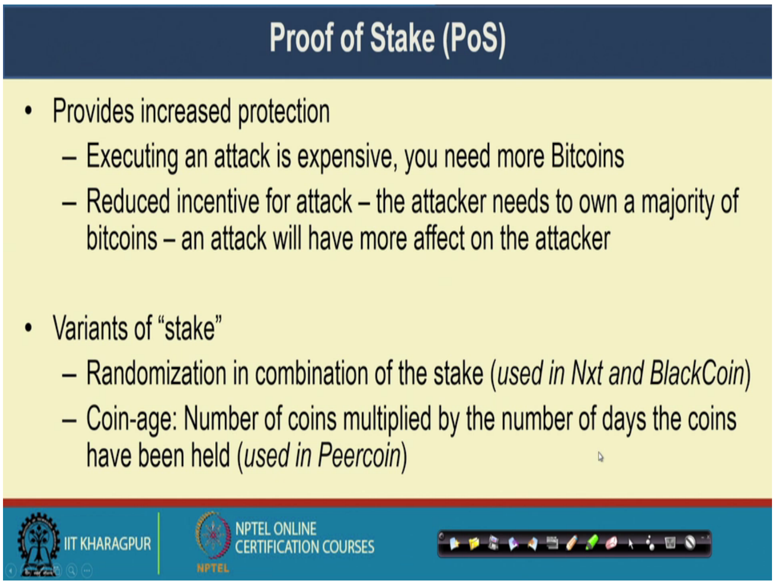
Now, the broad difference between a proof of work based system of a under proof of stake this is system is as follows, in case of proof of work the probability of mining a block depends on the work done by the minor. So, the amount of the work if the minor has huge resources huge computing resources, if the minor can do a huge amount of work the probability of getting a new block gets interest.

On the other hand in case of proof of stake the amount of bitcoin that the minors hold that instruct that which minor can generate the next block. So, if a minor holds one percent of total bitcoin the minor can the minor can mine one percent of the proof of stake block.

So, by putting this kind of restriction that on the amount of bitcoin that the minor holds and a proportional do that, the minor will be able to generate the proof of stake block, you can you can basically reduce or you can reduce certain this kind of monopoly problem or you can you can make the monopoly problem to appear as a difficult problem for a proof of based stake base system, because the inherent assumption is that by the proof of work base system the bitcoin is widely distributed.

So, every minor will be able to participate in the mining procedure proportional to the amount of bitcoin that he or she passes.

(Refer Slide Time: 28:15)



Proof of Stake (PoS)

- Provides increased protection
  - Executing an attack is expensive, you need more Bitcoins
  - Reduced incentive for attack – the attacker needs to own a majority of bitcoins – an attack will have more affect on the attacker
- Variants of "stake"
  - Randomization in combination of the stake (*used in Nxt and BlackCoin*)
  - Coin-age: Number of coins multiplied by the number of days the coins have been held (*used in Peercoin*)

So, this proof of based proof of stake based system or POS based system it provides in a increase protection. So, executing an attack is expensive you require more bitcoin, if you want to generate more block and you also have reduced incentive for attack, because to generate the attack you need to have a huge amount of bitcoin in your whole. Now, if you already have a huge amount of bitcoin in your whole and if you are get generating an attack on the blockchain network; that means, you will be mostly affected because you are you are holding a majority of the bitcoins with you.

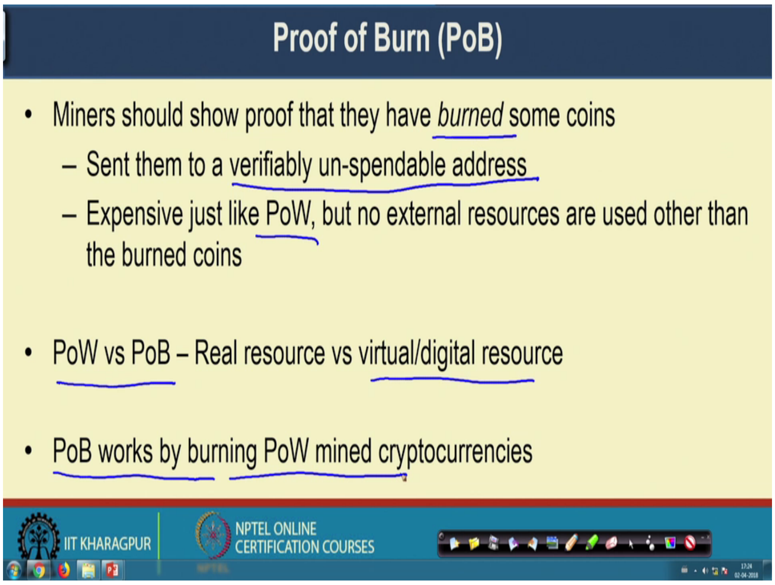
So, that way the attacks are more expensive in a proof of stake based system. Now they are multiple variance of stake or stake is basically the term will finish that you have there are multiple variants of stake, that has been discussed in the literature one idea was to make randomization in combination of the stake, which is used in this next and black coin cryptocurrency.

So, the idea is that you consider the amount of bitcoin that you have as an input and at the same time you apply a randomization function and based on that randomization function you decide that who will be the minor who will generate the next block. Then there is another one which has been used in another cryptocurrency called peer coin the concept of coinage.

So, the coinage is that number of coins multiple by the number of days the coin have been held. So, to participate in a peer coin system it is apart from holding a huge amount of bitcoin with you not huge amount of bitcoin sufficient amount of bitcoin with you have to all also ensure that you are holding those bitcoin for certain duration.

So, this way if some attacker just collect the huge amount of bitcoin by launching some attack or participating in some transactions, immediately he or she you will not be able to participate in the mining procedure. So, that way this coinage also prevents the case when the attacker can do certain transactions immediately to gain more amount of bitcoins and by gaining more amount of bitcoins get more probability to mine a new block. So, these are the 2 variants of proof of work based system.

(Refer Slide Time: 30:46)



Proof of Burn (PoB)

- Miners should show proof that they have *burned* some coins
  - Sent them to a verifiably un-spendable address
  - Expensive just like PoW, but no external resources are used other than the burned coins
- PoW vs PoB – Real resource vs virtual/digital resource
- PoB works by burning PoW mined cryptocurrencies

So, another consensus mechanism that has been discussed widely in the literature, it is called proof of burn in case of proof of burn the minor should show a proof that they have burned some coins.

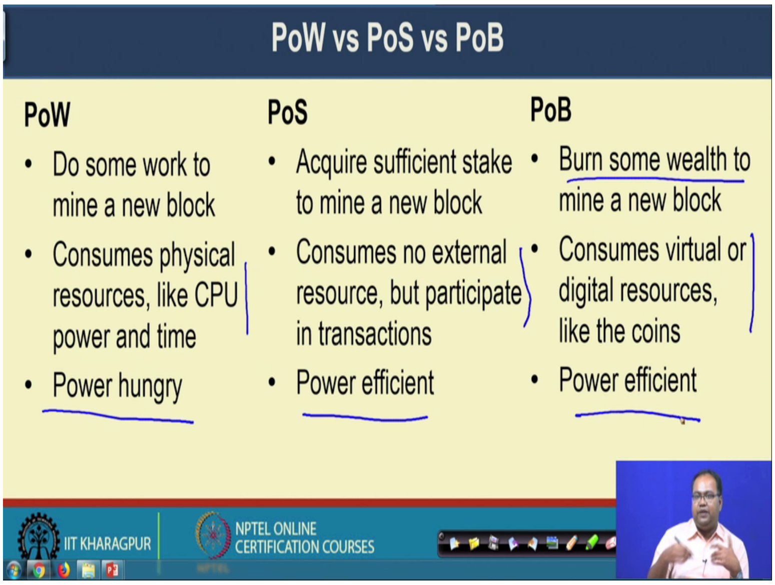
So, by the burning it is like that they have to send them to a verifiably un spendable address and during the discussion of bitcoins free to have. So, new that how you can write a script through, which you can sent some bitcoin to a verifiable un spendable address where no one will be able to spend that bitcoin. So, you have to burned that coin. So, idea here is that it is as expensive as proof of work. In case of proof of work your investment was the physical resources like your computational powered and the computation time and the electricity bill that you have to provide for that and the physical money that you have to invest to purchase computational hardware, here you have to spend digital or logical resources which are bitcoins.

So, you have to spend certain bitcoins to participate in the mining procedure to show that you have interest in generating the mining. So, if the attacker wants to attack this system, the attacker actually have to make a loss of huge amount of bitcoins. And at the same time this particular system is power efficient, because you are you are not utilizing physical hardware to do the work, that that you are spending this digital currencies for that and that is why although I it is expensive like proof of work, but it is it is efficient in terms of the power consumption, because now it now you are not utilizing this power hungry hardware to perform the hash functions.

So, the difference between proof of work and proof of burn is that. In case of proof of work you are utilizing real resources whereas, in case of proof of burn you are utilizing virtualized or digital resources, but remember that all these proof of burn or proof of stake mechanism that became after proof of work; that means, once the proof of work get settle down and people have certain amount of digital currencies with them, then gradually you can move to proof of stake or proof of burned based mechanism.

So, this proof of burned works by burning some proof of work mined cryptocurrencies. So, the original crypto currencies were mine by proof of work then you are burning them to participate in the next mining procedure when the proof of work system got saturated.

(Refer Slide Time: 33:30)



PoW vs PoS vs PoB

PoW
- Do some work to mine a new block
- Consumes physical resources, like CPU power and time
- Power hungry

PoS
- Acquire sufficient stake to mine a new block
- Consumes no external resource, but participate in transactions
- Power efficient

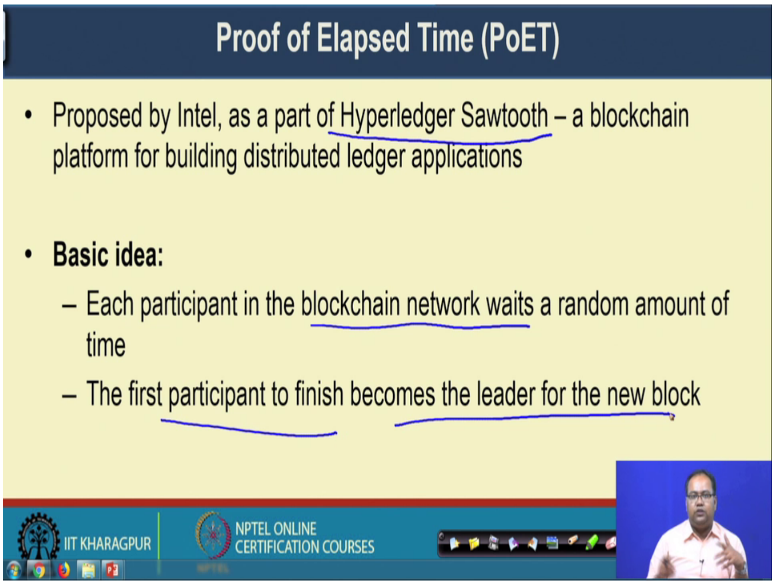
PoB
- Burn some wealth to mine a new block
- Consumes virtual or digital resources, like the coins
- Power efficient

So, this is the broad difference between the 3 proof of work proof of stake and proof of burn. In case of proof of work you do some work to mine a new block. So, you find out hash function for the which is computationally difficult. In case of proof of stake you acquire sufficient stake or wealth to find the new block you have to show that you have certain amount of bitcoins with you so, that you can participate in the mining procedure.

In case of proof of burn you have to burn some wealth to mine a new block. So, so, you have to just like proof of work you have to you have to expense certain bitcoin the rather than the physical currency to participate in the mining procedure.

In case of proof of work it consume physical resources like CPU power and time a proof of stake as such it consume no external resource, but you can participate in the transactions. In case of proof of burn you consume actual digital resources like the coins. Now, the proof of work it is a power hungry mechanism proof of stake it is partition proof of burn, it is also power efficient because you are burning and the digital currency and not the physical currency.

(Refer Slide Time: 34:52)



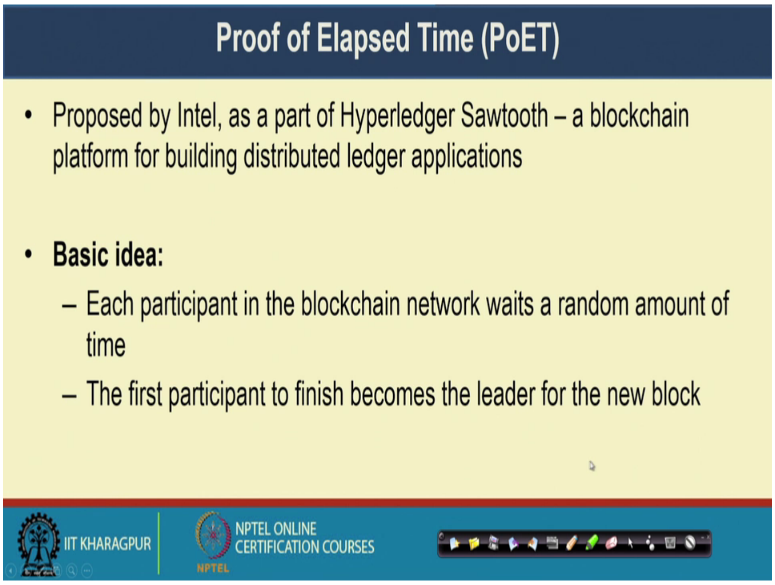
Proof of Elapsed Time (PoET)

- Proposed by Intel, as a part of Hyperledger Sawtooth – a blockchain platform for building distributed ledger applications
- **Basic idea:**
  - Each participant in the blockchain network waits a random amount of time
  - The first participant to finish becomes the leader for the new block

There was another consensus algorithm, which was proposed by Intel as a part of the Intel, Intel blockchain environment, which is called hyper ledger sawtooth that algorithm is called the proof of elapsed time.

So, the idea of this proof of elapsed time is very simple like each participant in the blockchain network waits a random amount of time. The first participant to finish becomes the leader for the new black. So, you actually make a randomization among the miners. So, the minor who will be able to complete that random waiting first, that minor will be able to proposed the new block.

(Refer Slide Time: 35:30)

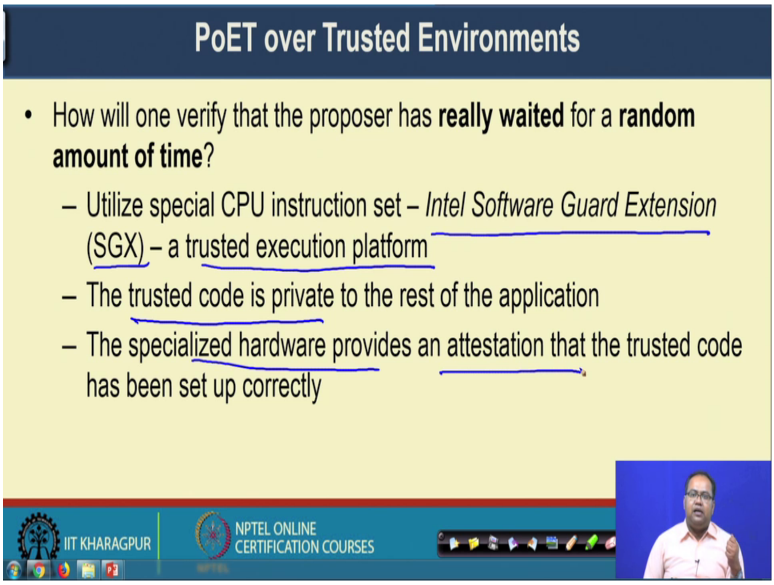


Proof of Elapsed Time (PoET)

- Proposed by Intel, as a part of Hyperledger Sawtooth – a blockchain platform for building distributed ledger applications
- **Basic idea:**
  - Each participant in the blockchain network waits a random amount of time
  - The first participant to finish becomes the leader for the new block

But, here the challenge is that how will you verify that the proposed that has really waited for random amount of time.

(Refer Slide Time: 35:33)



PoET over Trusted Environments

- How will one verify that the proposer has **really waited** for a **random amount of time**?
  - Utilize special CPU instruction set – *Intel Software Guard Extension* (SGX) – a trusted execution platform
  - The trusted code is private to the rest of the application
  - The specialized hardware provides an attestation that the trusted code has been set up correctly

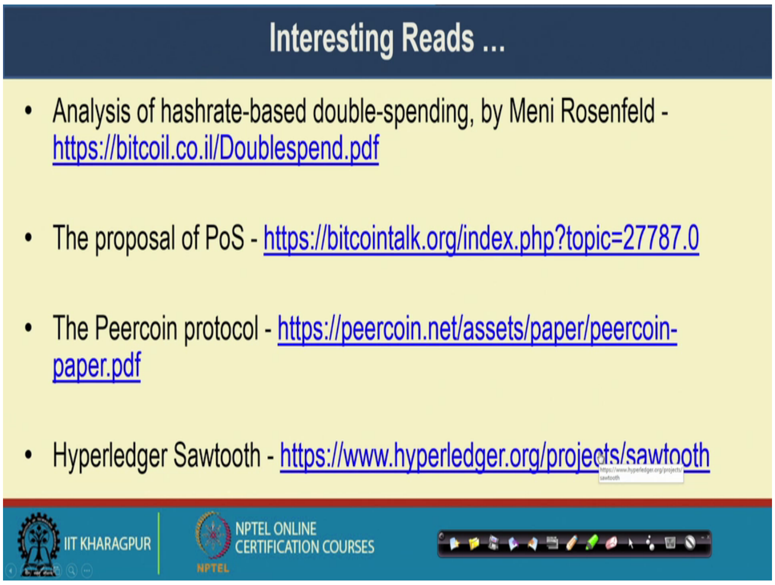
.

So, if it is a software control then attacker can make a change in the software code and we claim that, well I have waited for 120 second before participating in the mining procedure.

Now, to verify that Intel utilizes special CPU instruction set, which is called the Intel software guard extension or SGX, which is based on a trusted execution platform. So, this trusted execution platform is hardware code the hardware platforms where you can write trusted code in a private way, and that code is private to the rest of the application. So, it is completely hardware control it is not software control.

So, that specialize hardware it provides an attestation that the trusted code has been set up correctly and the trusted code say, if you have implemented is randomization waiting time as a part of the trusted code that have been implemented correctly and that have been instituted correctly. So, you are giving a guarantee from the hardware itself not under software level. So, that will not be able to modify that.

(Refer Slide Time: 36:48)



Interesting Reads ...

- Analysis of hashrate-based double-spending, by Meni Rosenfeld - https://bitcoil.co.il/Doublespend.pdf
- The proposal of PoS - https://bitcointalk.org/index.php?topic=27787.0
- The Peercoin protocol - https://peercoin.net/assets/paper/peercoin-paper.pdf
- Hyperledger Sawtooth - https://www.hyperledger.org/projects/sawtooth

So, here are some interesting reads regarding this is a different kind of different kind of consensus algorithm blockchain consensus algorithm. So, the first one it gives analysis on this double spending mechanism on bitcoin are. So, it is a nice statistical analysis of double spending then that second link is on proposal of proof of stake.

So, you can look into different interesting ideas there that hardware is the peercoin protocol that has utilize the proof of burn mechanism, under fourth one is the hyperledger sawtooth platform. So, you can explode the internal details and architecture of distorted platform. So, these are all about the basic consensus protocol in a in a bitcoin type cryptocurrency environment that utilize permission less the blockchain environment.

So, this proof of elapsed time remember that this proof of elapsed time that particular algorithm it was implemented by Intel al Intel under the permission model latter on we will discuss the permission model in details, but initially people have proposed that for the permission less model as well. So, the only difficulty there is that you have to proposed that the special Intel stake hardware which implements are trusted execution environment.

So, the last algorithm proof of elapsed time that is that is both for the permission less as well as per the permission environment, but for the other consensus algorithm that we have discussed to proof of work proof of stake and proof of burn and they are primarily for the for a permission less the environment.

So, that is brief idea about different kind of consensus algorithm and in the next class. So, we will talk about the basic mining properties and the task of a minor in bitcoin. So, see you in the next class.

Thank you.