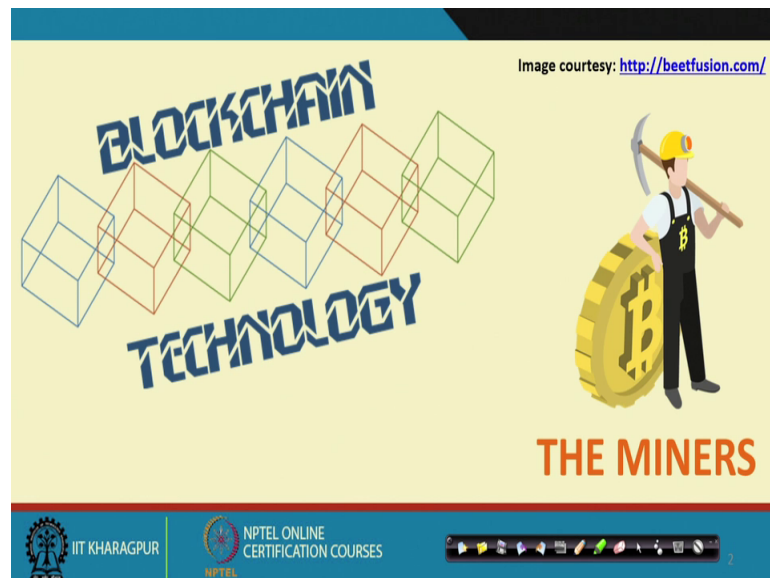


Blockchains Architecture, Design and Use Cases
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 13
Consensus in Bitcoin – III (The Miners)

So, welcome back to the course on Blockchain. In the last a lecture we have discussed about this Bitcoin mining procedure, and a we have looked into the consensus protocol in a permission blockchain environment with the focus to the proof of work base system in bitcoin network.

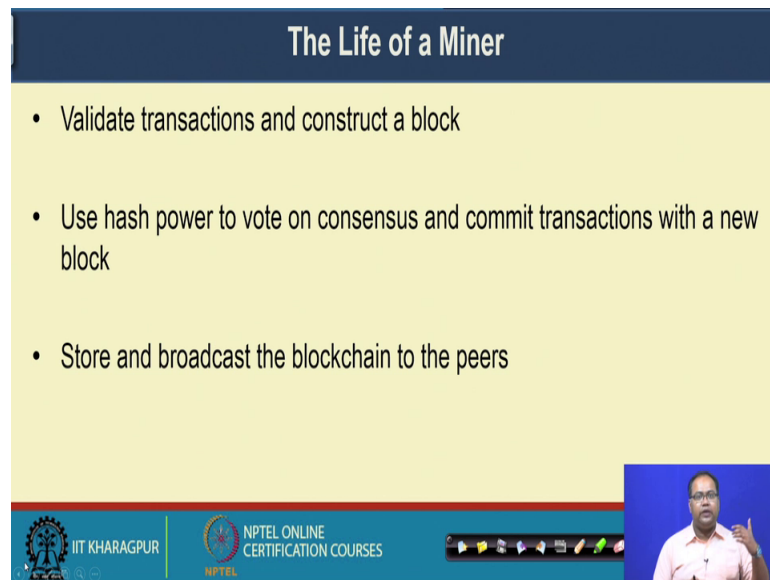
(Refer Slide Time: 00:30)



And we have looked into that how this proof of work based mining procedure; it generates a consensus mechanism among the different miners who are proposing new blocks. And make a tamper proof architecture of the entire blockchain ah.

So, in today's lecture we will explore that further and we will look into the different task of the miner and what are the incentives to the miner to participate in this mining procedure. And, that mining procedure how motivate them to implies some kind of economical properties or economical feature in the environment to control the entire mining presidio ah. So, let us look into the details of the bitcoin miners.

(Refer Slide Time: 01:40)



The Life of a Miner

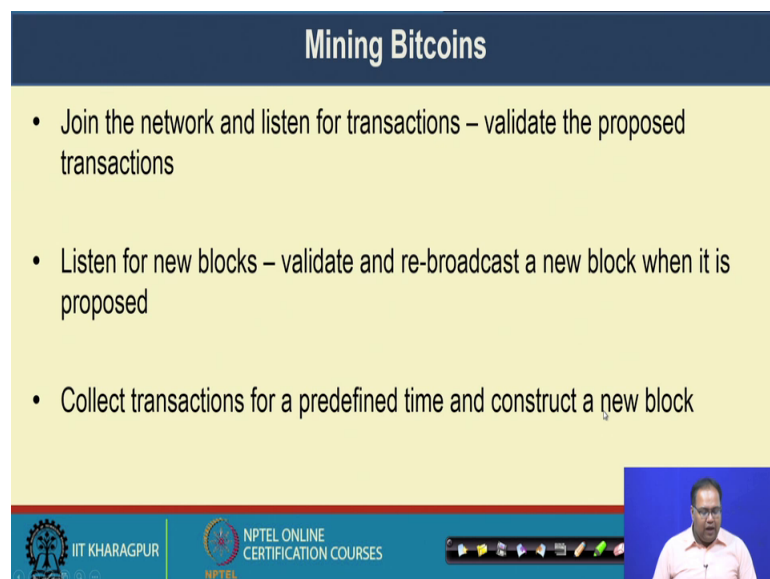
- Validate transactions and construct a block
- Use hash power to vote on consensus and commit transactions with a new block
- Store and broadcast the blockchain to the peers

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

The slide features a dark blue header with the title 'The Life of a Miner' in white. Below the header is a light yellow background with a bulleted list of three tasks. At the bottom, there is a dark blue footer containing the IIT Kharagpur and NPTEL logos, a navigation bar with icons, and a small video inset of a man in a pink shirt speaking.

So, well. So, the life of a miner of something like this, their task is to validate the transaction and then construct a new block. Once they have constructed a new block then they imply their hash power to vote on consensus. They vote on consensus in the sense like to find out that who is going to complete the work first and then accordingly propose that block as a new block. And commit the transactions in that new block and attach that new block to the existing blockchain. And then stored and broadcast that new blockchain to the peers. So, that way the entire blockchain gets propagated in the network.

(Refer Slide Time: 02:22)



Mining Bitcoins

- Join the network and listen for transactions – validate the proposed transactions
- Listen for new blocks – validate and re-broadcast a new block when it is proposed
- Collect transactions for a predefined time and construct a new block

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

The slide features a dark blue header with the title 'Mining Bitcoins' in white. Below the header is a light yellow background with a bulleted list of three tasks. At the bottom, there is a dark blue footer containing the IIT Kharagpur and NPTEL logos, a navigation bar with icons, and a small video inset of a man in a pink shirt speaking.

So, this mining bitcoin the entire procedure has 6 different steps. So, the first steps is that to if you want to be a miner you have to join in the bitcoin network and listen for the transaction, then validate the proposed transactions which are coming from the client.

So, the next step is to listen for the new blocks validate those new blocks and rebroad broadcast a new block when it is proposed to if you are getting a new block from 1 of 1 of your peer then you validate that new block and we broadcast it in the network. Then collect the transactions for a predefined time and construct a new block with the transactions, which are not already included in the blockchain. So, as a miner you take those transactions and construct the new block.

(Refer Slide Time: 03:18)



Mining Bitcoins

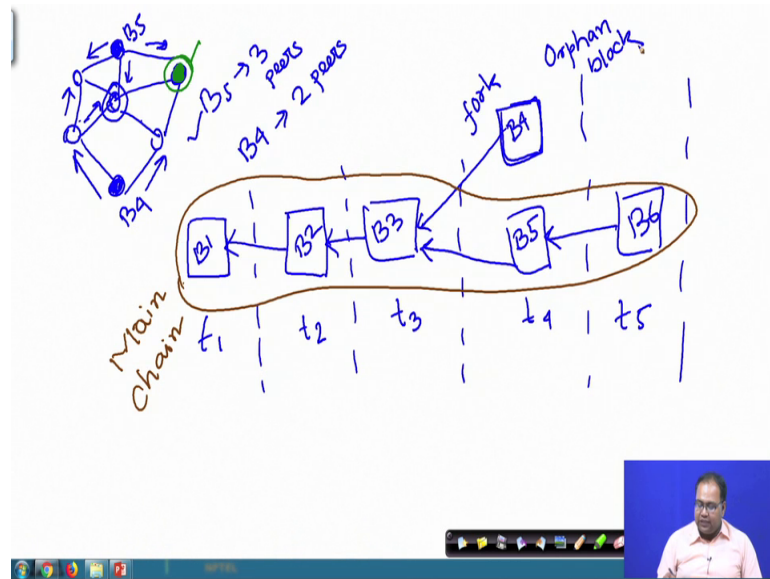
- Find a nonce to make the new block valid
- Broadcast the new block – everybody accepts it if it is a part of the main chain
- Earn the reward for participating in the mining procedure ▾

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Then your task is to participate in the mining procedure where your task is to find out a nonce to make the block valid by utilizing the predefined difficulty function for that; that means, have been certain minimum number of zeros at the prefix of the obtain hash value. So, we have to generate the nonce according to that which is the mining procedure.

So, once you have got a new block you broadcast that new block to your peers and everybody in your peering system they will accept that block. If it is part of the main chain. So, this concept we have discussed earlier, because in a typical blockchain environment it may happened that a multiple blocks are generated together. So, you had a block earlier.

(Refer Slide Time: 20:05)



So, assume that this is the blockchain this is the longest chain every block is pointing to the previous block by the nonce and then at this. So, this is a time instance t 1, this is a time instance t 2, this is a time instance t 3, and then a time instance t 4 2 miners have found out a same block. If 2 miners are found out the same block and both are the valid blocks, then they propose those blocks to the peers and if boths are valid block they gets propagated.

So, the idea is there here I am just trying to draw a bitcoin network where are you have multiple peers. Now assume that this is 1 miner and this is another miner. So, this miner has a found out block I am naming this block as B 1 B 2 B 3 B 4 and B 5 say this miner has found out block B 4, this miner has found out block B 5. So, this miner will broadcast this B 4 block to it is peers than this peer will again rebroadrer broadcast this B 4 block. Similarly this particular miner it will start broadcasting B 5 block and this intermediate node, it will get certain number of B 4 blocks and certain number of B 5 blocks.

So, it will accept the block which it has received from more number of peers. So, it has say 1 2 3 4 5 different peers. So, if it receives B 5 from say it has received B 5 from 3 peers and it has received B 4 from 2 peers, then this miner it will accept the block that it has received from maximum number of peers and rebroadcast that block.

So, that way this the next block say which is getting generated say B 6, it is say B 5 it is now getting propagated and this miner it has say this miner it has received, this miner it has it has received the block B 5 it has accepted block B 5 and after accepting block B 5 it is it has got successful in generating block B 6, now it accept this block B 6 with B 5.

So, now at instance B 5 so, now, this becomes B 1 B 2 B 3 B 5 B 6 this becomes the longest chain in the network. And this particular blockchain is utilized and the additional block that we had earlier we call this is a fork and this particular block it is not getting added further.

So, this blocks are not become the part of the main chain. So, this chain is termed as the main chain, this termed as the main chain in the blockchain network and this block before it the block before it does not become part of this main chain. So, we call this block as the orphan block orphan block.

So, that way to entire blockchain gets propagated in the network. So, these way the block get broadcasted in the network.

(Refer Slide Time: 08:09)

Mining Bitcoins

- Find a nonce to make the new block valid
- Broadcast the new block – everybody accepts it if it is a part of the main chain
- Earn the reward for participating in the mining procedure

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

And, whenever the miner has found out a new block by participating in the mining procedure, they earn certain reward for participating in the mining procedure and this individuality runs in different round. So, at every time instance you are generating new blocks one after another.

(Refer Slide Time: 08:30)

Mining Difficulty

- A measure of how difficult it is to find a hash below a given target
 - Bitcoin network has a global block difficulty
 - Mining pools also have a pool-specific share difficulty
- The difficulty changes for every 2016 blocks
 - Desired rate – one block each 10 minutes
 - Two weeks to generate 2016 blocks
 - The change in difficulty is in proportion to the amount of time over or under two weeks the previous 2016 blocks took to find (en.bitcoin.it)

Handwritten notes:
256 bit
at least 64 bit → Zero

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, we have a term called mining difficulty. So, this mining difficulty is a measure of how difficult it is to find a hash below a given target.

So, it should be fine to find a hash below a given target. So, if you remember the mining procedure, the mining procedure says that we are going to generate a 256-bit hash function. And we say that there is a mining difficulty, the difficulty represented in this way that well out of these 256-bit hash, the first 64 bits should be 0.

So, at least the first 64 bits would be 0. So, this says that well you have to generate a hash function where in the final hash result at least for 64 bits should be 0 and after that the remaining bits can be zeros and ones. So, this is the difficulty of the mining procedure and based on that we define a metric called mining difficulty. So, we have a concept called mining pool that we will discuss later. In the mining pools, they also have a pool-specific share difficulty.

Now, this difficulty parameter I am going to discuss is the mathematical formulation of this difficulty parameter. So, this difficulty parameter changes for every 2016 blocks. So, our desired rate is that we want to generate 1 block each at 10 minutes. So, at every 10 minutes my target is to generate a new block. Now, if you try to generate a new block at every 10 minutes and if you do the computation in that we will find out that well to generate 2016 blocks you require exactly 2 weeks. So, within 2 weeks you can generate 2016 blocks.

So, this difficulty level it is re adjusted at every 2 weeks. So, at every 2 weeks you find out that how many blocks you have generated? Whether you have generated 2016 blocks in less than 2 weeks' time of duration they; that means, the difficulties going to be too simple for the miners. So, you increase the difficulty and if you finding out that well the miners are taking more than 2 weeks of duration to generate 2016 blocks, then it means that that current difficulty is going to be too hard for the miners.

So, you reduce the difficulty in that way so, with this idea in mind. So, we define difficulty or you set the difficulty by utilizing this formula.

(Refer Slide Time: 11:07)

The slide is titled "Setting the Difficulty" and contains the following text:

- Compute the following for every two weeks / *2016 blocks are generated*

$$\text{current_difficulty} = \text{previous_difficulty} * \frac{(2 \text{ weeks in milliseconds})}{(\text{milliseconds to mine last } 2016 \text{ blocks})}$$

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

So, you compute the difficulty at every 2 weeks or you can you can just re compute the difficulty after every 2016 blocks have been generated. So, you can compute a on either every 2 weeks or after 2016 blocks are generated. So, our expectation is that within 2 weeks we want to generate 2016 blocks.

So, that inter block generation time becomes equal to 10 minutes. So, we said the difficulty in this way. So, the current difficulty will be previous difficulty the difficulty that was earlier multiplied by 2 weeks in millisecond the total 2 weeks duration divided by milliseconds to mine the last 2016 blocks.

So; that means, if you are taking less time to mine 2016 blocks compared to 2 weeks then you are going to increase the current difficulty. So, if you if you can generate 2016 block faster; that means, the current difficulty is going to be too easy for the miner.

So, you increase the difficulty level if you are taking more time compared to 2 weeks to generate this 2016 blocks; that means, this time this milliseconds to mine in last 2016 block this terminology becomes more than 2 weeks equivalent in millisecond, if you are taking more time than 2 weeks; that means, the mining is becoming too hard. So, you reduced the current difficulty level.





So, that way the bitcoin network dynamically changes the difficulty level. Now, let us look into that how this difficulty level is related to the hash rate? That means, how many, hash you can perform?

(Refer Slide Time: 13:00)

Hash-rate versus Difficulty

- The hash is a random number between 0 and $2^{256}-1$
 – To find a block, the hash must be less than a given target
- The offset for difficulty 1 is $0xffff * 2^{208}$
- The offset for difficulty D is $0xffff * 2^{208}/D$
- The expected number of hashes we need to calculate to find a block with difficulty D is $(D * 2^{256}) / (0xffff * 2^{208})$

48 010
 48 bit 208 bits
 256 bit

Now, the hash that we are going to generate as you are using double SHA 256 for generating the hash function. So, this hash is random number between 0 and 2 to the power 256 minus 1. So, to find block our objective is the hash must be less than a given target ah. So, we offset the difficulty level 1 as 0 at 0 f f f into 2 to the power 2 0 8; that means, out of the 256 blocks we are saying that the initial 48 bits we will want as the 0 and the remaining bit we want we as the 1. So, that is the offset for difficulty 1.

Now, accordingly we define the offset for difficulty D is all once into 2 to the power 208 divided by D . So, this many number of zeros for different values D by doing this computation you can find out that how many zeros you want at the beginning? That determines the number of zeros that you want at the beginning the example that I have given for difficulty level one. So, for difficulty level 1 we want that the 208 bits. So, out of this 256 bit hash the 208 bits should be equal to can be either 1 or 0 ok.

So, we have control over this 48 bit we want that this initial 48 bit should be all 0s um. So, so that is for the difficulty level 1 accordingly we define the difficulty level B the number of initial bits that we want. So, the expected number of hashes, we need to calculate to find a block with difficulty D is something equal to D into 2 to the power 256 divided by this offset. So; that means, it comes to be D into 2 to the power 48 divided by this offset value ah. So, that is the expected number of hashes that you need to perform.

So, this difficulty level dynamically changes the amount of hash that you want to do. So, if you if you are providing more difficulty that then. So, if you increase the value of D if you are providing more difficulty value. So, you have to generate more number of hashes to get the resulted target well.

(Refer Slide Time: 15:56)



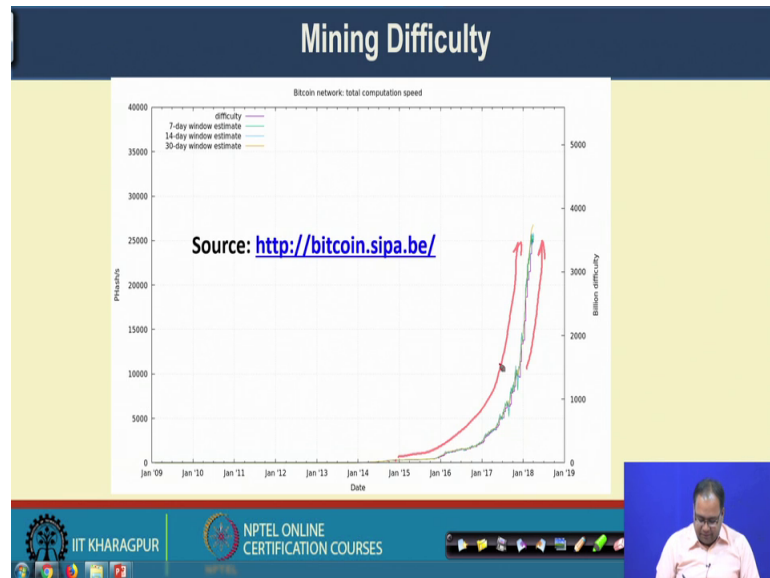
The slide is titled "Mining Difficulty" and contains the following text:

- Current difficulty: 3511060552899.72 (as of 2nd April, 2018)
– <https://blockexplorer.com/api/status?q=getDifficulty>

The slide features an illustration of a miner with a pickaxe and a Bitcoin symbol. At the bottom, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a small video inset of the presenter.

So, this is the current mining difficulty as of a second April 2018 ah. So, this large number represents the current difficulty level for a blockchain network, for a bitcoin network ok.

(Refer Slide Time: 16:18)



So, if you look into that how difficulty level has changed over time? Ah. So, this curve gives you that how the difficulty level a changes got changed over time. So, you can see that a mostly from January 15 to the current time, we have a sharp increase in the difficulty level. So, later on will see that presently more and more miners are coming with higher hardware or high power hardwares to mind the blocks.

So, that way the mining has become more faster now a days. So, to control that the bitcoin network has gradually increase the difficulty and we can see a certain sharp in increasing the difficulty level in the last a few months, where a large number of miners are participated in the mining procedure with which specialized mining hardwares

(Refer Slide Time: 17:26)

Mining Hardware

- Specialized hardware
 - GPU
 - FPGA
- ASIC – *Application Specific IC SHA256*
 - Released in 2013
 - Fast computation of SHA256




Image source:
<https://steemkr.com/bitcoin/@pawank/bitcoin-mining>

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, as I have mentioned there are multiple a specialized mining hardware's, which are available now a days in the market ah. So, initially people have started doing the mining on the standard computer, then they have find out that well by participating in the bitcoin mining procedure you can get more benefit you can get more than you can earn bitcoin.

So, the miners they have started developing hardware's for that, and initially people have moved from the CPU based hardware to the graphic processing unit GPU based hardware's and gradually recently they have moved to the hardware based on APJ boards. So, this diagram actually shows you a hardware with multiple APJ boards ah. So, then in 2013 so, we had based ASIC based mining hardware, the full form is of ASIC is application specific application specific integrated circuit, application specific integrated circuits. So, this ASIC was designed to perform this SHA 256 hash in a faster way. So, if you remember that in bitcoin mining procedure we apply SHA 256 bit hash function.

So, to increase the mining speed what you have to do that you have to generate more number of hashes per unit time. So, this ASIC at the first ASIC was released in 2013 for this first computation of SHA 256 based bit hash function and this diagram is for a mining hardware corresponds to this ASIC design.

(Refer Slide Time: 19:05)



The slide features a dark blue header with the title 'TerraMiner IV' in white. Below the header, on the left, is a photograph of a black, vertical mining rig with its side panel removed, revealing internal components like fans and circuit boards. To the right of the image is a yellow background containing a bulleted list of specifications. At the bottom of the slide, there is a blue footer with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a small video inset of a man in a pink shirt.

TerraMiner IV

- ASIC based bitcoin mining rig
- 2 Terahash per second
- Cost: USD 3500 approx

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSES

So, here is an use case which we called as the terra miner 4 ah. So, this terra miner 4 is a ASIC based bitcoin mining rig which is has multiple such APJ boards in bill, which can perform first computation of hash function it can perform 2 terrahash per second, that many number of hash it can performed. So, you can imagine that how many number of such 256 bit SHA 256 hash function, it can perform and the current cost a for this hardware is approximately 3500 US dollar.

But, nowadays even this hardware is not sufficient people have started building up mining pool or combination of multiple hardware's together to perform this mining a operations.

(Refer Slide Time: 20:00)

Mining Pool

- Pooling of resources by the miners
 - Share the processing power over a network to mine a new block
 - Split the reward proportionally to the amount of work they contributed

Pool Name	Percentage
ETC.com	24.2%
SlushPool	18.7%
AntPool	14.4%
ETC.TOP	9.6%
ViaBTC	9.5%
Unknown	9.3%
F2Pool	7.1%
ETCC Pool	4.4%
BitClub Network	2.9%
BitFury	2.4%
Bitcoin.com	1.4%
SBCON	1.2%
BitCOIN	1.2%
KanoPool	0.8%
GBMiners	0.8%
ConnectBTC	0.2%

Hash-rate Distribution:

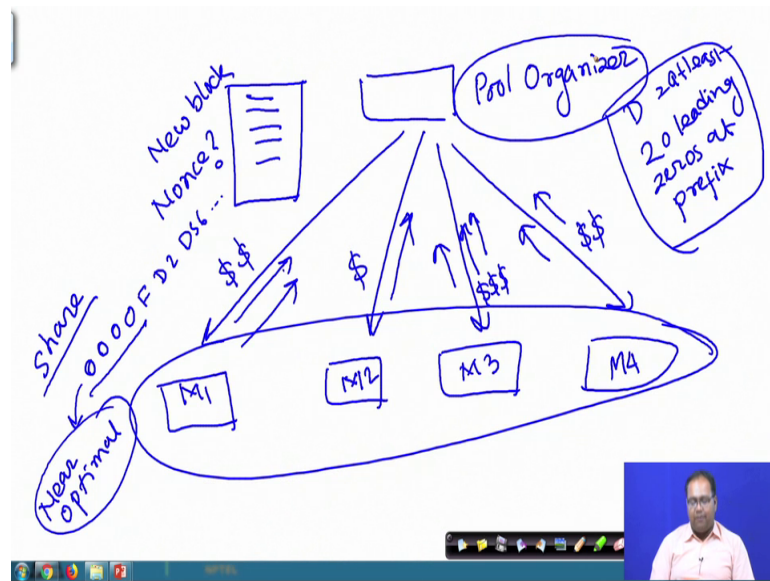
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Well the point that I mention that the mining pool it is an interesting concept in a blockchain network and bitcoin network. So, the idea of this mining pool is that you combine multiple miners together; the resources available from multiple miners together and then you ask the miner to generate the hash in a distributed way.

So, every miner will start to generate the hash for a block and they will basically share their pricing power over the network to mine a new block. So, the broad idea can be explained with an example.

So, let me show you an example of that.

(Refer Slide Time: 20:44)



So, you have a pool controller or some time will we call it as pool organizer, who is a whose start case to construct a propose a new block. So, the pool organizer say has constructed a new block with multiple transactions and the task would be. So, this is the new block that has been constructed by the pool organizer and the pool organizer has constructed the new block and the task is to find out the nonce for this block.

Now, there are multiple miners say M 1 M 2 M 3 and M 4. So, we have multiple miners. So, the pool organizer informs these new block to all the miners. And ask them to find out the hash value corresponds to that. Now, what happens every miner independently tries to find out this nonce value and whenever they are finding out a nonce value, say assume that the current difficulty level ask for say 5 say 20 leading zeros 20 leading zeros at the prefix say this the current mining difficulty. If this is the current mining difficulty then what individual miner can do they can try to find out the hash value where there are approximately a 20 leading zeros at the prefix. So, the miners can propose something called a share.

So, what is the share get like a whenever the miners are generating blocks, the miners will generate blocks something say they can generate the block something like 2 D 5 6 something like that. Here I do not have 5 20 leading zeros so, this index. So, this 4 0 signifies for 16 leading zeros ah. So, in this case this is the kind of we call this kind of hashes as a near optimal hash. So, this a kind of near optimal hash. So, this near optimal

hash ensures that well this particular block is not the optimal 1 that is intended for, but this particular miner is close to optimal.

So, that way it is miner also forwards this near optimal blocks to the pool organizer as well as the blocks which is optimal. So, if the miner can find out a hash one of the miner can find out a hash where you have at least 20 leading zeros, I should mention it as at least at least 20 leading zeros at the prefix then that is the solution.

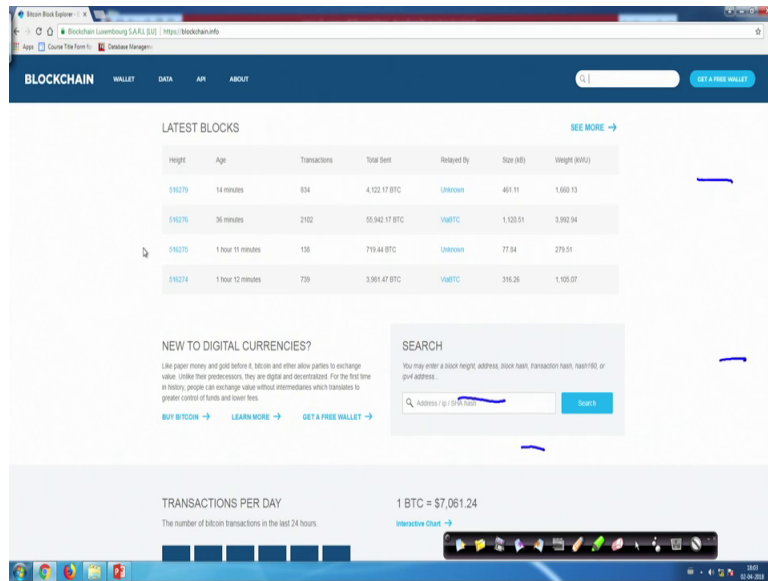
So, assume that M 2 has were able to find out such a block and M 2 is sharing this block with pool organizer and M 3 was a able to find out 3 such near optimal hash values, which are closer to the original hash value and M 4 was able to find out 2 such hash value ah. So, the idea is that the way they have participated in this mining procedure. So, whenever all it is 4 miners they are trying to collectively find out the nonce value for a single block, the probability that one of them will be able to find it out it becomes hash compared to if a single miner tries to find out the hash value for the entire block.

So, that way this mining pool concept, it can increases the probability of a getting a new block and at the same time this near optimal solutions that every miner is sharing with the pool organizer from this near optimal solution the full organizer can decide that how much work has been done by individual miners. So, this miner was able to send a 2 a such near optimal solution. So, the idea is that whenever you are paying to this miner you say pay 5 say 2 dollar to this miner this miner able to generate 1 year of optimal solution. So, you pay 1 dollar 1 to this miner this one was able to generate to near optimal solution.

So, you paid 3 dollar to this one this one able to generate to near optimal solution. So, you pay to pay 2 dollar to this miner. So, that way the total block reward that the pool organizer is getting that particular block reward can be shared by multiple miners who are participating in the mining pool ok.

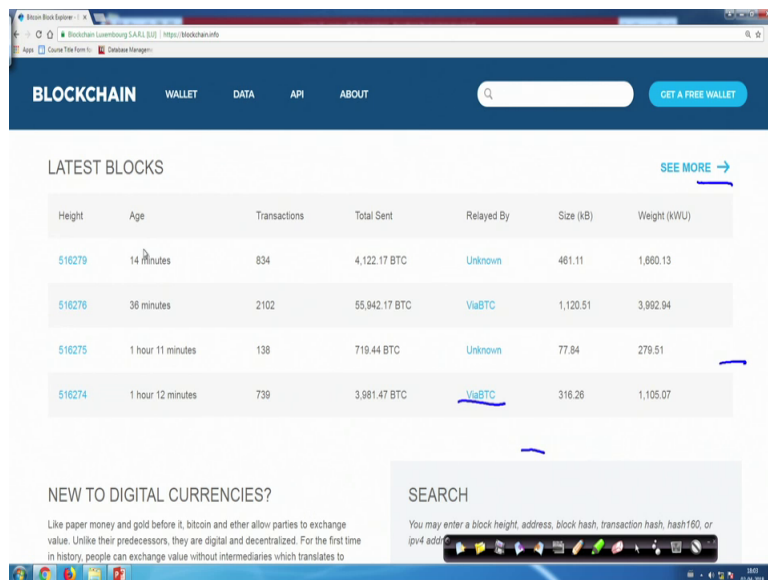
So, that is the broad concept of mining pool and there is a distribution of multiple pool which are there in the today's bitcoin network. So, this BTC dot com an pool BTC dot top via BTC they actually text huge share of the mining pool and a one of the interesting statistics a that I can show you.

(Refer Slide Time: 26:36)



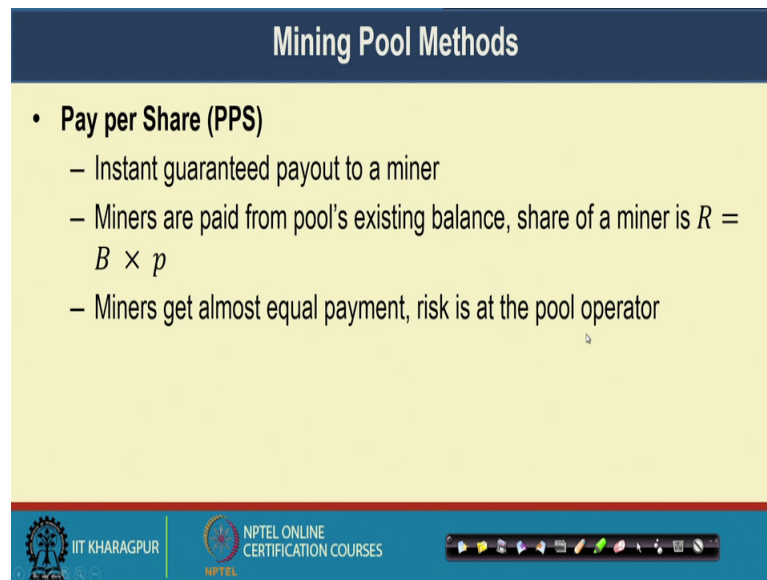
So, well in this a the blockchain that info website you can see you can see the latest blocks which are being generated by multiple miners who are actually generated the block.

(Refer Slide Time: 26:47)



And, this is the height of the block. So, currently the bitcoin blockchain has this many number of blocks 5 1 6 2 7 9 number of blocks.

(Refer Slide Time: 28:06)



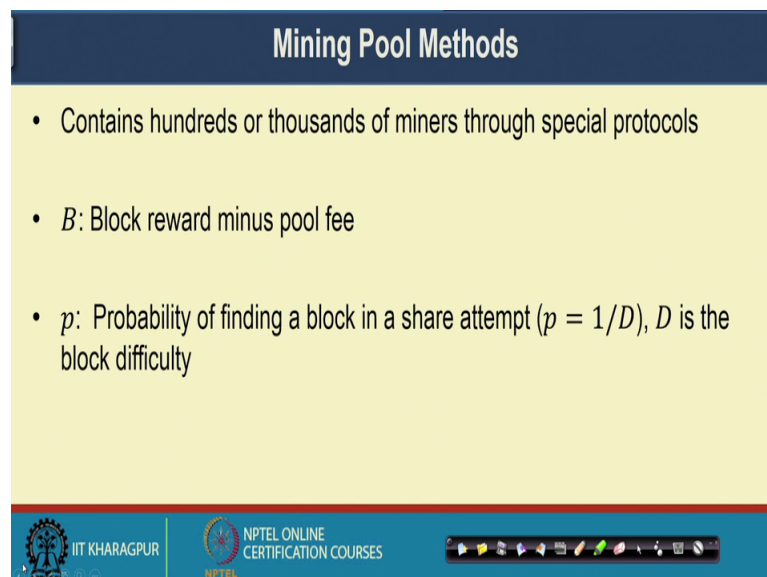
Mining Pool Methods

- **Pay per Share (PPS)**
 - Instant guaranteed payout to a miner
 - Miners are paid from pool's existing balance, share of a miner is $R = B \times p$
 - Miners get almost equal payment, risk is at the pool operator

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Ok. So, let us look into that how the shears are distributed among different miners in a mining pool.

(Refer Slide Time: 28:13)



Mining Pool Methods

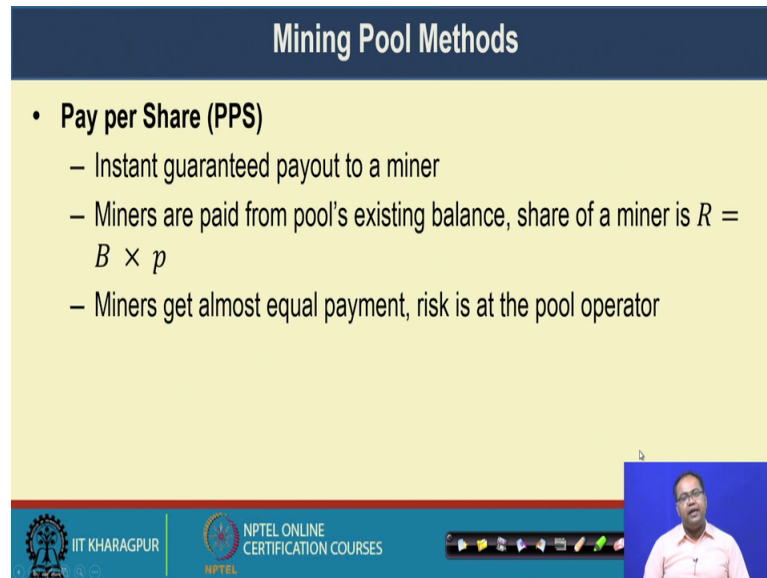
- Contains hundreds or thousands of miners through special protocols
- B : Block reward minus pool fee
- p : Probability of finding a block in a share attempt ($p = 1/D$), D is the block difficulty

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, in a mining pool there can be hundreds or thousands of miners, who communicate with each other to some special protocols that I have discussed earlier. So, assume that capital B is the block reward minus pool free. So, every pool has whenever you are participating to some mining pool, you have to give some fee for that and B is the block $B - 1$ minus the pool fee the effective reward that you are getting.

And p is the probability of finding a block in a shared attempt whenever multiple miners are trying to do that, and if D is block difficulties then you can say that $1/D$ is the probability for finding a block.

(Refer Slide Time: 29:00)



The slide is titled "Mining Pool Methods" and features a yellow background with a dark blue header. A single bullet point is listed under the heading "Pay per Share (PPS)". The bullet point contains three sub-points: "Instant guaranteed payout to a miner", "Miners are paid from pool's existing balance, share of a miner is $R = B \times p$ ", and "Miners get almost equal payment, risk is at the pool operator". At the bottom of the slide, there is a blue footer with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a small video inset of a speaker.

Mining Pool Methods

- **Pay per Share (PPS)**
 - Instant guaranteed payout to a miner
 - Miners are paid from pool's existing balance, share of a miner is $R = B \times p$
 - Miners get almost equal payment, risk is at the pool operator

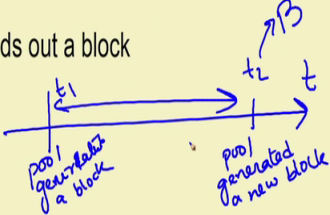
Now, you have multiple mechanism like a for distributing the share 1 is called the pay per share in pay per share architecture, you have instant guaranteed payout to a miner ah. So, whenever miner is joining in the mining pool, you pay the miner from the pools existing balance and share of the miner is calculated as a B times p.

So, this constant amount of money is given to every individual miner who is joining in the pool and in this particular architecture pay per share the miners get almost equal per payment ah, but a risk is at the pool operator. So, it may happen that a the pool is not able to find out any new block, but because this is a kind of instant payment and a guaranteed payment to the participant or to the miners who are participating in this pool, it may always happened that the pool is not getting any reward they were not able to mine any new block, but still the operator need to pay to the individual miners who are there?

(Refer Slide Time: 30:14)

Mining Pool Methods

- **Proportional**
 - Miners earn share until the pool finds a block (end of mining round)
 - $R = B \times \frac{n}{N}$, where n is amount of his own share, and N is amount of all shares in the round
 - Payments are made once a pool finds out a block



The diagram shows a horizontal timeline with two vertical tick marks labeled t_1 and t_2 . Below t_1 , it says "pool generated a block". Below t_2 , it says "pool generated a new block". A blue arrow labeled B starts at t_2 and points to the right, representing the block reward.

Then there are methods like proportional a share in case of proportional share the miners on share until the pool finds block ah. So, at each of every mining round whenever the pool is finding out a block, you find out that what is the total share of the individual miners.

So, the share buy a share we mean the near optimal solution that the miners are able to find out assumed that capital N is the total amount of shares in the round and small n is the amount of the share of a particular miner. So, you divide the block reward in proportional to the amount of share that has been generated by the miner in this current mining round. So, a mining round means say at say this is the time instant at this particular time instance, this pool has pool generated a block generated a block and again say that t_1 a t_2 the pool has generated a new block.

So, within this time duration we compute these shares and in proportion to that share the total mining reward is so, the pool is generated a new block means; at this time the pool get some reward be this reward is distributed among a individual miners in the pool. Then a we have pay per last n share PPLNS.

(Refer Slide Time: 31:55) \

Mining Pool Methods

- **Pay per Last N Share (PPLNS)**
 - Similar to proportional
 - Miner's reward is calculated on the basis of N last shares
 - Miners get more profit for a short round

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

In PPLNS is method it is similar to the professional share the only difference is that here in capital N, we are considering the amount of all shares in the round in case of PP in the in the next method we consider only the last N shares.

So, among the last N share a how much share was obtained by a particular miner and that way the miner get more profit ah. So, in that way if you are round is small; that means, if you can quickly find out new block. So, you will get more share in this particular pay per last N share method.

(Refer Slide Time: 32:46)

Mining Pools – Pros and Cons

- **Pros**
 - Small miners can participate
 - Predictable mining
- **Cons**
 - Leads to centralization
 - Discourages miners for running complete mining procedure

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, the advantage of mining pool is that small miners can participate in a mining pool and you have a kind of predictable mining like a whenever you have large amount of miners who are participating in the a mining procedure, you can say that well there is a high probability that the pool will be able to find out a new block, but the problem with this kind of a architecture is that it leads to centralization.

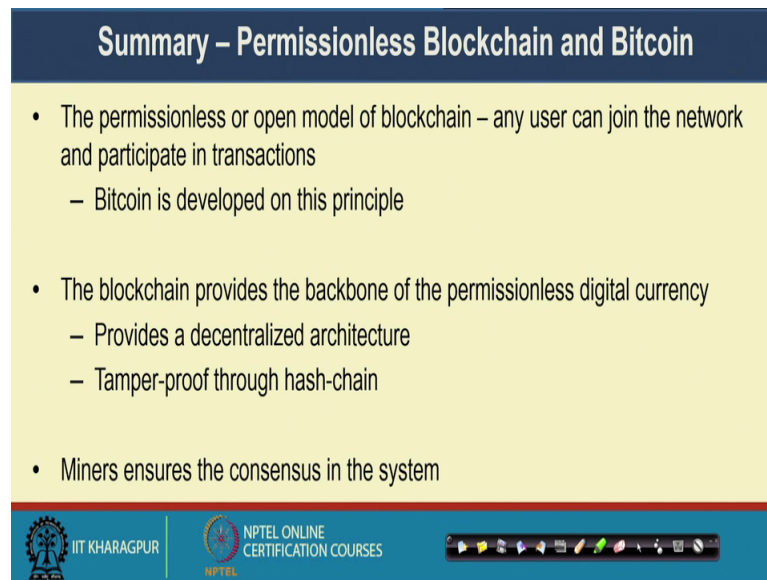
(Refer Slide Time: 33:24)

Height	Time	Relayed By	Hash	Size (KB)
516279 (Main Chain)	2018-04-02 12:18:47	Unknown	00000000000000000000007e238a5203abb85237975d1437b2845cd12574dbf4db	461.11
516278 (Main Chain)	2018-04-02 12:12:13	BTC.TOP	00000000000000000000164f6c29c87000819eb377e6c2a849b4a80278b3190b	981.3
516277 (Main Chain)	2018-04-02 12:03:33	BTC.com	0000000000000000000034506ad1f0f0ac2484ae5f6b11b8cd1ca57baDec27f67	1,133.24
516276 (Main Chain)	2018-04-02 11:56:47	ViaBTC	00000000000000000000439b4f0b9321291e8877803e487e440b248bd146b23ae	1,120.51
516275 (Main Chain)	2018-04-02 11:22:28	Unknown	00000000000000000000037c4408b564831c78b2bd30d81263271ecb04a9426975	77.84
516274 (Main Chain)	2018-04-02 11:20:48	ViaBTC	0000000000000000000015b5bd5cd3438dcaec9610c7a85ab99e4d579dc2132b4	316.26
516273 (Main Chain)	2018-04-02 11:14:26	BTC.com	0000000000000000000038bca9f6e8343af73c31276398514de3b174971de095	78.37
516272 (Main Chain)	2018-04-02 11:12:25	ViaBTC	000000000000000000000341bea614960357f82abf6d2b7edfbc8e55e34006721f	40.83
516271 (Main Chain)	2018-04-02 11:11:29	Unknown	000000000000000000004a59701a050833244e5309d6939532b7763124796ac3a0	70.73
516270 (Main Chain)	2018-04-02 11:10:02	BTC Pool	000000000000000000001a958ec7344b6a7053438692d2736024e6e304ac2931	211.31
516269 (Main Chain)	2018-04-02 11:06:28	BitClub Network	000000000000000000001125962b14de1f032c4165c56303e4e5303037026d113c	520.4
516268 (Main Chain)	2018-04-02 11:03:19	BTC.com	000000000000000000000011388	

So, if you if you look into this it is a blockchain data info website and if you look into this a blocks recent blocks, which are being relayed by multiple miners you will find out that the same miners is realying multiple blocks 1 after another. So, this BTC dot com is relaying multiple blocks similarly via BTC is also relaying multiple blocks. So, all the blocks that are getting relayed they are actually coming from they are they are coming from some fix number of mining pools either via BTC or say via BTC or BTC dot com again via BTC.

So, a notion of monopoly you can see in can be seen with this architecture. And it also discourages the miners from running the compute mining procedure, because it happened that the miner well if they had able to generated some 4 4 almost complete a block or almost complete has on your optimal has their happy that well they are going to get some amount of share. So, they may not participate further in the future.

(Refer Slide Time: 34:44)



Summary – Permissionless Blockchain and Bitcoin

- The permissionless or open model of blockchain – any user can join the network and participate in transactions
 - Bitcoin is developed on this principle
- The blockchain provides the backbone of the permissionless digital currency
 - Provides a decentralized architecture
 - Tamper-proof through hash-chain
- Miners ensures the consensus in the system

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Well a in summary in a till now, we have look into the permission less or the open model for blockchain. So, we have look into the permission less or open model for blockchain where any user can join the network and participate in the transactions and bitcoin is developed based on this principle.

So, the blockchain it provides a backbone of the permission less digital currency by providing a decentralized architecture and by providing architecture, which is tamper proof with the help of hash 10 based technology. And then this mining procedure in a permission less blockchain it ensures the consensus in the system ah. So, that is the broad idea of a this permission less blockchain architecture so, in the next a week classes will start with another model of blockchain, which is called the permission model of blockchain and we will see that how a traditional distributed system algorithm becomes more powerful for permission blockchain environment. And then from there we look into different application of blockchain apart from the financial domain, see you again during the next class and ah.

Thank you very much for attention.