Introduction to Blockchain Technology and Applications

Prof. Sandeep Shukla
Department of Computer Science and Engineering
Indian Institute of Technology-Kanpur

Lecture No. 08
Blockchain Technology and Applications

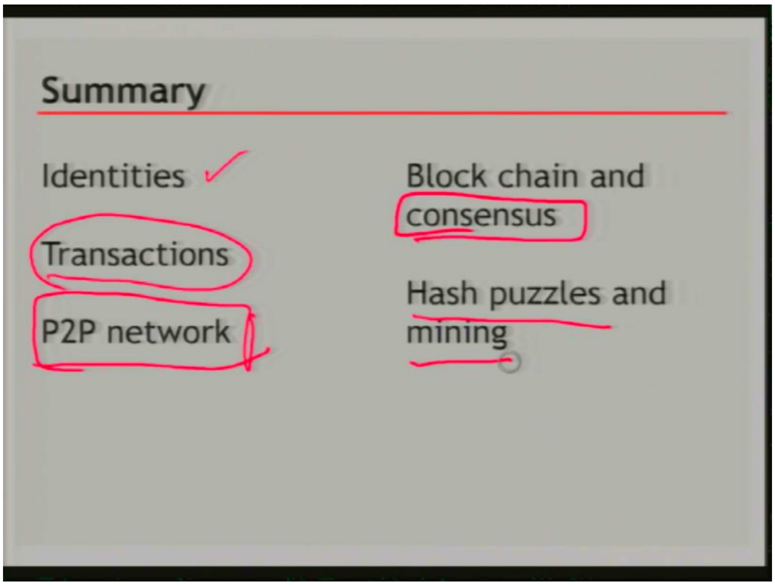
Welcome back. So, we have been discussing in the last few sessions about the bitcoin, blockchain, consensus mechanism. And we have seen that consensus in bitcoin is actually a heuristic method. It uses incentives for miners to behave properly according to rules. It also uses the, you know, flexible deadline for achieving consensus which basically leads to an eventual consistency of the blockchain on all its replicas.

It also you know allows you to the world any sybil attack by making the probability of making your being the being the next reward winner proportional to your global hash power. And we also saw the economics that should be the mind of the miner in terms of whether to participate in the mining process or not. When we go into the, you know, public blockchains, the private blockchains or permissioned blockchains.

We will see that most of them did not have a currency associated with them. And if they did not have a currency associated with them, a currency is not mined within the blockchain or if the currency that is mined does not have any market value. Then we have we need another kind of consensus we cannot depend on this kind of participatory consensus mechanism. So but we will we will get to that later.

When we go into the permissioned, non permission blockchain on non public blockchain and but for public blockchain, most of the public blockchains use some form of mining, which are, you know, some variant of this and so, let us understand it finally, you know putting it all together.

(Refer Slide Time: 02:23)



Summary

Identities ✓

Transactions

P2P network

Block chain and consensus

Hash puzzles and mining

So, there are several concepts that we have discussed. We discussed the notion of identities in case of permission free, permission-less blockchain, what we see that identities are not tied to real world identities, your public key hash of the public key is kind of your identity. And this means, that I can create as many identities as I want. And many times the way the blockchain transaction rules are, you have to create multiple identities.

For example, if you are paying somebody some amount and you have some left, then you have to create an alternative address that is controlled by you to which you have to send the rest of the money or that is called a change address. So, every time you make a new transaction, you have to create a new identity. So, everybody will have many identities. So, in a network with a with such kind of identity, which is not tied to real world identity, there is a possibility of a sybil attack which means that somebody might create too many identities to wield more power.

Let us say in a, if there is a voting being done, to do some computation or to do leader election and so on. So therefore, what we have seen is that to do it, the Sybil attack, the mechanism of consensus in blockchain has built in criteria that the probability of you being the winner in cases of competition to be the maker of the next block, your probability will not depend on how many identities you have, but rather it will depend on how much resources you have.

So, by creating more identities, you cannot increase your resources. So, therefore, the processes sybil attack proof, you also saw the transactions, how the transactions are represented and you know the transactions are represented by giving transaction number inputs and outputs. And then every time you make a new transaction, you have to spend from the output of a previous transaction if that output was assigned to you.

And by using your signature, you prove that you actually are the rightful or authentic owner of that outputs destination and therefore, you are to use that amount and finally the amount should be such that the input amounts should be equal to the output amount and in case you are giving a transaction fee, the input amount should be little more than the output amount. So, therefore, not having balance will not be a problem like as we were discussing earlier that you have to check your balance.

In your account is more than your amount transaction amount that problem cannot happen here because your input some of the input should be equal to the sum of the outputs or inputs should be slightly more than the outputs in case of transaction fees. We also saw that all transactions are actually broadcast to everybody and the broadcast mechanism is through a peer to peer communication.

And what it means is that, so, bitcoin is an application level protocol, bitcoin protocol and underneath it is there is a network and above the network like TCP IP layer, you have also another layer which is the P2P layer. So, whenever you are trying to put a transaction into the network, you basically broadcast it to all your neighbors and then your neighbors will broadcast it to their neighbors, and so on.

And then eventually some of the nodes will actually receive same transaction from multiple different sources because you are broadcasting it this way. And they will have to ignore the ones that they already have seen. And we will talk about that in the next series of lectures in the class, but that is the idea. So the P2P network is one of the, you know underlying layer of protocol on top of TCP IP and below the bitcoin protocol.

The consensus mechanism is what we focused mostly on in this lecture, and it is very important for us because without the consensus, we cannot decide what should go into the blockchain next. And so the block that is added at any point in time should be, you know, decided based on a consensus. But we also saw that this consensus mechanism here is not exactly like the consensus mechanism that was considered in distributed computing like in the context of distributed databases.

Because there are so many impossibility results which might make you consider abandoning the idea of building a consensus protocol in a de-centralized distributed in environment like this but we saw that we actually change the model. We basically change the model in the sense that malicious nodes we assume maybe meant to behave according to rules by giving incentives.

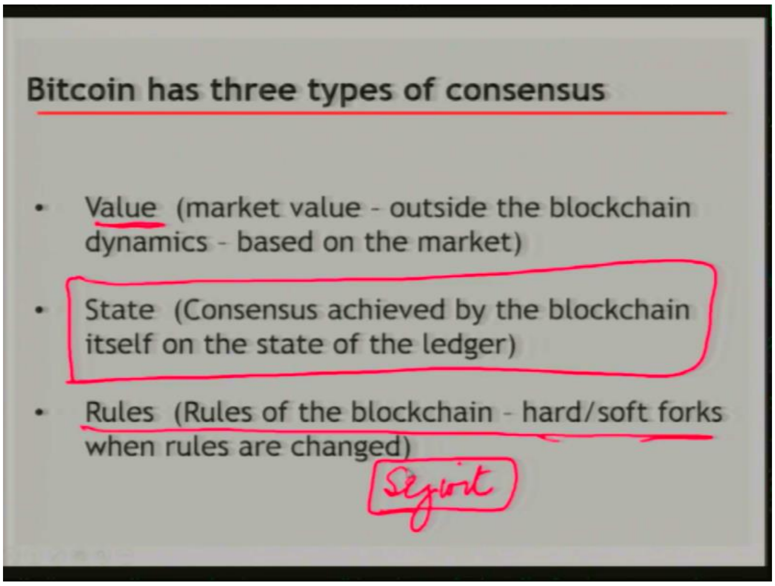
So, therefore, the whole assumption about maliciousness that is used in the old literature is a little bit changed. Second thing that we are doing is that we are not saying that consequences should happen within each round. So when a set of transactions; when each node accumulates enough transactions; they may propose a block, they solve the hash puzzle, and then they broadcast if they win.

And then multiple people may actually win at the same time or close to each other in time. And then they might broadcast there is also there might be a race condition, however, eventually be race condition will be resolved. And that is, what is the eventual consistency? So, we are allowing our consensus to be based on eventual consistency which is also different from the traditional model of a distributed consensus.

Finally they are guarantees are probabilistic, which is that the nodes the way they behave, and their possibility of broadcasting or not broadcasting is all probabilistic. So therefore, it is a randomized consensus. And all this thing together gives us the, the protocol that works in practice. And finally, the other issue the hash puzzle we have been talking about from the very beginning. And we see we saw how the hash puzzle plays important roles in the mining miners are made to solve the hash puzzles to show their proof of work.

And the proof of work we assume is actually dependent on how much computational resources you are putting in and therefore, person who solved the hash puzzle faster, has more computational resources, and therefore the probability of them winning the competition to make the next block is proportional to the computational resources that they have. So that is the kind of the summary of what we have been discussing.

(Refer Slide Time: 10:14)



Bitcoin has three types of consensus

- Value (market value - outside the blockchain dynamics - based on the market)
- State (Consensus achieved by the blockchain itself on the state of the ledger)
- Rules (Rules of the blockchain - hard/soft forks when rules are changed)

Segwit

Now few more general things about bitcoin. So, bitcoin actually has 3 types of consensus. And all the 3; consensus are not done through the bitcoin protocol. So, the second one here in this list is actually called a state consensus. That is, the blockchain runs the protocol, so that the state of the ledger consistent throughout all the replicas. So that is the consensus that we try to achieve through this protocol.

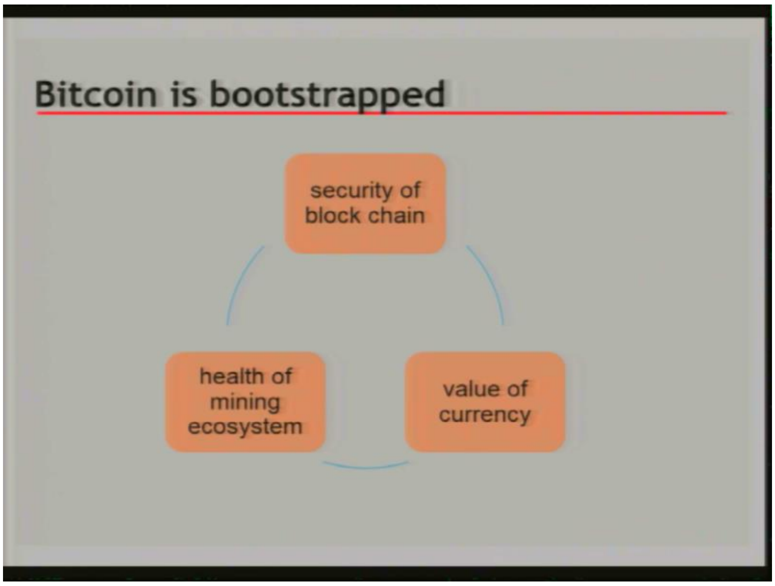
And that is what we discussed all along in the last few sessions. But there is also a value consensus that is the bitcoins market value. This market value is not now has nothing to do with the bitcoin protocol. It has to do with lots of extraneous factors such as you know, what is the news in the market or how the investors seem they bitcoin. Bitcoin going up and down up or down in value.

And therefore, this is also done through a distributed system process there is no central authority or bank that decides the value of the market value of the bitcoin, but, actually it is decided on by a decentralized process based on demand and supply and then there is a there are rules. So, we said that there are certain rules in bitcoin, for example, how the transaction validity plays out how the hash puzzle works out, what is the difficulty of the hash puzzle.

And all these things are actually the rules and this rule should be played along by everybody. So, that is another consensus. And then if a large number of nodes decide to play by a different rule, then there is something called forking in the blockchain. So, you will see that 2 years ago, there was a change in the block structure and this is called the Segwit. And because of segwit, there was actually a fork, in the hard fork in the bitcoin.

And there was a block cache version of bitcoin that forked out of the blockchain. So this; so, we worried about the second type that is the ledger consensus, but the other consensus are also important in the entire scheme of things. The other issue is that we want to point out is that bitcoin is bootstrapped.

(Refer Slide Time: 12:47)



Bitcoin is bootstrapped

Now, what do I mean by this? So when the bitcoin came into existence, very few people knew about it, only people in crypto community knew about it and the amount of for mining resources was you know desktops and laptops and so on, and therefore be anybody and everybody had almost equal chance of winning the next block. And what that meant is that nobody had the ability to overpower the existing chain and creator.

You know, fork or create a different chain than the legitimate consensus chain. And that has changed drastically over time as some people have put in more resources for bitcoin mining, and therefore the health of the mining may be deteriorating. And as we get news of the health of the mining system, being bitter being worse, for example, if there is news that China is going to nationalize all the wallets, blockchain mining companies and put them, consolidate them.

That would mean that investors will immediately panic that there might be a 51% hash power within that consolidated company. And therefore, the blockchain can be easily subverted and your old transactions may become invalid, people will take out their investment from bitcoin. And what that would do is that the price of the bitcoin the value of the currency will fall. So health of the mining ecosystem and the value of the currency are related to each other, the how they are related to each other.

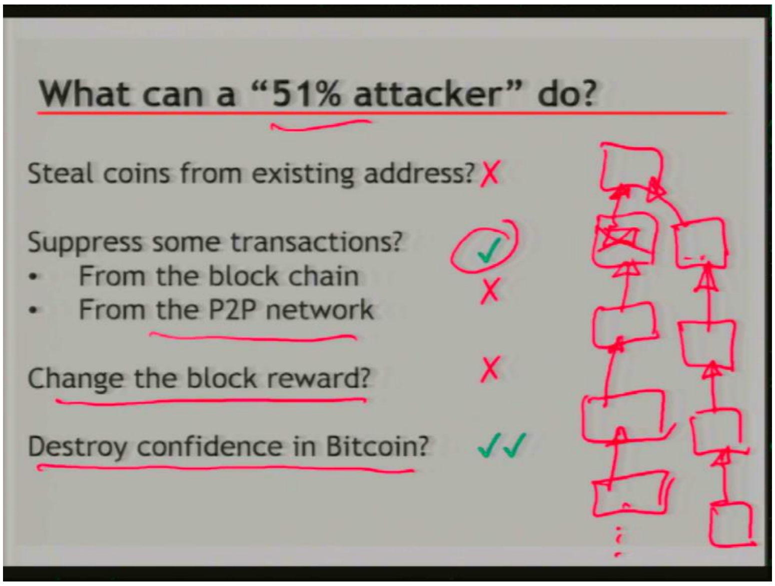
So, we just saw we just described how the health of the mining system influences the value of the currency. On the other hand, the value of the currency also influences the health of the mining system, because if the value is very small, people learn will not invest in computational resources to do mining, very few people will do mining and therefore there will be no competition to create the mining.

And therefore lesser mining resources, there are the chances of somebody actually among the risks of the miners becoming 51% becomes higher. So, therefore, the value of currency falls means that a lot of people will leave the mining business. The other thing is the security of the blockchain if the security of the blockchain which is dependent on the health of the mining system we have been saying this that if the mining ecosystem is not healthy, then you might see 51% attacks and maybe other kinds of attacks.

And therefore, you will see that the blockchain security is compromised once the security compromises the value falls, because investors will fly because they will see that there is no value in the in the currency there is no security so anytime the bitcoin, old transactions become invalid and so on, nobody is going to invest. So as the value of the currency falls, the more miners will flee and then the security will decrease.

So, this is kind of a cycle so in that sense that all these 3 things kind of is must be in equilibrium in order for the bitcoin to retain its value, retain its security of the ecosystem and have enough miners to mine bitcoin. So that is, the point that is discussed here.

(Refer Slide Time: 16:22)



What can a "51% attacker" do?

Steal coins from existing address? ✗

Suppress some transactions? ✓
- From the block chain
- From the P2P network ✗

Change the block reward? ✗

Destroy confidence in Bitcoin? ✓✓

Now, one more thing is that we keep hearing in the news about 51% attack possibility. So what can a 51% attack do? 51% attack can actually do a lot of things but not everything. For example, a 51% attacker cannot steal point from an existing address, because that existing address might have points and it received those clients through some approach as output of a previous transaction and only way to steal those clients is to know the private key of that addressing.

If you did not know that private key, you can never redeemed the coin. So 51% attacker or not, it is cryptographically protected. It is not based on the consensus, the 51% attacker can only influence the consensus or how the blockchain develops, but it cannot subvert cryptography. Second thing is that can it suppress some transactions from the blockchain? Yes, because it can actually if it has 51% power, it will start developing another chain.

So, if this is the original chain where your transaction was there, and then it will start and then you actually got 6 confirmations. So you are now or got 5 confirmations and you are waiting for a one more confirmation before you are you can redeem. At that point, the 51% attacker can come and start building here, another branch of the chain and since he has more hash power, he keeps building more and more of these.

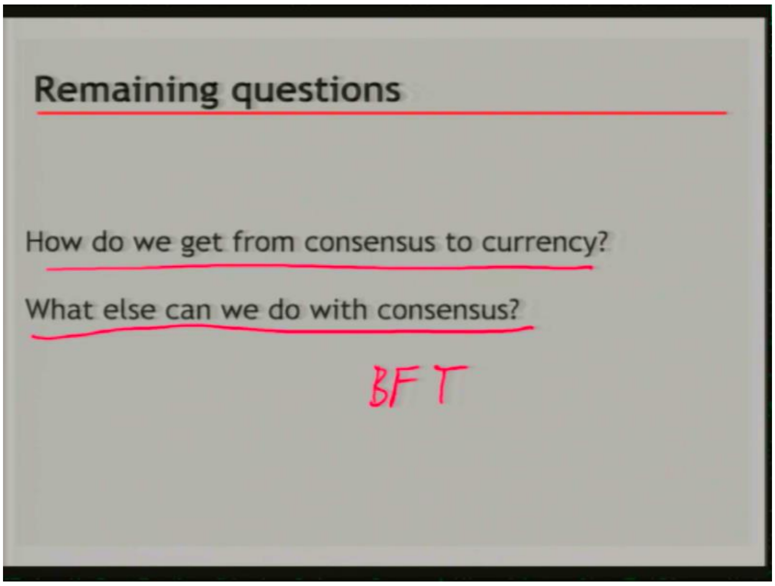
And others also get fooled and start building on this and this becomes longer. So then your transaction becomes no longer part of the permanent record. And therefore, you are you cannot redeem that money. So, that is a possibility. And that possibility can also happen if you had six confirmations if 51% attacker attains let us say 90% so in that case, he can really build every 10 times, 9 blocks will be built by him, and therefore, he can very quickly surpass even the 6 length long confirmation.

So that is a real possibility depending on how much above 51% is and even with 51% there is a probability that you will make more than half the blocks and therefore he can surpass the existing chain. But he cannot surprise the transaction when the transaction is being broadcast into the P2P network that requests an attack on the P2P network by network cyber attack rather than on the consensus process or on the block making or under any other cryptographic technique.

So that he cannot do carry change the block reward, no he cannot change the block reward because block reward is part of the rule. And therefore, you know even if you are 51% you cannot make blocks which gives you more reward because if you do give yourself more reward, then others will not validate that block and therefore, you know, you will not be able to do this. Now, what you can do very well is the, destroy the confidence in the bitcoin ecosystem.

And therefore, the value of the bitcoin will fall miners will flee and the whole bitcoin infrastructure will collapse. And that is what we were trying to actually say in the previous one, that all of these things should be in equilibrium so that the entire ecosystem does not collapse. The value collapses the miners flee and therefore, you know transactions cannot be cannot be put in into the block or securely and things like that.

(Refer Slide Time: 20:20)



Remaining questions

How do we get from consensus to currency?

What else can we do with consensus?

BFT

So, the remaining questions that will take up next in the next classes is that how do you get from consensus to currency? And so, because we discussed consensus and we discussed, you know, creation of currency, but eventually there has to be a mechanism and how the way the consensus gives us currency, and that is called a Bitcoin mechanism. And we will be taking up bitcoin mechanism as our next topic.

And the other question is, what else can we do with consensus? And this is the, question that we will be pondering even after when we talk about other blockchain systems, all of which will require some form of consensus. And so we will look at what other consensus mechanisms are there we see in some cases, we directly do Byzantine fault tolerant consensus, or randomized, Byzantine fault tolerant consensus.

Sometimes we do other techniques but eventually we have to have some form of consensus in order for creating permanence and verifiability in a decentralized system. So that is basically the end of this and we will be actually talking about the Bitcoin mechanics, how the transactions look like what are the different things that go into a transaction, and then how the transactions, how the blocks look like.

And how the transactions are stored in the block what kind of data structure it is stored in now you might say that if we are not interested in crypto currency, why are we going to go into that much detail of Bitcoin mechanics? The reason is that many of these concepts that are being used. There are actually pretty general so many of the bitcoins, many of the blockchains actually use those same techniques.

So, for example, the way the transactions are stored inside the inside a block is called a Merkle tree. So we discussed Merkle tree before, so all the transactions are not stored like a, like an in an array or something they are actually put into a Merkle tree. And we saw that the reason why we use Merkle tree is because the searching for a transaction is faster. So the, that is the next one of the lesson from Bitcoin blockchains block structure.

That you if you have a lot of transactions, you might you might be better of putting them in a Merkle tree. And then we will see that in even later we will see that in ethereum, this Merkle tree has been further optimized. So that is the one thing. The other thing that we will look into is that in a Bitcoin the, you did not just put your signature and you did not just put your destination address, but you actually write some scripts.

And those scripts are executed by everybody who wants to validate that transaction. And this scripting execution basically make allows you to add the script. How did that script language how much power that scripting language has determines how many clever way clever types of transactions you can do? So we will see that there are many type of transactions other than just kind of transactions you have seen so far.

For example, there are multi SIG transactions which allows you to jointly do something. And then multi SIG allows you to do further things like an escrow transaction. And then you can also do what is called micro payments. So there are many different ways of doing transactions cleverly with the help of the scripting language and that is called a Bitcoin scripting language. But you will see that even with the bitcoin scripting language, you have a very limited power, you can only do certain things.

And that led people to think that why cannot we write much cleverer transactions and therefore, they started thinking about a new language for writing clever, complex transactions and that led to the idea of smart contracts. So will not get into smart contracts until we get to ethereum but smart contracts are basically pretty generic language compared to Bitcoin scripting language to write complex rules for transacting.

And that means that we evolve from blockchain 1.0 to blockchain 2.0 as we introduce smart contracts. So, in order to understand smart contracts, we have to first look at bitcoin scripting language and understand its inadequacy which led to the smart contracts. That is another reason why we want to go into the Bitcoin mechanics in a more details, even though I am like totally opposed to the crypto currency.

Because the be unless we see what exists and what are its pitfalls, we cannot evolve to the next good thing and that is another thing that we will study in the bitcoin mechanics lectures after we are done with the bitcoin mechanics lecture, we will move to the ethereum. And we will look at smart contracts. But in this course will not be actually teaching you how to write new smart contracts. We will see some examples you will get some ideas, but the point we try to.

You know, put across to you is not to make you become a Bitcoin or ethereum, expert or programmer of smart contracts but rather conceptually understand what the blockchains are, what the dynamics are, and how you can use blockchain for many applications. And after we are done with the smart contracts and in ethereum context, we will move to a permission blockchain which is hyper ledger.

And we will see how hyper ledger uses smart contracts. How hyper ledger does consensus. So, consensus in ethereum is very similar to that of blocked blockchain, Bitcoin blockchain, but consensus is hyper ledger is entirely different. So, because of that, we have to understand how the consensus is done in hyper ledger and what are the other possibilities in hyper ledger to do the consensus.

And interestingly, in hyper ledger, they have a pluggable consensus so you can write your own consensus and plug it into the hyper ledger. Hyper ledger is an open source system, open low open source blockchain so ethereum and bitcoin as well. So, then we will see, what are the other applications that people are using and why are they not using one of these previous blockchains and developing their own.

So for that we will look at least one for specifically designed for IOT systems and it is called Iota and then we will look at one for the financial, you know, players, and that is called KIOTA. And then if we have time, we will see a few other blockchains. And then we will look at least 1 or 2 applications like land record on a blockchain or medical information on a blockchain this kind of an application. So, at the end, you should have a very good idea about the underlying theory of the blockchains.

And then, what are the different types of blockchain the evolution of blockchain technology and where it is applicable and how to apply them and then eventually choose choosing which blockchain is your, most applicable for, your application, and whether blockchain is at all applicable for your application. So this is the game plan here in the rest of the course. So, we will see you next time with the Bitcoin mechanics.