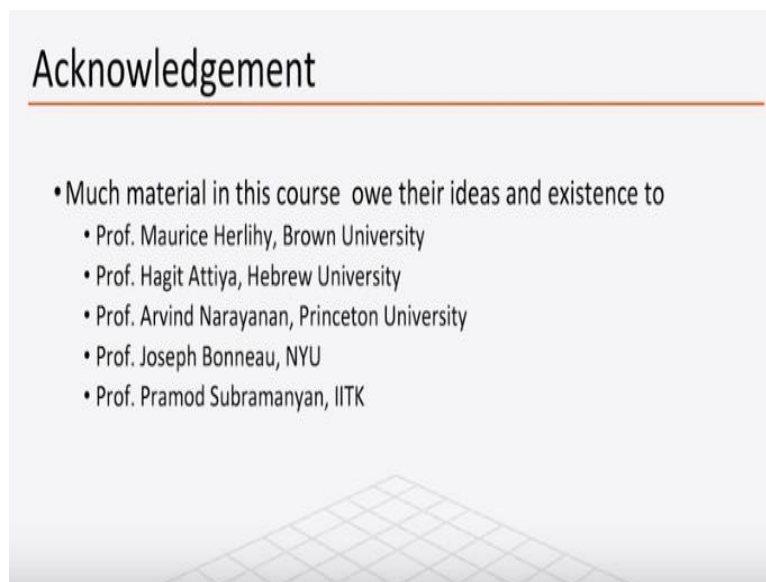


Introduction to Blockchain Technology & Applications
Prof. Sandeep Shukla
Department of Computer Science and Engineering
Indian Institute of Technology-Kanpur

Lecture - 01

Welcome to the Blockchain Technology and Applications course. I am Professor Sandeep Shukla from IIT Kanpur and I will be teaching this course. So this course, the material on blockchain today is quite commonly available at various you know universities and various conference lectures and so on.

(Refer Slide Time: 00:37)



So I must acknowledge different colleagues from various universities whose lectures and whose material and books I have used to prepare the material for this course.

(Refer Slide Time: 00:51)

What is Blockchain?

- A Linked List
 - Replicated
 - Distributed
 - Consistency maintained by Consensus
 - Cryptographically linked
 - Cryptographically assured integrity of data
- Used as
 - Immutable Ledger of events, transactions or time stamped data
 - Tamper resistant log
 - Platform to Create and Transact in Cryptocurrency
 - log of events/transactions unrelated to currency

So what is a blockchain. If you think generally, a blockchain is a linked list. So what is a linked list? All of you know that a linked list is a set of blocks which are connected to each other by some kind of a link. In case of a data structure linked list, you have the nodes and nodes are connected by pointers and pointers are basically memory addresses.

But, in case of a blockchain the blockchain is a distributed data structure, which is replicated at various nodes or various computers and therefore, the linking is not based on memory addresses. So we have a different notion of linking between nodes and each of these nodes are called blocks. So therefore, you can imagine a blockchain as a series of blocks and each block is connected to its previous block by some kind of a link.

So and it is replicated all over because replication gives you number of different advantages like if one of the replica gets corrupted, the other replicas are there to make sure that the integrity of the information contained in the in the data structure is maintained. And also replication gives you some kind of guarantee of integrity of data.

And it is distributed in the sense that the different computers involved in the blockchain platform actually are running distributed algorithms in order to maintain the data's consistency and integrity. And the consistency of the data is maintained by

a process called consensus. Consensus means that everybody agrees that the data that goes into the data structure is what they agree to put there.

And the linking as I said before, traditional link list the linking is through memory addresses. But in this case, we cannot use memory addresses for linking. So there is a cryptographic technique called hashing. So we actually use something called a hash linking and the integrity of the data is maintained because of cryptography techniques and consensus and replication.

Therefore, blockchain is a data structure that is maintained distributedly and that is replicated and main purpose of blockchain is to maintain the integrity of the data. And what is the integrity? Integrity means that the data once it has been agreed by all the relevant parties to put in the data structure, it has not been tampered with it. Nobody has come and changed the data and claim that this is the data that was put in.

That is made virtually impossible in a blockchain and that is the main property of the blockchain that it maintains the integrity of the data and as we will see that most of the applications where blockchain is used be it cryptocurrency or be it some other application, the integrity of the data is the main thing in blockchain. So what is blockchain used for? So first of all, you know many times we keep logs of events, right.

So when somebody accesses your computer, the computer keeps a log of the user names and how they authenticated themselves. Microsoft Windows gives event logs every event that happens like you open a new program on your machine or something crashes or any kind of event or you know it, you get connected to the internet. All these events are kept in event logs. So logs are very important.

When you do banking transaction bank keeps logs of when you interacted with its banking servers and what you did, what transactions you made, all this are logged. The main problem with keeping logs without any notion of protection of the integrity is that somebody can tamper with the logs and somebody can delete some of the accesses. And therefore, later on when you check the log, you would know some part of its history.

So therefore, the blockchain is designed in such a way, so that it is an immutable ledger of events, which means it is a log that cannot be changed by a malicious party or by mistake. And therefore, all the data that you put in there could be event logs, it could be transactions, it could be various kinds of accesses and modifications you do to some other thing like a data or you do a property transaction.

All these things logs has to be kept in an immutable ledger. And that is what blockchain provides. So and the tampering of this data is made virtually impossible. So we do not say it is impossible to tamper, as we will see, as we learn more that there if you have a very high computational power, which is almost impossible for individuals together.

But if you can gather that kind of computation power you can actually subvert and this all the protection and change but since it is virtually impossible, we would say that this is a tamper resistant log. And therefore, having these properties, we basically use blockchain as a platform to create and transact cryptocurrency. So cryptocurrency as we will see bitcoin ethereum, these are cryptocurrencies.

And we will see that one of the first application of blockchain was bitcoin. So the whole idea of creating currency, that whose transactions whose creation whose use everything has to be put in a tamper proof log, and without a trusted third party or without a central agency, which keeps track of this logs and it will be clearer as we go into the course. And also you know many people confuse or conflate the idea of bitcoin and blockchain.

And as we will see through the course, that cryptocurrency is just a part of the story. And there are any number of other applications in which we need to keep tamper proof or tamper resistant logs and their blockchain is a very good you know platform to use.

(Refer Slide Time: 07:50)

Why a course on Blockchain?

- Have you seen the news lately?
 - Bitcoin
 - Ethereum
 - Blockchain for E-governance
 - Blockchain for supply chain management
 - Blockchain for energy management
 - Soon: **Block chain for Nirvana**
- Is it just a hype and hyperbole?
 - Hopefully this course will teach you otherwise
 - Even if you do not care about cryptocurrency and its market volatility

So why do we need a course on blockchain, right? So it seems like you know if you look at the news and if you read mostly you know technology news, you will see a lot of news on what is happening in bitcoin. Its price is going up and down, various kinds of other issues that come up. Sometimes there are cyber-attacks on cryptocurrencies or sometimes people use cryptocurrency for various reasons or cryptocurrencies are being used for illegal activities.

Ethereum is another such cryptocurrency. Now you will also hear a lot of news like for example, you will hear that United Emirates is fully going on with blockchain for their most of the E-governance applications. Governance means that you know all kinds of things like property registration, and you know car licensing, or you know license, driver licensing all kinds of things they are doing on blockchain.

And many other countries are doing the same thing. Same thing you will hear a lot about supply chain management on blockchain or you will hear energy management especially in case of micro grids, and renewable energy, you will hear a lot about the applications of blockchain or you know electric vehicle charging stations and paying for the, you know electric charging and all that on a blockchain like in Germany.

So very soon you will hear that the blockchain is for everything, for Nirvana. So people often say that okay, so this is a new hype and a lot of hyperbole. So what we will see in this course, is that it is not a hype, and it is a technology, quite

transformative technology. So many people compare it with the advent of the Internet in transforming our lives and digitalization.

And similarly, people say that or predict that blockchain is going to be as transformative in the way we digitalize our functioning and our governance and our industrial dealings or financial markets and so on so forth. So even if you do not care about cryptocurrency and its market volatility, which is one of the biggest criticism of cryptocurrency, you will see a lot of application of blockchain which has nothing to do with cryptocurrency.

And this course, will try to teach you why that is the case. And in fact, I personally is a strong critic of cryptocurrencies like bitcoin and others. And therefore, my interest is that people learn that even if you do not care about cryptocurrency, you should care about blockchain as a technology, because it is a transformative technology. So this course is about that. So let us start with some examples where we can use blockchain.

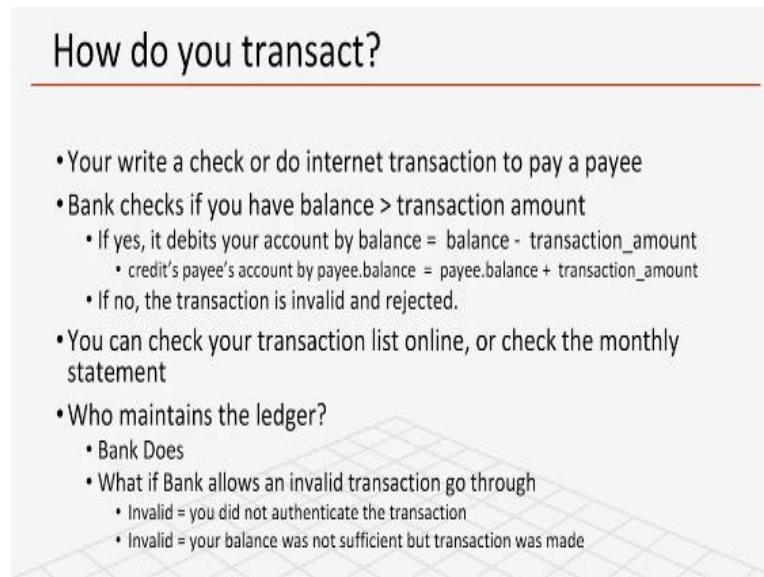
So I will first discuss some problems that you can probably solve with blockchain, and I am not going to initially talk about how we can solve it with blockchain because we have not taught you how the blockchain works, but I will tell you what the problems are with our traditional way of digitalization and probably hint at you know maybe blockchain might provide a solution. So this example is by you know from Arvind Narayanan's book.

(Refer Slide Time: 11:26)



So we will discuss how we do banking today, right. So in a bank banking system, we have multiple players, right. So we have customers ourselves, we have the bank and we have the bank employees and we have a regulatory agency. In case of India it is the RBI.

(Refer Slide Time: 11:48)



How do you transact?

- You write a check or do internet transaction to pay a payee
- Bank checks if you have $\text{balance} > \text{transaction_amount}$
 - If yes, it debits your account by $\text{balance} = \text{balance} - \text{transaction_amount}$
 - credit's payee's account by $\text{payee.balance} = \text{payee.balance} + \text{transaction_amount}$
 - If no, the transaction is invalid and rejected.
- You can check your transaction list online, or check the monthly statement
- Who maintains the ledger?
 - Bank Does
 - What if Bank allows an invalid transaction go through
 - Invalid = you did not authenticate the transaction
 - Invalid = your balance was not sufficient but transaction was made

So what happens is that when you do transactions, right. So there are multiple ways you do transactions. So let us consider two of them. One is you write a check to give money to somebody or you do an internet transaction like you log in to your banking server and then you authorize the transaction and it goes through.

What the bank does and it does automatically not necessarily through intervention of human employees is that it checks if your balance is greater than your transaction amount. If it is not, then it will say it is an invalid transaction, it will reject the transaction. If it is yes, then it will transfer the transaction amount from your account to the other person's or payee's account and your account will be debited by that transaction amount.


Now how do you know that this is done properly and correctly? You check your transaction list online or you get your monthly statement and then you check that all the transactions you made are recorded correctly. Now the question is who is maintaining this ledger from which this monthly statement is generated. The bank does. Now because of regulatory framework that we have, we do not see banks doing something wrong in this case.

We never, almost never find that, you know I made a transaction. And it was it went through. But now in my statement, I do not see it, or I do not see a normally do not see that I never did a transaction and it is appearing in my statement. This kind of things did not and does not normally happen. But it could happen. How could it happen? If the ledger is wrong.

Or if somebody inside the bank tampered with the ledger and put a transaction in there, which was not made by you. In those cases, we say that it is an invalid transaction. And you say that I did not authenticate and authorize this transaction. Or your balance was not sufficient and the transaction still went through and you do not have a overdraft account. In such cases, we say that the transaction is invalid.

Then you go to the bank, and in most cases, the bank will be very surprised and they will not know, they have to investigate. And all kinds of stuff can happen.

(Refer Slide Time: 14:14)



Bank Frauds

- You find a check was used to pay someone but you never wrote the check
 - Someone forged your check and/or signature
- You did sign a check for x amount, but the amount field was modified
 - How do you prove to the bank that an extra 0 was not there in your signing time?
- The monthly statement says that you did a transaction but you did not recall or the amount of a transaction is different from what you had done
 - Someone got your password, and possibly redirected OTP to another SIM (SIM Fraud)
 - Bank employees themselves might have done something
- How do you argue to the bank? (Non-repudiation)
- How do you argue that the amount was modified? (Integrity)
- Finally, do you tally your transactions when you receive your monthly statement?
 - Most people do not

In case of checks also somebody can forge your check. It recently happened to one of the top medical educational institutes recently. About 12 crores of money was transferred through forged checks. And those checks were checked under UV light by the banking authorities and then they turned out to be authentic checks but the institute said that it did not do the transaction.

Or what if an extra zero is put at the end of the amount field and somehow tampered with. So monthly statement will claim that you have done it, but you say that no. And another possibility is somebody obviously got your password and somehow fooled you into revealing your OTP or did the same fraud to get your OTP instead of you getting them. And in those cases also you would not know what is happening.

So it is a very difficult for the argument with the bank. So if you go and say that if you repudiate that I have not made this transaction, the bank may not believe it, because it will think that you are, you have no proof that you did not do it. So it is called non repudiation, you do not have the non repudiability, If you argue the amount was modified than the amount that you actually transacted, then you questioning the integrity of the data that is being now presented to you.

And there also you if you do not have a proof of what the original amount then your word against there's. And finally, do you even tally the transactions like if you add the entire debit and credit when you get your monthly statement. Most people do not do and therefore, we depend or we trust the bank on all these issues. So the way the bank maintains its data about your transactions is not very transparent to us.

We trust them to do it and we trust them because they are answerable to the regulatory authority RBI, and therefore we trust them. But that is what we call by a trusted third party enforced trust. And that is often a problem in case of rogue banks and things like that. And so we are advocating here is more transparency in the way the transactions are done and transactions in records are maintained.

And as we will see, that the blockchain could be one of the solutions which will provide transparency and also maintain the integrity of the data and therefore provide more reason for us to trust the banking system without a trusted third party enforcing the trustworthiness.

(Refer Slide Time: 16:56)

Supply chain and provenance

- You buy ice cream for your restaurant from supplier B
- Supplier B actually transports ice cream made in Company C's factory
- Upon delivery, you have been finding that your ice cream is already melted
- Who is responsible?
 - Supplier B is keeping it too long on the delivery truck?
 - Supplier B's storage facility has a temperature problem?
 - Supplier C says it's supplier B's fault as when picked up – ice cream was frozen
 - Supplier B says that when received, the temperature was too high, so C must have stored it or made it wrong
 - How do you find the truth?
 - Put temperature sensors in B's truck and storage, C's factory and storage, and sensor data is digitally signed by the entity where the sensor is placed and put in a log
 - You check the log – but B and C both have hacked the log and deleted some entries?
 - What to do?

Now second problem I want to talk about here is the supply chain provenance. So what happens in a supply chain is that you order something your business and you order something from another supplier and that supplier also orders various parts from a third supplier and the third supplier orders various parts from a fourth supplier. So this is what is called a supply chain.

And when the final product is made you as a business is making product whose quality depends on the quality of the components and other things that you have got through the supply chain. And therefore, if your quality has a problem, maybe it is not your manufacturing problem or your construction problem, but it is somewhere down the line in the supply chain and you have to attribute whose fault it is.

And to do that, you have to have proper transparency about where all the components are coming from. Normally, we only know the person who supplied us but that supplier also dependent on a third supplier, third supplier dependent on fourth supply. And we do not know any of that most of the time unless we go and investigate. And also there are quality guarantees that are not enforced from your end at the every step between two consecutive suppliers.

So I will give you a very simple example. This is an example I heard from Maurice Hurley. So suppose you are restaurant and you are buying ice cream from supplier B. Supplier B is not manufacturing or producing the ice cream but it is actually supplying from company C's factory. So to your customer, you are responsible for the

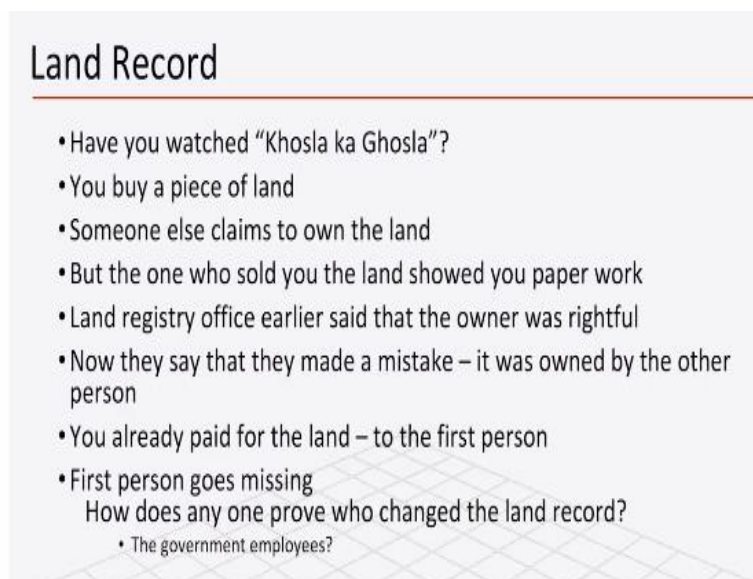
quality of the ice cream, but the ice cream every time you are getting seems to be melted.

So who is responsible? So you can say to supply B that you probably kept the ice cream too long in your truck or your temperature has a problem in your truck. Or you can say supplier C, you made melted ice cream when it was picked up by supplier B, it was already melted. And supplier B says that when it received, the temperature was too high and therefore, this is the problem. So how do you find the truth?

So one possibility is that as a restaurant, you can put temperature sensors on the truck of supplier B as well as in the factory of supplier C where it stores its freshly produced ice cream. And then you get the sensor data from the suppliers directly through wireless network. And then you keep a log and you check the log, you would know whether B or C had a bad temperature and that is why it happened.

But there are certain problems and we will talk about that. We will come by, revisit this problem about the integrity of the data that is coming from the supplier B and supplier C even when you actually put those sensors, and we will see how maybe the blockchain might be a solution. A third problem here is Land Records.

(Refer Slide Time: 20:12)



Land Record

- Have you watched “Khosla ka Ghosla”?
- You buy a piece of land
- Someone else claims to own the land
- But the one who sold you the land showed you paper work
- Land registry office earlier said that the owner was rightful
- Now they say that they made a mistake – it was owned by the other person
- You already paid for the land – to the first person
- First person goes missing

How does any one prove who changed the land record?

- The government employees?

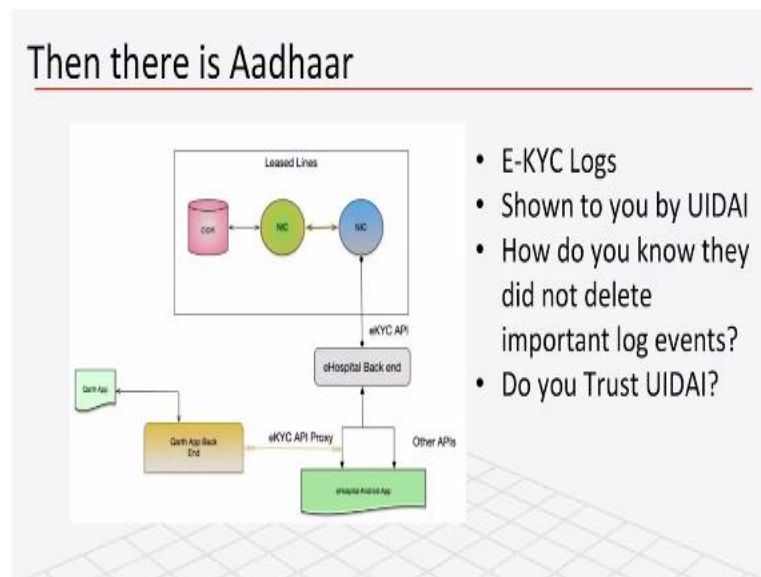
So many of you have watched this movie, “Khosla ka Ghosla” right. So so you buy a piece of land and somebody claimed that he owns the land and showed you some paperwork, and you paid him or her the money and land registry office, you checked

and land registry office said yes, this land belongs to this owner. So you trusted that, and you went ahead and paid. And then this person disappears.

Then a third person comes and says that this land actually is mine. And so sale is not legitimate. So at this point, you go back to the registry and registry says oh, we made a mistake. Actually, some data was missing. And now we know that this person is right. Now you basically have no land even though you paid somebody who is now missing. So somebody might have changed the land record twice.

Once in the name of that other guy and then name of this guy and all the logs for this change of this data has also gone missing, because we are trusting the land registry authority to maintain the integrity of the land record. And also if any access is made for changing any of the land records, maybe the logs has to be protected also but the logs were not protected properly, because it is an insider who has managed to delete relevant entries in the log so it is not clear who accessed the log.

(Refer Slide Time: 21:42)



Also there has been a question about your Aadhaar accesses. So remember that there was a case where people who did the using Aadhaar authentication, they did their KYC, or getting SIM card from Airtel. The Airtel bank also made an same E-KYC to create an account in your name and then all the you know cooking gas subsidy was being now deposited to that bank account.

Now this is actually this was shut down later on this process but we need to know who is accessing our data in the other database for doing E-KYC. So then UIDAI decided that through their website, you can go there and see who accessed your Aadhaar information or who did E-KYC on your this thing. But it did not show the demographic lookup properly but it showed the E-KYC logs. But this logs are now maintained by UIDAI.

And if you trust UIDAI, then you will say okay, these are the only times when somebody did E-KYC on me. But if you if you think that somebody is doing E-KYC and somebody inside the UIDAI might have deleted the logs, there is no way to prove or disprove that. So there is a trust problem that can build up.

So therefore, you know in this case also the tamper proof property of this logs, should be somehow convincing to the customers or to the users so that they can trust that whatever they are getting as log of their E-KYC is indeed the only times when their E-KYC was done. So now we have spoken about four problems. One is your banking transaction logs and their tampering possibility.

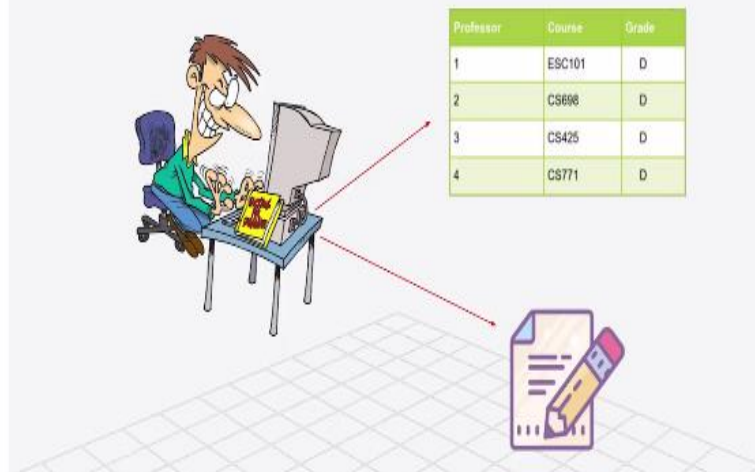
Second we talked about supply chain data and supply chain provenance and their tamper proof property. Third thing we talked about land registry and need for the integrity of that data and maintaining keeping the integrity of the logs of accessing and modifying that data. Fourth thing we are talking about the E-KYC logs maintained by UIDAI.

And in all these cases in the current traditional system, we have to trust a third party or we have to trust the authority who is maintaining the data to actually maintain the integrity of the data. And that may or may not be very prudent to trust. So then finally, the great submission and management system in a university or in an institute, where professors submit grades online, and it goes to a database.

And that database is now you know maintained and then the students when they log in to see their grades or you know print out their grade card, they actually access the database.

(Refer Slide Time: 24:57)

A student Online Grade Submission and Management System



Now between the time professor submits the data and when the student sees the data, between that time if somebody insider actually changes the grade, then there is no way for the professor to know because professor might have 400 students in the class and unless there is an investigation when he might have written records of the thing of the data.

But if nobody has complained and there is no way for the student to know unless the grade change has been very drastic, like somebody is supposed to get an A and got an F. But otherwise, there will be no way to know that the data integrity has been violated. And the person who did this inside might also remove the log of accessing that database and that could be a problem.

And therefore, there is not enough transparency in which the data is maintained without you know leaking out the private information like the grades of students, but there should be transparency of how the data is maintained and some kind of a proof that the integrity of the data has not been tampered with. And then only there will be full trust from the students or from the professors that this system is tamper proof.

And there is no way for somebody to come and change the data from inside or by through some cyber-attack or something like that. So these are the things where blockchain might come handy as a technology to solve this questions that I have raised so far. So people might expect that oh, so this is a course on blockchain. So it

might be about bitcoin and ethereum and we would learn how to actually transact and all that stuff, but that is not the case.

And here is why I would argue that why I do not want a course on bitcoin or currency. However, if you are in the full dynamics of bitcoin and how it works and how you actually make transactions and how you can make you know micro payments and all that with bitcoin, then you can actually go to Coursera. And there is a very nice course by Professor Arvind Narayanan who actually from Princeton, and whose course is about bitcoin only, right? But our course is not on bitcoin.

(Refer Slide Time: 27:27)



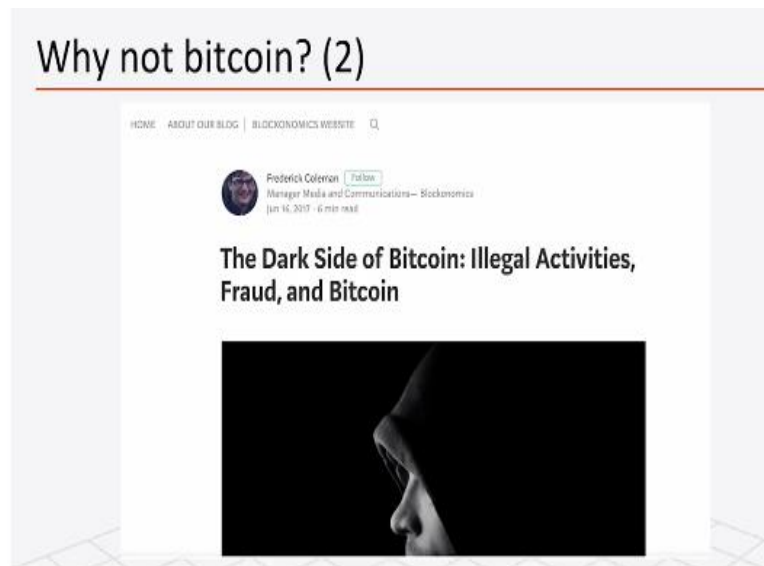
And the reason is that bitcoin is something that has also raised a lot of concern about cryptocurrency. So one of the very early story after the bitcoin came into existence was the history of the Silk Road, Silk Road was in underground market and the underground in the sense that it was being carried out in the dark web. So dark web is basically is the part of the web where people do not have direct access.

Like we go to a website of a news organization or an institute or a business. These are places which are accessible through the web, but they are not accessible directly by common people. You have to know exact address and their location and probably very strong authentication. And many times you cannot even go to them without using some anonymous browsers like Tor, Tor browsers.

And there the people from the underground operations of drug and other things extortions and all that stuff they actually transact in bitcoin and Silk Road was dismantled by FBI around 2013 or so. But they are still a lot of business in the dark web that happens using bitcoin because bitcoin is almost anonymous. There is no way if you ask me to send money to a particular bitcoin address, there is no way to know whose address it is even from the law enforcement agencies.

And therefore, it is very difficult to trace. And this is the same thing that is happening today when there is a ransomware attack. And ransomware attackers encrypt your entire disk by sending a malware through your phishing link or something. And then they actually demand money to unencrypt or decrypt your device by and they want you to pay in bitcoin or ethereum because of the anonymity that they can hide behind. So that is one of the problem of bitcoin.

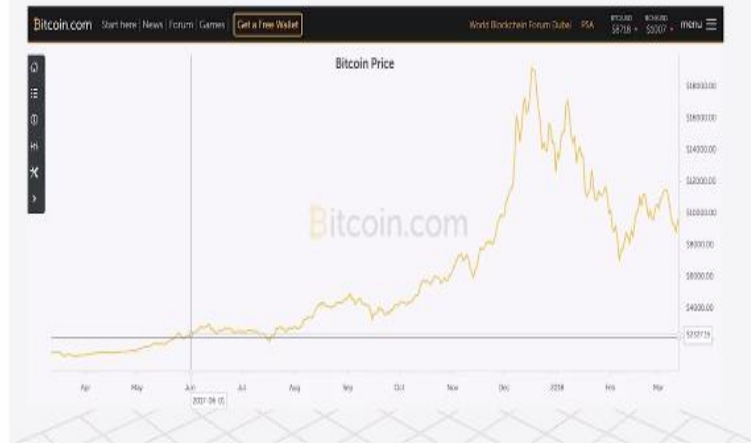
(Refer Slide Time: 29:42)



So illegal activities and all ransomware these are some of the problems. But there are other problems, right?

(Refer Slide Time: 29:50)

Why not bitcoin? (3)



So one of the things you would know that bitcoin prices go up and down, sometimes they went to close to \$20,000 a bitcoin and now I think it is about 12,000. Sometimes it was 5000, sometimes it came down to 8000. So if you think that investing in bitcoin is a good idea, that is not something that I would advocate. If you want to invest and quickly make money in in a couple of days, and you have a lot of money, maybe you can invest in bitcoin.

But otherwise as a long term asset, I do not think the bitcoin is a little too risky unless you have that kind of risk appetite you probably do not want that. The other thing is that the way bitcoin works. So we talked about the consensus mechanism, right? So we have not we will discuss this later in the class how the consensus works. There are many ways to arrive at consensus.

So consensus is when all the parties agree that this transaction indeed took place. And then only it goes to the ledger, right? So this consensus process in bitcoin because of its anonymity and the fact that it is anybody can join the bitcoin network. So therefore, we cannot tell whether people are honest. So therefore, the consensus mechanism has to be very, very cryptographically challenging.

And to solve those cryptographic puzzles, and we will talk about that later in the course. It requires the immense amount of computational power. And when you do that kind of computation for arriving at consensus, and you actually have to arrive at many consensus over a short period of time.

(Refer Slide Time: 31:35)



And therefore the amount of energy that you require to do that kind of computation is enormous and that is very harmful for the environment.

(Refer Slide Time: 31:56)



And we will see that if you look at the statistics that bitcoin mining today, actually process of arriving at a consensus actually is also called a bitcoin mining The reason why it is called mining is because anytime a consensus is arrived, there will be only one winner whose selected data will be actually made permanent into the data store or in the blockchain and they get some reward.

So in the beginning, bitcoin was giving 50 bitcoins as reward. If your data collection becomes permanent, then they halved it to 25 bitcoins and at this moment it is 12.5

bitcoins that you can get, but this is how bitcoins are also created. Therefore, this consensus process in bitcoin is also called bitcoin mining.

And this mining process is so expensive in terms of computation and therefore in terms of power consumption, that it is consuming more electricity than 159 countries, including Ireland, and most countries in Africa. So you can think how wasteful it is to actually mine bitcoins. So and any other cryptocurrency that is also based on participation of public anonymously would have to have a similar kind of consensus process.

And therefore, they will also be wasting a lot of power and that is a big concern for from the environment point of view. Also it becomes very expensive to buy equipments, which are capable of doing such computation. And therefore, it get more tilted towards people who have deep pockets. You and I with our regular laptops or other machines we cannot, you know have the ability to win this process of consensus.

So we cannot make bitcoins whereas there are people who have invested millions of dollars in buying equipments and paying electricity bill and air conditioning bill for their huge compute farms, and therefore they are able to do this. So this makes this entire bitcoin ecosystem very tilted towards those people.

(Refer Slide Time: 34:10)



And the other thing is that most of this bitcoin mining companies, now actually there are companies which actually can only afford such large-scale bitcoin mining and this many of these companies are in China. Now what happens is that it is provable, that if one person or one player in the bitcoin platform has more than 51% of the computational power, then he can actually completely change the data in the bitcoin network.

So earlier we said that in a blockchain, the data that we store after a consensus is tamper proof, right. Nobody can come and change the data. The reason why they cannot do that because to the amount of computation they have to do, in order to tamper it is too much because they have to then undo all the computation that was done to store that data and any other computation that was done to store data subsequent to that.

So this is an total amount of work, computational work that somebody has to do to tamper with. But if I have majority of the computing power in the entire ecosystem, then I can actually completely change the entire chain, chain of data, all the data I want to change and all subsequent data. Now think about this.

If one country has most of these or majority of this companies who are doing bitcoin mining, if they want to get together and then their total computational power becomes above 51%, then bitcoin will have no integrity of its transactions. And therefore the entire ecosystem will fail.

Also because of this environmental concerns and volatility of the cryptocurrency and so on, we may be the country in which all these companies are there and they are consuming power, they are polluting the environment, the country might decide that they will curtail the activities of this companies and therefore, there will be another kind of problem. And when this kind of news has come, you will see the bitcoin prices fall.

The reason is, even though it may be a speculative news, because we are now dependent on all these different extraneous things which are not imagined by the originator of the bitcoin and originator of the bitcoin was an anonymous person who

used the name, Satoshi Nakamoto. And in 2009, he wrote the first you know version of the bitcoin and he launched it and he also wrote a white paper.

And his idea was to get rid of the tyranny of the large banks, right. So in 2008, there was a international financial meltdown and it turned out that the banks did a lot of things which are not properly you know correct things to do. And in fact, from the writing and from the original message that was in the first block of the bitcoin blockchain, it seems like he was actually trying to emancipate people from the, from the hold of the banks.

And then they want the entire world everybody to become part of a currency system, which is not dependent on a central bank or on the banks to actually decide the, you know the value of the money. But unfortunately, the way it worked out and way it unfolded is that only a handful of companies are now doing most of the bitcoin mining.

And then the all the transactions that are happening are also by only a you know only 1, 2% of the people who are involved in the bitcoin ecosystem. And the same thing is happening in ethereum that 90% of the transactions are done by maybe hundred players when there are about 6 million players in the ecosystem.

So you can see that there is a huge amount of inequality that is building up in the cryptocurrency system when there are only handful of players who are doing all the activities, all the transactions storing all the currencies, and the rest of the other people are doing very little. And therefore, the entire dream of Satoshi Nakamoto whoever he is, is not being translated to reality. So that is another problem.

And as you know that in India, the RBI has put a blanket ban on bitcoin as a transaction medium and or any kind of cryptocurrency and there is a good reason for that, and we will not get into that, but that is how it is. So then there is another problem. That this problem has been happening because of various reasons.

(Refer Slide Time: 39:18)

Why no money business?



So that so common people so bitcoin if you want to directly play into the bitcoin ecosystem, do mining, do transactions, you have to be computationally savvy, right you have to know how to create a private key, how to create a public key, how to tell other people that this is my public key which basically get shortened to your wallet address.

And then you have to store your private key very securely in order to so that nobody knows your private key. Because once they know your private key, the money is no longer yours because they can use your private key to spend the money or transferr the money to another account. So this cryptography, the public key, private key is very important for operating in the, in the bitcoin or ethereum economic.

Now common people, businessmen, they might not be computationally savvy so they have another way of investing in the bitcoin or ethereum or any kind of cryptocurrency is by going to an exchange cryptocurrency exchange and say that I am giving this kind of money and give me this worth of cryptocurrency. Now what this company will do is give you some kind of a paper or some kind of a link that says that you now own so many bitcoins because you give me this amount of real money.

And then all the private key and everything will be stored at the exchange. So there is a there are two kinds of wallets like hot wallet and cold wallet, and most of the keys that are not very frequently used are put into the cold wallet and the hot wallets are the ones that are being used very commonly.

Now this happened in one of the exchange Mt. Gox where there suddenly the exchange owners, they said that there is a so many millions of worth of cryptocurrency has been transferred to somebody else's account and as I said that once it is transferred to an account, the account number is actually a public key in a hash form, and therefore no way to know who is behind it.

So the police or anybody cannot really find the person whose wallet has got that money. So therefore, the owner said that, you know the private keys were stolen, and therefore this happened. People suspected that the stealing person is one of the exchange owners only. And since the actual people who purchased bitcoins from this exchange did not keep their own keys, the keys were in the cold wallet of this or cold vault of this exchange.

So therefore, they have no recourse, then they could not get the money. And this was a huge loss for a lot of people. More recently, there was another case.

(Refer Slide Time: 42:24)



So this is the Quadrige is another such exchange. And in that exchange, what happened is that the person who owned the exchange also had the in his cold wallet, a lot of keys \$145 million worth of cryptocurrencies keys he had and then he died. And with him the password or code for accessing that wallet, you know went away and nobody there was no backup.

Nobody else knew that code, and therefore \$145 million worth of cryptocurrency was lost and the losers were people who actually bought them. And now recently the news is that they are exhuming his body to figure out if he actually made a disappearing act by killing somebody else like so they want to check whether this person who is buried as him is really him. So this is this has come to that.

So this is the other issue about cryptocurrency is that if you are not tech savvy and you are not doing it yourself, you are dependent on this exchanges and all this happenings can happen to you and you may lose a lot of money.

(Refer Slide Time: 43:36)



The other thing that is also happens is that there are bugs in the code of the blockchain ecosystem, or in case of ethereum the bug was in the smart contracts. So smart contracts are programs that work on your behalf, from your address, from your account and do transactions and other things. And so in this case, there was a bug reentrancy bug.

And therefore, attackers could actually make transfer from all of this smart contracts from various people's accounts \$30 million worth of ether to their accounts. Fortunately, some of the good hackers, they realize this is happening. So they actually also use the same bug to actually siphon off rest of the money of the rest of the accounts to their address and later on they paid it back to the rightful owners.

But the \$30 million worth of ethereum, ether that was lost was lost to the hackers. So these are the kind of things that are concerning about cryptocurrency.

(Refer Slide Time: 44:47)

Bitcoins and other cryptocurrencies

- Too much interest by investors to park their assets
- Less use as a medium of value exchange
- Private Key stealing or private keys at exchanges — risk
- Coding vulnerabilities — risk
- Volatility
- Energy Waste — climate impact
- Too much concentration in one country — risk
- Regulatory risk
- Usage for criminal activities — Silk Road

So in summary, I would say that, let us admit that bitcoin first brought to us the technology of blockchains. So it was a very good thing that happened. The Satoshi Nakamoto actually he understood how to create an ecosystem in which there is replication, distributivity, consensus mechanism, all this technology and algorithms that already existed in the distributed system literature.

He actually brought them together and also brought together the some already existing concepts of digital cash and the idea of what we call no double spending and all that thing together, he brought them together and created bitcoin. So we are kind of like happy to have the technology with us, but bitcoin as such or if you consider ethereum and other cryptocurrencies, we have seen in the last 10 years or so there is too much interest by investors to park their assets there.

And if that happens, then the whole idea of a currency, what is a currency, currency is something through which you exchange value, right? Now if you just park it somewhere then it is not being used as a currency. It is been being used as a storage medium of value. And so that is one problem. So it is not being used so much as medium of value exchange.

The private key stealing and private keys at exchanges is putting people to enormous risk of losing large amounts of money. There are vulnerabilities in the coding of the smart contracts and other parts of the code, which poses risk of losing money. There is also market volatility based on various news as I was mentioning, and therefore there are lots of possibilities of losing money. There is a lot of energy wastage.

We talked about that climate impact and too much concentration in one country, which is also a problem. And then there is regulatory risk because regulators of different countries are framing their rules for allowing or disallowing cryptocurrency or regulating them. And also criminal activities use bitcoin. So all this together basically makes us not to focus on bitcoin or cryptocurrency in this course.

Even then we will talk quite a bit about the bitcoin and ethereum because of learning from them the technological underpinning, which is very useful and very worthy to understand. So we will talk about bitcoin, how it works, how the consensus works there. And also we will talk about ethereum and smart contracts and all that. But we will not focus on this application of blockchain and cryptocurrency.

We will focus on application of blockchain for non cryptocurrency usage in this course.

(Refer Slide Time: 47:49)

Again, What is a blockchain?

- Blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activities and therefore cybersecurity concerns as a whole.
- Attractive properties of Blockchain
 - Log of data with digital signature
 - Immutable (once written – cryptographically hard to remove from the log)
 - Cryptographically secure – privacy preserving
 - Provides a basis for trusted computing on top of which applications can be built

So then, coming back to blockchain, now let us say blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activities

and therefore cyber security concerns as a whole. So trusted computing is a concept that when you do computing and if you depend on the results of the computing and by computing we not only mean number crunching, we also mean the entire ecosystem.

The exchange of information over the network, the storage, the databases, all these things are we are clubbing together as computing. But when you do computing and your system depends like E-governance system or your identity system or your grade management system or your property registration system, that dependent on a whole computing ecosystem.

So but then if you are depending on the computing ecosystem, there are many different possibilities by which data in that ecosystem can be impacted and tampered with and be it while it is transiting through the network, be it while it is in storage, be it while it is being computed. So therefore, we have to worry about trusted computing when you can trust the computing environment to produce result.

Keep the integrity of the result and give me transparency of how it is processing the data, how it is storing the data and how it is protecting the data against various kinds of attacks and that is what blockchain can give you. And the attractive properties of blockchain for this purpose is that it gives you a tamper proof log of data with authentication which means that the data also is signed by whoever created that data and then it is immutable or almost immutable.

So which means that once written, it is cryptographically very computationally hard to remove that log or to tamper with the log. And if you want the transparency but not reveal the private information, you can do that in blockchain. So it is it can you can make it privacy preserving. And it provides a basis for trusted computing on top of which applications can be built.

(Refer Slide Time: 50:22)

Trust Model

- Cyber Security is all about who you trust?
 - Trust your hardware to not leak your cryptographic keys?
 - Trust your O/S to not peek into your computation memory?
 - Trust your hypervisor to not mess up your process memory?
 - Trust your application to not be control hijacked or attack other applications?
- Where is your trust anchor?
 - Hardware?
 - Operating system?
 - Application?
 - Manufacturer?

So let us talk a little bit about when we said trust, what do you mean by trust? So trust model that you assume in case of computing environment, we have to consider what are the trust is kind of like opposite of your attack model. Like who can attack or how threat model like what are the threats to the integrity and privacy and availability of the information? So first of all, you can put your trust on the hardware and say that hardware will not leak your cryptographic key.

But is that true and it is not necessarily true because there is something called side channel attacks. So which people have shown that they can actually get your cryptographic key while you are doing encryption or you are doing decryption, they can look at the power that you are drawing from the your power you know source or they can look at the electromagnetic signature or they can look at the timing and all kinds of things by which they have shown that they can reveal your cryptographic key.

So unless your hardware is in a proof to that kind of manipulation, your hardware may not be trustworthy. So nowadays there is a lot of work on how to make a hardware trustworthy by using enclaves and other kinds of mechanisms and even there we have people have shown their ways to subvert the protections that the hardware companies come up with. You must have heard of Intel's meltdown and Spectre bugs that came out two years ago.

So you may or may not be able to trust the hardware. So in that case, if you do not trust your hardware, you have to make sure that you do the protection against any kind of key leaking and all that stuff at the next layer which is the operating system layer or firmware layer. And there the question is, now operating system is basically create processes and they have memory in which the computational results and stuff are temporarily kept.

And this memory is also hierarchical. So which means that some of part of the memory addresses sometimes come to the caches, and all that stuff happens. So therefore, the question is, are there ways in which people can peek into your cache or peek into your memory and then look, get your private information, your private key and all that stuff? So that has that is another question of trust.

Now if you you are using virtual machines, then you have to know whether your hypervisor leaks information, they can peek into your process memory and all that stuff. And then your applications may be also have bugs and there may be cyber-attack. And while the application is using some of your data, it may actually tamper with that or it may actually reveal private keys and all that stuff if your application is using your private key without any protection.

So the question is, what is your trust anchor? Right is it in the hardware? Or is it in the operating system? Is it in the application or you trust a manufacturer like Intel or others to actually give you a trusted platform?

(Refer Slide Time: 53:43)

Trust Model (2)

- In many real life transactional activities – trust model is the inverse of the threat model
 - Do you trust your bank to not take out small amounts from your balance all the time? (Watch – “Office Space”)
 - Do you trust the department of land records to keep your record's integrity?
 - Do you trust UIDAI officials to keep your aadhaar data from unauthorized access?
 - Do you trust your local system admins to not go around your back and change settings, leak passwords, change database entries, and remove their action from system logs?
 - In the patch management system of your enterprise, are the patches being put -- all have digital certificates? Who put them? Do you trust your employees to do the correct thing and not put a malware as patch?

The but in case of the applications like E-governance and you know grade management system or whatever, the question is, do you trust the bank that they are not taking away small amounts from your balance all the time? There is a movie called Office Space that was taking only a you know fraction of a cent from every transaction, and very soon they accumulated millions?

Do you trust the land record department to keep the integrity of the land records? Do you trust the UIDAI officials to keep your other data access logs you know integrity of that? Do you trust your local system administrators to not to go around your back and change your data or read your data and then delete all that information from the system log.

If you have a patch management system in your enterprise, how do you know that the patches are being made, or somebody is doing an unauthorized patch to attack your system and things like that. So that is those are the problems that you have to worry about. So far, we have spoken about the trust model and corresponding threat model which are kind of inverse of each other.

(Refer Slide Time: 54:55)

Digital Currency ideas

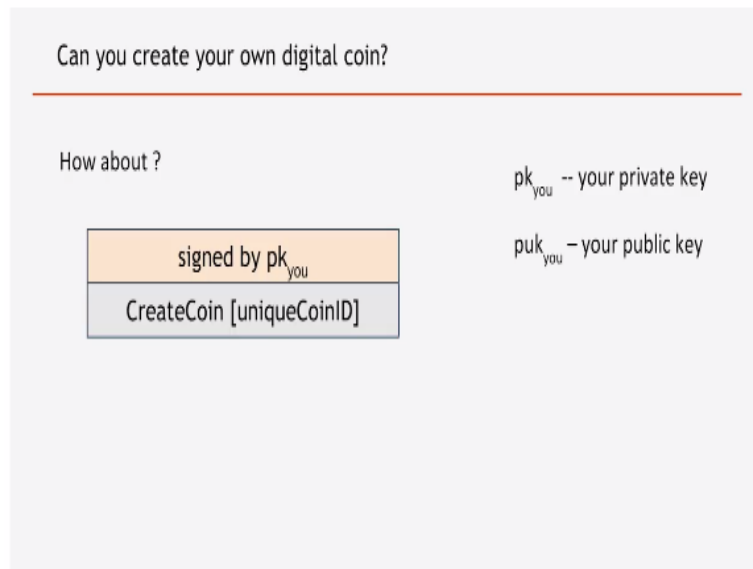
Now let us look at some of the cases that we talked about before in detail in light of what we have discussed since then.

(Refer Slide Time: 55:05)



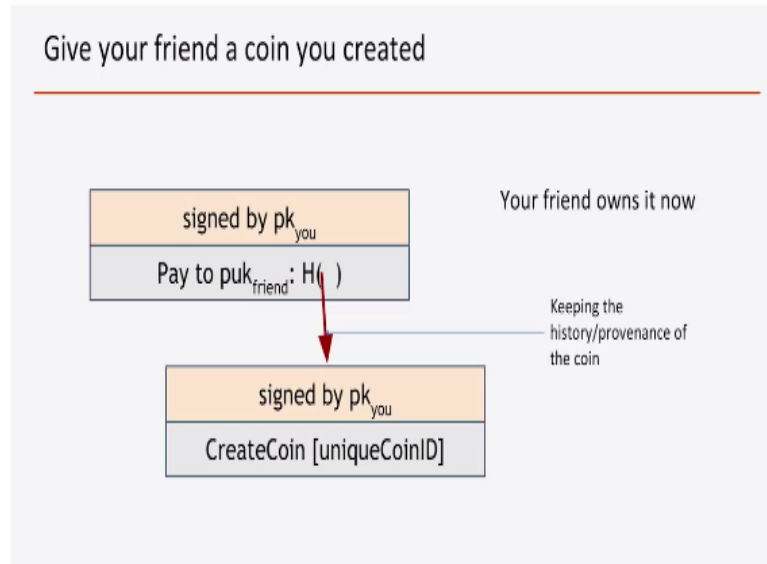
So let us first look at how one can create a digital coin. And this is Arvind Narayanan's crypto coin version 1.

(Refer Slide Time: 55:15)



So what you can do, you can say that I am going to be your mint, and I am going to create a digital coin. And then I will give it a coin ID. And then I will have a public key and private key and I will sign the coin with my private key. Okay, so anybody who has my public key because public keys are usually known to everybody else, so he can check that it is my signature and once it has my signature it is a valid coin.

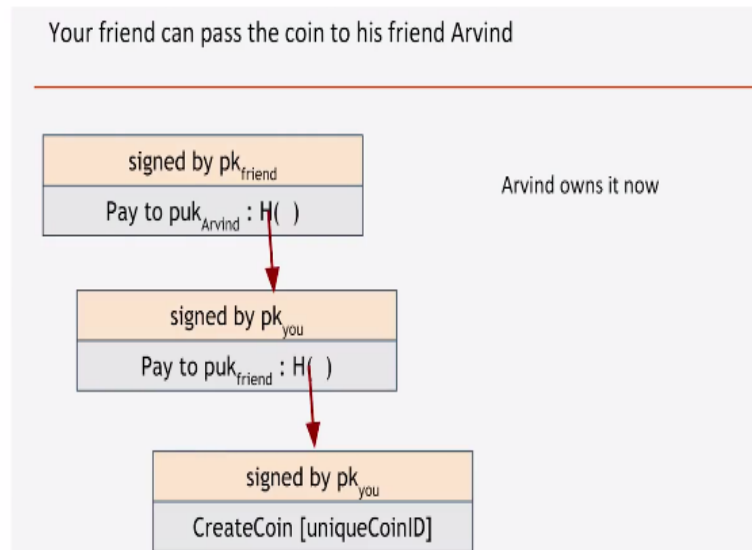
(Refer Slide Time: 55:50)



So then, so I can then give the coin to somebody else. Maybe in exchange of some value, you know in the real world. Like I buy a book from him. And then I give it to a friend. So how do I give it to a friend? The friend creates an public and private key. And I give the friend I say that pay to his public key address this coin, and I sign it with my private key. So anybody can check whether I signed it by using my public key. And I also in order to keep the history of how this coin was created, and who

gave it to whom I created a link to the previous information that the coin was created by me. So this red link that you are seeing here is actually that link that is keeping that history along.

(Refer Slide Time: 56:43)

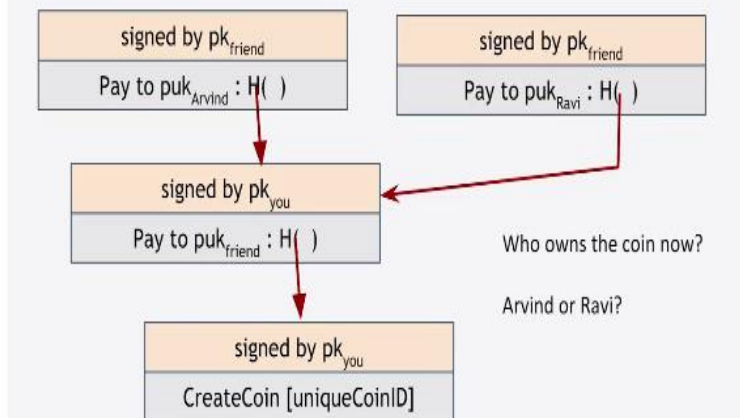


Now since I have now the coin I earned it by giving you a book or something selling your book. So now I want to give it to Arvind who now gives me something like maybe another book. So I want to give the money to Arvind. So I say that pay to Arvind's public address, public key and then I sign it, right. And I am the friend. So I sign it. And then I keep a link to the previous to previous link to information, pieces of information.

So if anybody wants to check where this coin came from, then he has to basically go down the links and see where the coin was created, who got it first and who got it second, and so on. So this is way so every time I pass the coin, all this information is also passed about the coins history. So Arvind now owns the coin.

(Refer Slide Time: 57:35)

double-spending attack



But if I am dishonest, what I can do, since this is digital, so I have no problem to pass it on to multiple people. So I actually give a copy to Ravi, another friend for another thing that I get from him and do the same linking and all that. Now the question is I had only one coin. Now I gave it to two people.

Now these two people will have to you know both have the same coin that is not possible right because if you have a real world coin, then you could not have given to two people since you are digital you are cutting and pasting. So you can actually give it to two people. And this is what is called a double spending. So I have done a double spending, which cannot be done in a real money monetary system.

Because then, you know if I can do double spending, I can do triple spending, and then the value I got from this one coin is twice the real value, right? Because I got something from Arvind I got something from Ravi, but I am just giving them the same thing. And they also when they try to use it, they will it will be a problem. So this is called a double spending or since it is actually an attack, call it a double spending attack.

(Refer Slide Time: 58:56)

Major challenge in Digital Currency Design

How do you stop double-spending?

So major challenge has always been in the digital currency. From 80's people have been trying to solve this problem of creating digital money and this all this people have come to this problem that how do you stop double spending. And if you can do double spending, you can do triple, quadruple all kind of spending.

(Refer Slide Time: 59:18)

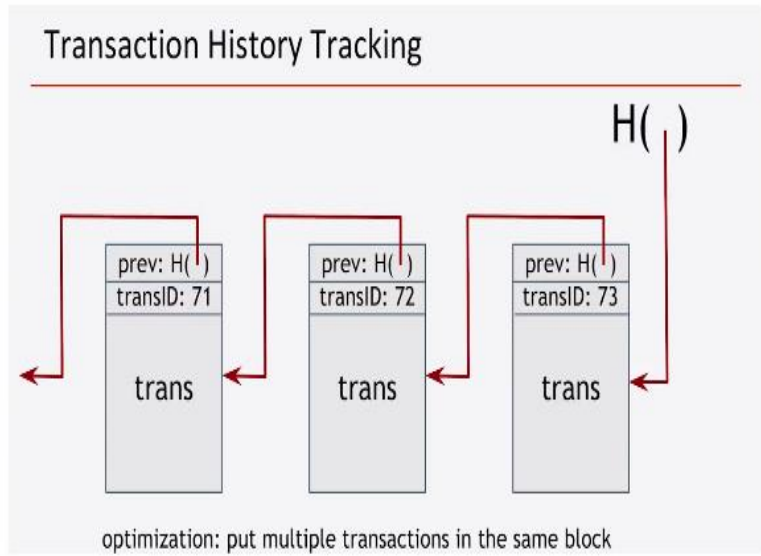
Arvind Narayanan's CryptoCoin-version 2

Double Spending Proof Digital Currency

CryptoCoin-v.2

So we have to do something more than what we just showed you in the version 1. So version 2 is how we can make a double spending proof digital currency.

(Refer Slide Time: 59:37)



So what we, what Arvind did is that saying that we will create a history of all the transactions. So earlier when we were giving the coin to somebody, we were not giving any number to it, right. So we were just connecting them through this links. Now we say that we will have various transactions and each transaction will basically spend one coin, but we need to know where that coin came from, from which transaction.

So we have to go and see the next transaction and finally, there will be a transaction when the coin was created, right. So this history has to be kept.

(Refer Slide Time: 1:00:17)

CreateCoins transaction creates new coins

transID: 73		type: CreateCoins
coins created		
<i>num</i>	<i>value</i>	<i>recipient</i>
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...

Who keeps track the transaction History?

Who Arbitrates when a double spending is tried?

Which of the transactions is valid?

← coinID 73(0)

← coinID 73(1)

← coinID 73(2)

And this history now the data structure in which you keep the history and all that stuff is a matter of details like, but the main question is, who keeps track of the transaction

history? Like who tells me that somebody is trying to do a double spending. And then if I have done a double spending to give the coin to two people, who decides who actually gets the money and who is the one who is not going to get the money.

And so which means that somebody has to tell me which one is a valid transaction, which one is not a valid transaction.

(Refer Slide Time: 1:00:54)

PayCoins transaction consumes (and destroys) some coins, and creates new coins of the same total value

consumed coinIDs: 68(1), 42(0), 72(3)		
coins created		
<i>num</i>	<i>value</i>	<i>recipient</i>
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...
signatures		

Valid if:

- consumed coins valid,
- not already consumed,
- total value out = total value in, and
- signed by owners of all consumed coins

So concept of validity here would be that the coin that has been used in the transaction is a valid transaction. Also, it is not already consumed, and the total value out of this transaction should be total value in. So if I have multiple coins from multiple sources, I can use that in one transaction because not everything has the value of one coin. So I can get three different coins to buy a thing worth of three coins.

But then the total value in and value out should be the same. And then it should be signed by the owners of all the consumed coins, right. So this is the matter of validity. So that history that you saw, has to be of valid transactions, right? So somebody has to check the validity of the transaction and somebody has to use the history to tell me whether double spending is being done.

(Refer Slide Time: 1:01:45)

Immutable coins

Coins can't be transferred, subdivided, or combined.

But: you can get the same effect as subdivision by using transactions

- create new transactions

- consume your coin

- pay out two new coins to yourself

So now how do you actually maintain the coins? Whether you make the coins immutable and all this is a detail so we will not worry about it at this point.

(Refer Slide Time: 1:01:56)

Trusted Third Party

Crucial question:

You become the central Trusted Party keeping track of transaction history, arbitrating validity of transactions

Why should people trust you??

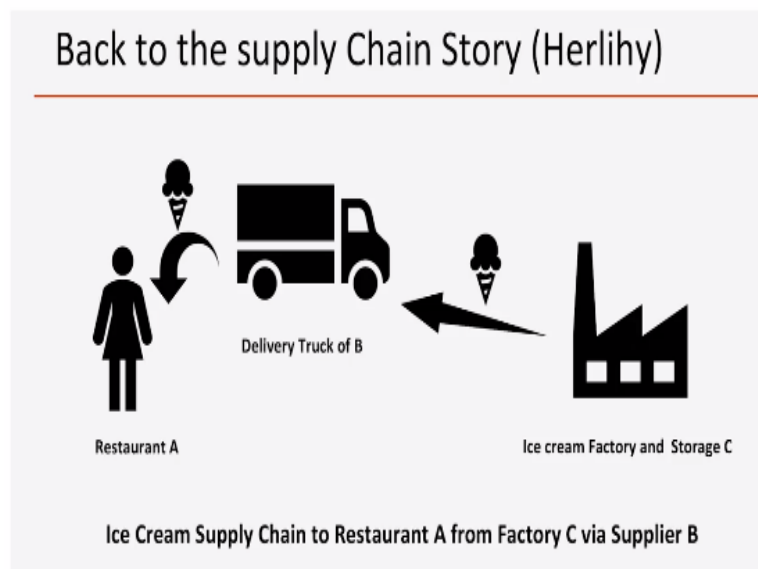
So the crucial question is who maintains the history and who validates the transactions, and who tells me that this is invalid because there is a double spending. So one possible solution, of course, is having a trusted third party, right. So and once you have trusted third party, we are back to the same conventional problem that I have a trusted third party.

He maintains the ledger of transactions and he checks consults the ledger every time and coin is trying to be used in a transaction to ensure that this is a valid transaction. And but the question is, should we trust the trusted third party. The trusted third party

might be a biased entity, and they might actually always arbitrate in favor of some people and arbitrate against some people.

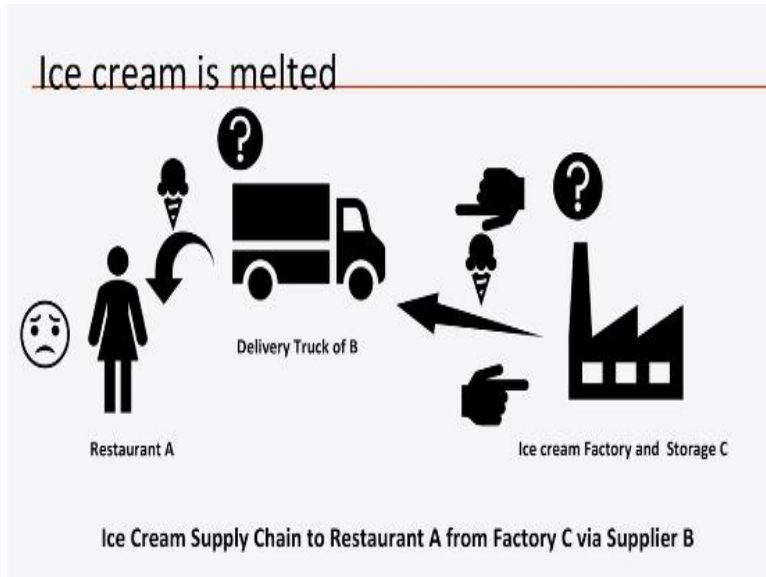
So it defeats the purpose of a distributed consensus mechanism and all that and that is where the blockchain based solution comes into play. So trusted third party is not our preferable solution because that solution already exist and being used today. But we want to remove the trusted third party and create a trust system in which we can transact trusting the system, not trusting a single entity. So that is the about that cryptocurrency issue.

(Refer Slide Time: 1:03:27)



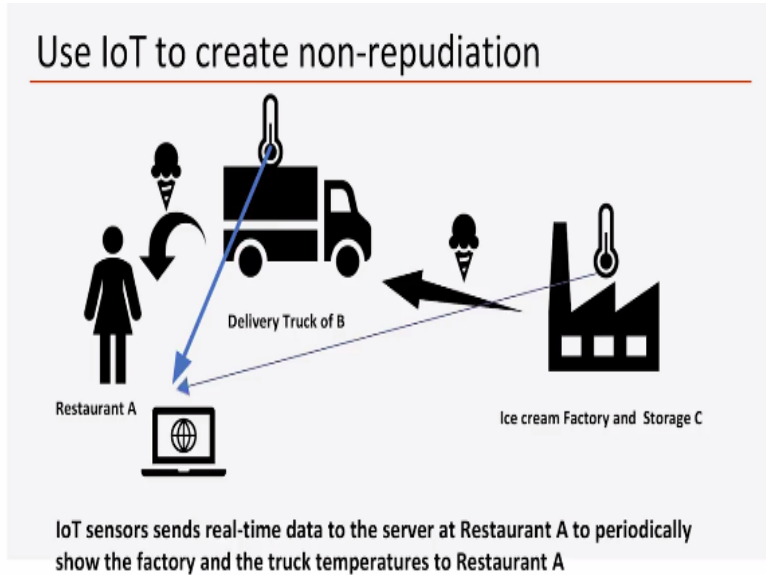
Now back to the supply chain story, right? So you have the Ice Cream Factory, you have the delivery truck, and you have the restaurant. And this question was that who is melting the ice cream, whether it is the factory when it supplies it to the truck, or the truck is actually keeping it at a very high temperature and the ice cream is melting.

(Refer Slide Time: 1:03:46)



So let us see what solutions, so the question is here is about, you know supply chain integrity. And when I get melted ice cream, I asked questions to both of them and both of them point fingers at each other.

(Refer Slide Time: 1:04:02)



So as I said earlier that I could put an IoT or Internet of Things type of sensor in each of these places in the factory and in the, in the truck. And I can say that send me your temperature every second or every 30 seconds. And I will keep track of your temperature where you store and I will actually decide who is responsible for this.

(Refer Slide Time: 1:04:34)

What can go wrong?

- IoT sensor data may be intercepted by a middle man and changed before it reaches the server (**data integrity**)
- IoT sensors may be stopped and old readings may be replayed (**replay attack**)
- What the server gets purportedly from factory C, may be manufactured by supplier B (**Authenticity**)
- If restaurant A claims that C's temperature reading shows that ice cream was melting in the storage, C can say that message you received is not from me – there was an MITM attack (**repudiation**)

- So restaurant A will not be able to pinpoint any one in the supply chain with full confidence!!

However, there are multiple problems that can occur. So let us talk about what can go wrong. First of all, if you do nothing other than just make these IoT devices send information, then the information is not encrypted and digitally signed, then somebody can do a man in the middle attack. So they can actually intercept the message, change it.

So maybe the company B will try to do that to make company C look bad by intercepting the temperature coming from company C and then replace it by a higher temperature. So data integrity could be a problem. And other thing is that if your temperature keeps going up because cooling system fail, you might fool the restaurant by doing a replay attack.

Which means you record the whole temperatures and then you replay it and send it repeatedly to the restaurant and the restaurant will think that your temperatures are fine. So that is a replay attack. Again data integrity issue. Then if the temperature that is coming from factory C is actually being manufactured by supplier B by replacing or jamming the signals from the factory C and pretending to be factory C and send the restaurant the bad information.

So there is an authenticity problem, right. When the data comes to a trust that this data is actually from factory C and not by sent by somebody else. And then if something like this happens or not happens if factory C claims that this is what happened his

temperature was fine, but the temperature you are seeing is actually somebody else did an attack and man in the middle attack and sent wrong temperature information.

And there is so he is repudiating what information has come from his supposedly from a sensor and that repudiation, so non repudiation is not a property. So restaurant A is again at a loss even though he spent money putting sensors with communication capabilities, but he is not happy because he cannot decide what happened.

(Refer Slide Time: 1:06:47)

What can be done?

- Use a message integrity proof (**Hashing**)
- Use digital signature of the individual IoT devices (**Authenticity and non-repudiation**)
 - assuming the digital signatures cannot be forged
 - private keys are kept safe
- Use authentic time stamping with the IoT data before hashing for integrity (**avoid replay attacks**)
- So now factory A can pinpoint with some basic security assumptions about this infrastructure

This can be solved without any blockchain issue, right. You can use message integrity proof by hashing or message authentication code. You can use digital signature for all IoT devices and then you have the authenticity and non-repudiation. You can use time stamping to stop replay attacks. And now factory A can get all the data with authentication with privacy and with integrity, everything, fine, right.

(Refer Slide Time: 1:07:20)

Concurrency Issue

- A has other suppliers for other goods required for its business (multiple concurrent supply chains)
- B and C has multiple other consumers of their services
- So if there are N suppliers who are also consumers of some of these entities, we have an N^2 messaging problem

A offers that every one can look up their data from my server, so you can get linear number of messaging

But do you trust A as purveyors of your data?

But the problem does not end here because supply chain problem has a concurrency problem. Because A is not the only consumer from supplier B or supplier C. Supplier B, C have other consumers. Similarly, restaurant A has other supply chains, right. So it gets meat from somewhere, it gets vegetables from somewhere. So there are many parties involved and if you want to check supply chain provenance for all your supply chains, then you have a n square problem.

Because every party should be able to send information to everybody else whatever the sensor readings are and the sensor could be temperature, it could be about the pH level, it could be about various things. And therefore, it is a huge amount of crisscross information. And that needs to be addressed because it is not going to scale. So restaurant A may say, okay, I have a very good nice data center.

So I will keep everybody's information. So you just only have to send to me and then I will give a nice interface to the information I collect. And everybody else, every other restaurant and every other supplier can log in to it and look at the information and make themselves happy, right. But then why would you trust A to be the purveyor of your data. What if A wants to make some other entity look bad and tampered the data.

So when you when that entity, another entity looks up the data for that entity sensors, you might see wrong information, right? So you cannot trust a single entity to do all the job because then it becomes a trusted third party again.

(Refer Slide Time: 1:09:02)

Solutions?

- Have a trusted authority or a cloud provider to become a publish-subscribe service provider
- Every supplier sends their IoT data with message integrity, authentication code etc., to the cloud server
 - Every consumer subscribes to the events they are interested in on the cloud
 - Every supplier becomes authenticated data generator on the cloud

What if the cloud provider cannot be trusted?

So you can use a cloud provider and say instead of A, B, or C or anybody, the cloud provider collects all the information and most IoT vendors now is giving a solution based on this cloud based data collection, and then interface to the cloud to look at the browse the data and do analytics on the data. But what if the cloud provider cannot be trusted? That is a possibility. Right? Because again, a trusted third party.

(Refer Slide Time: 1:09:31)

Create a framework on which data is crowd sourced, validated by the crowd for the crowd?

- You get a block chain
- But now the question is as concurrent messages come in to this framework, how do you order them?

DISTRIBUTED CONSENSUS IS REQUIRED TO DECIDE

1. of all messages coming in concurrently how are they ordered
2. But if some of the crowd are malicious, and tries to allow data that are wrong, or ordered wrong?
3. You need Byzantine fault-tolerant consensus


So then, the question is, you can use blockchain because blockchain is not a trusted third party. Blockchain is create trust computationally by using a distributed consensus mechanism. So all the information that comes to the blockchain is seen by all the players in the blockchain and all the players have to somehow agree that the information is correct. And once the information put there, nobody should be able to tamper with it. Right?

So blockchain is actually a framework that can be actually a very good use in this supply chain case that we just described. So we will see later that various kinds of blockchain solutions to this kind of problems, not necessarily will take this problem, because this problem is probably a too simple a problem to discuss later.

But you get the idea that here, important part is that even with all the cryptographic measures like digital signatures, and you know encryption and message authentication code, you still have a scalability problem and concurrency problem that needs to be solved. And the one simple solution would be to have a trusted third party to collect all the data and keep it.

But trusted third party is not something we want because it again brings us back to the old traditional mechanism where you have to somehow put your trust on a trusted third party. Instead, if you can create a computational platform in which trust is by virtue of the computational process, then it is much better solution and more fair solution. So that is what we would like to do. So we are at the end of our first lecture.

(Refer Slide Time: 1:11:20)



Conclusion of the First Lecture

- Blockchain is about
 - Distributed Record Keeping
 - Trust Model varies – but usually single point of trust is not good
 - Based on Trust Model –
 - Permissioned Blockchain
 - Non-permissioned or public block chain
 - Also, private blockchain
 - Data integrity (No one has tampered with the data after its creation)
 - Authenticated Transactions or event logging
 - Strong Cryptographic Application
- Blockchain is certainly not ONLY
 - Cryptocurrency
 - In this course, cryptocurrency will be avoided

So in the first lecture, what we learnt is that blockchain is about distributed record keeping. Trust model varies, but having a single point of trust is never good. And based on the trust model, you may have to use blockchain. But depending on who you trust and how much you trust, you have multiple different types of blockchain. So we

will see permission blockchain non permission or public blockchain and also private blockchain.

So these are the some of the different alternatives and based on how much you trust which party and how much you know about the players who will be actually participating in the consensus process, in the validation of the data process, then you have to choose the different types of blockchain and we try to learn how those things are done, or what are the different considerations that go into choosing these kind of alternatives.

Data integrity, we talked a lot about. No one tampered with the data, after its creation is very important. And that is where blockchain comes into play and authenticated transactions and event logging is something very important if you want to know not necessarily the data itself, but meta data, that is the data about who access the data and who modified the data, who added the data, that kind of information.

And strong cryptographic applications. Blockchain is a strong use of cryptography. And blockchain is not certainly only about cryptocurrency and in this course, we will not be focusing on cryptocurrency. But we will talk about some of the technology of bitcoin and ethereum and all that, because we need to understand the underlying technology.

(Refer Slide Time: 1:13:14)

Summary of Lecture 1

- What did you learn today?
 - The need to learn about block chain technology and its applications
 - Bitcoin and Cryptocurrencies are only an example application of the technology
 - This course is not about Bitcoin or Cryptocurrency – but more on the technology and applications
 - Trust Model determines whether you need blockchain and if so – what kind – permissioned/permissionless/private
 - Basic issues leading to the Bitcoin (Trust model again)
 - Basic issues in supply chain provenance and integrity and trust model
 - Concurrency is important to take into account
 - Fault-tolerant Consensus is a requirement for handling concurrency and trust model issues

So summary of lecture 1. So what did you learn? The need to learn about blockchain technology and applications is what we emphasized on today because of the various applications we talked about. Bitcoin and cryptocurrency are only examples of this technology. But these technologies have much broader usage and much more potential. Trust model depends determines what kind of blockchain you are going to use or if you at all need block, will blockchain solve your problem?

Because that is something also one has to take away from this course because many times we I get request that can you help us to do blockchain for our application. And when you actually investigate closely, their trust assumptions and their operating environment and you find that under their trust assumptions and everything blockchain is not required or it will be an overkill right.

So you have to also get the have to have the critical understanding of when blockchain can be of help and have value. And also what kind of blockchain is good for that particular application. Basic issues that led to the creation of bitcoin about the not trusting the banks and the or a trusted third party or a central authority and supply chain provenance and integrity and trust model concurrency issues that arise when there are many players.

And maybe in that case, central data collector like a cloud may be or maybe not a good solution. And fault tolerant consensus is required in working of the blockchain consensus mechanism and workout the trust model issues. So this is the introduction that we have gone through today. In the next lecture, we will talk about some basics of cryptography because you will you already heard a lot about private key public key and hashing and message authentication code in today's talk.

And many of you know what they are, many of you do not. So in the next lecture we will actually familiarize you with all those terms and what they mean and how they are calculated. So that will be, then the introduction to this course, will be complete once we have lecture 2 on crypto concepts. Thank you.