Introduction to Blockchain Technology & Applications

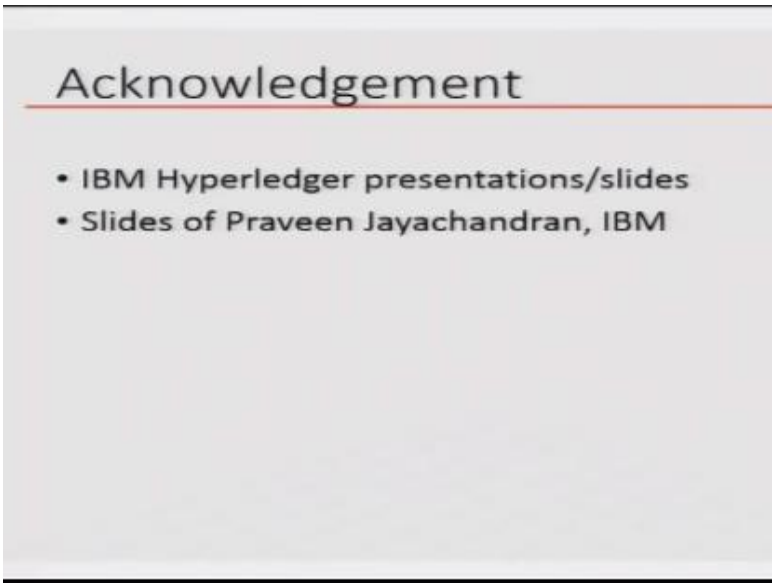
Prof. Sandeep Shukla
Department of Computer Science and Engineering
Indian Institute of Technology-Kanpur

Lecture - 19

Welcome to another session of blockchain technology and applications on NPTEL. So far we have been talking about the permissionless blockchain, which are mostly cryptocurrency blockchains. So what we are going to start in this session is the first case of a permissionless blockchain and this is one of the most used permissionless blockchain in the industry right now.

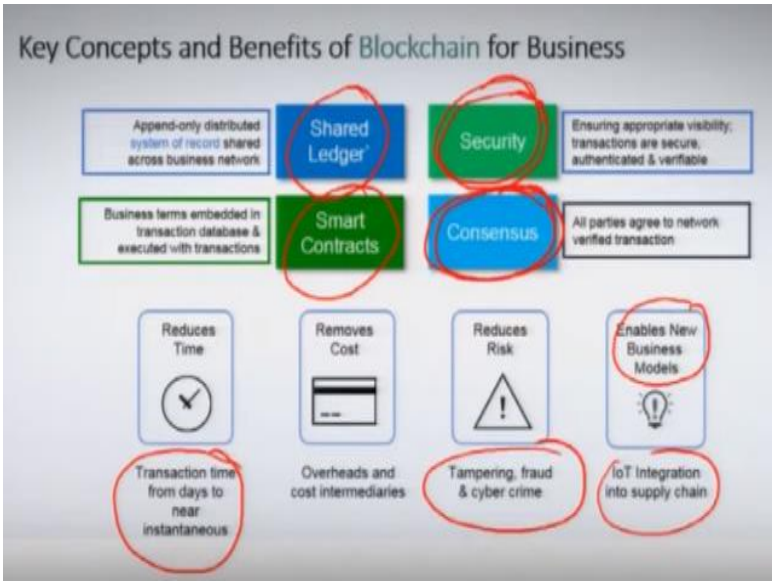
So this is the Hyperledger, which is actually propounded by the Linux Foundation. And in this session particularly we will actually go very superficially over the idea of Hyperledger what it is and what is the reason why it is so different from the bitcoin Ethereum type of blockchains. And then, in our next session, what we will do is that will actually go into more nitty gritty details of the Hperledger.

(Refer Slide Time: 01:18)



So a lot of the material in this session will be borrowed from IBM Hyperledger presentations and slides from Praveen Jayachandran from IBM.

(Refer Slide Time: 01:28)



So the idea is now we want to move into the blockchain for business. So what happens in a business and we already know that currently, when we have a system like a ecommerce system or grid management system, or payroll management system, usually they are centralized databases, and with a web server or some kind of a user interface, and then through web client or other kind of clients, we interact through the server to the database right.

So as we know that, that has an issue that the entire data is under the control of the company or the business that is hosting that server and the database server and therefore, there is lack of transparency. And also there are security issues, because of the centralization, there would be security issues, and certainly, there will be issues related to when you do not trust the particular entity that is hosting the application.

So that those are the reasons why a blockchain based solution which maintains the data integrity and also if designed properly and if the code is written properly, probably has quite a bit of better security is very good idea. But the other thing is that there are many such systems like client server systems, in which various parts of your business are hosted.

For example, you can have a university payroll system in a database server and the corresponding client server system through which it is interacted with. You might have the grid management system in another system. You might have the employee

HR related information on another system. And these things actually make the entire business process very fragmented and human dependent.

So what I want to do now is that I want to integrate all this into a single system, which is distributed, and because it is distributed, it has many players interacting with it. But earlier in a fragmented system where the people who are working on the payroll and people working on the HR database or people working on the student database, etc. they are different people.

They are full owner of those systems and any information that needs to go between these systems are usually done manually or through some kind of a offline mechanism and that basically leads to inefficiency. So what we are trying to now do is that we want to do a distributed information system and there are players or participants who will be all interacting with the same system.

And therefore, the notion of trust becomes a lot more important because we have many entities that are interacting with the same system. And we want to make sure that whatever it goes into the system is not tampered with by any of these entities. It is also want to make sure that they are not making any kind of changes or any kind of updates that are not acceptable to the other entities that are also using the same system for their information.

So all these things together will make this problem very challenging. So what we are doing is that learning from bitcoin and the Ethereum and smart contracts and all these ideas, we learned that we can create distributed system of records, which can be shared by many entities and these entities could be permissionless, which is the case with the cryptocurrency blockchain.

Or they could be actually permissioned, which means that everybody has some kind of a digital certificate or some other way of identifying themselves to the system, which makes it slightly better in terms of attributing who has made which transaction and then if they have done something wrong, then that can be traced back to that particular entity.

But having the ability to trace back or non-repudiation does not mean that they will not do bad activities or unwanted activities, because they might be doing it intentionally, or they might be infected by malware, and therefore very targeted malware, and they could do things like that. So therefore, I need some way of making sure that the entered data remains consistent across all the parties all the time.

And then we also want to make sure that any data that has been recorded remains untampered for once it is recorded for the future time. And therefore, ability to do that would come not by a database that is being connected to by a multiple of all these entities, but creating something like a blockchain, which is an append only distributed system, where integrity is very well designed.

Other thing is that many times across these different domains, different databases, people might have different kinds of business, process related data forwarding, data sharing, and many kind of functions that you want to call on a particular set of data, and then use the results for your computation and so on.

So therefore, normally if you are three disparate four disparate systems, then you have to somehow get the data from each of these systems and then try to do the computation on them and then put it on the other one. So in this case, you can automate all this through the use of smart contracts, right. So smart contracts actually can embed the business logic.

And that is another advantage that you are getting in a blockchain that has the ability to execute smart contracts. Now security is another issue and as we have seen in the previous sessions that security is not a given for blockchain. It is not like blockchain means it is secure. So you have to make sure that smart contracts are secure. You have to make sure their execution engines are secure.

You have to make sure your implementation is secure and all that things but that is something that you can probably do if you know exact what security properties you want. On the other hand, if you have three, four disparate systems, which are talking through manual intervention with each other, then the probability of making them secure is lot more difficult.

And finally, the consensus is something that even though you are we are distributed, and we even though we have parties that are involved in doing transactions or updates and fetching information from this distributed shared database, the parties will not do things unless everybody agrees or anybody who needs to agree, must agree to put something into the database or do make an update in the database.

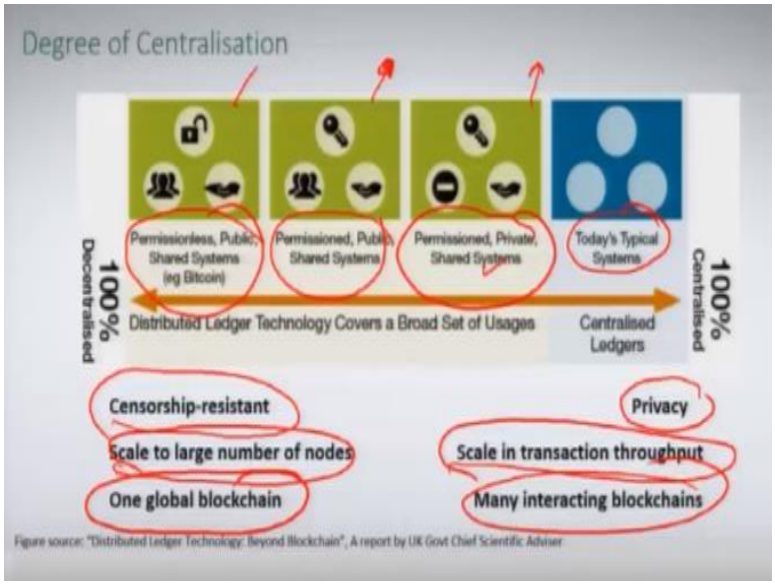
So consensus is important. So shared ledger, smart contracts, consensus, these are the things that we want to have and therefore we want to go for a blockchain based solution. Security is something that we claim to have better chance of making things secure is because otherwise, multiple disparate databases being mediated through other techniques, including manual techniques would certainly leak out data and so on so forth.

So the advantages that one could look for in such an implementation is that the total time should reduce because we are connecting multiple different data sources without manual intervention. I am automating the business logic through smart contracts. So I can assume that the things would be faster.

It removes the cost of intermediaries and various kinds of overheads when you want to have this interaction that is manual, or some cumbersome way of interaction. The tampering fraud and cybercrime can reduce if you design it correctly. Tampering is certainly property, tamper resistance is certainly a property of the blockchain. But fraud and cybercrime probably can only be reduced because of the transparency that you get.

So fraud is harder to carry out and then cybercrime also the same way. But again, I want to caution that these things are not just by virtue of being a blockchain, they do not come for free, they have to be properly designed into the system. And then new business models like IoT integration, etc., can also be made easier through this.

(Refer Slide Time: 10:33)



So as I said before, is that in today's typical system is centralized right. So you have database in which everything is logged, and every kind of updates, reading of information, creating creation of information is kept in a centralized system. Whereas in the blockchain spectrum, so if you go permissionless, public shared bitcoin shared systems like bitcoin Ethereum etc., then you have one kind of solution.

But then in a business scenario, the idea of having all the data on the blockchain to be public may not be very palatable to the industry people. On the other hand, you can also do permission, but public shared system. There also again, the privacy would be an issue, but it is permission. So attribution etc., would be easier. But if you have a permission, private shared system that is where this Hyperledger is placed, right.

So this is kind of bitcoin. This could be a private instance of a Ethereum, where you can instantiate a private Ethereum network for yourself or for your organization. That would be this and this would be Hyperledger. So some of the things about ledger technology as articulated in this document, Distributed Ledger Technology: beyond blockchain. It is a report by the UK Government chief scientific adviser.

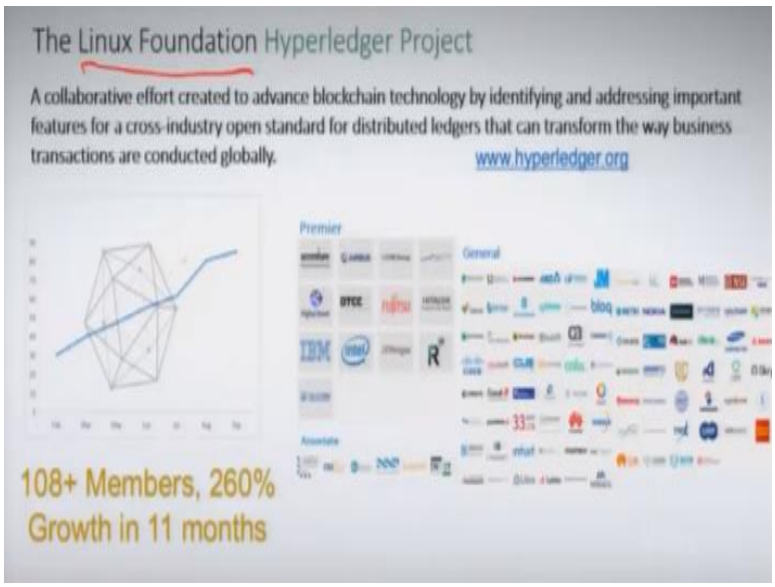
And there they basically say that the blockchain technology is a transformational technology for the upcoming future and there are certain things that you can get out of blockchain that you cannot get in the current systems. So censorship resistance is one such property. If you have something in the blockchain, it is replicated everywhere. So you cannot really you know suppress that information easily.

It scales to large number of participants. So that is one thing. You can also have one global blockchain or you can have many interacting blockchains. You can have privacy if you are going for this kind of a system. And the transaction throughput can also scale if you have a permissioned private blockchain compared to let us say bitcoin, where we saw that transaction throughput is very low.

You have about one block per 10 minutes, which is not really fast enough to do global scale business. So all these things are something that you can get from blockchain. And in particular in the business scenario to in order to integrate various information systems, which are normally run as separate client server system in a blockchain based solution, they will all come together and then because it is permissioned and because it is private privacy and other things can be done in a much better way.

And since it is permissioned and private, you do not have millions of nodes and therefore, you are going to get better scalability and throughput. And also you can, if multiple business entities are interacting through the blockchain, then one entity cannot suppress the information of another entity unduly without everybody's consensus.

(Refer Slide Time: 14:00)

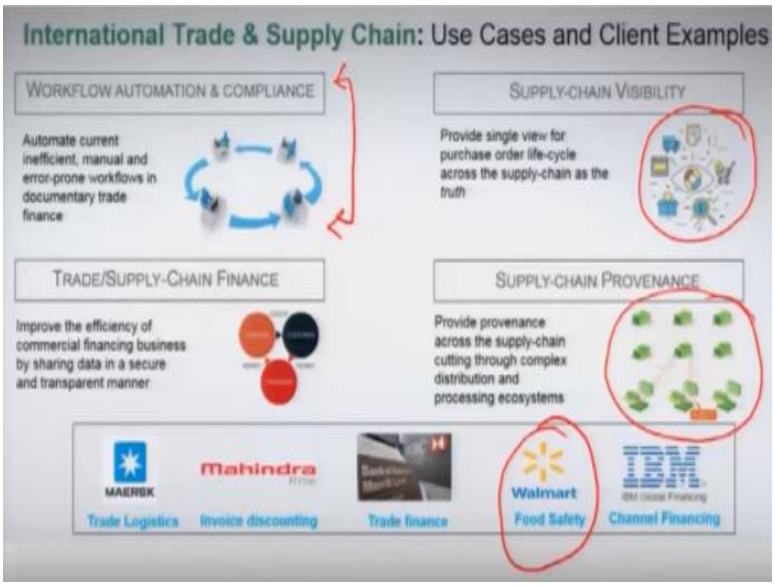


So with these in mind, Hyperledger project came into being. It is actually some champion by Linux Foundation. And they have multiple different projects, right? So they have Hyperledger composer, they have Hyperledger fabric, all kinds of other

family of products that are available. But they are based on the basic technology underlying Hyperledger is the same, whether it is composer or whether it is through fabric.

But the idea is that how easy it is to set up a blockchain and how easy it is to actually write create an application on top of that blockchain varies between, let us say the composer versus raw fabric.

(Refer Slide Time: 14:44)



So some of the used cases that IBM has already done is, as you can see that none of this has anything to do with cryptocurrency. It is all about creating the business process in a seamless kind of IT system using the blockchain right. So workflow automation and compliance is something that has been tried and then the idea is that when you have a workflow in terms of a business process.

For example you have a workflow that customer comes and makes a negotiation, signs a contract, then certain deliveries are done, deliveries are tested, testing is then reported for compliance, then the payment is done. All these things usually is done from desk to desk or from office to office in separate systems. Now in a blockchain all these things can be automated into a single integrated system.

And therefore, things can be done in a much quicker fashion. Supply Chain Finance. For example, you know you have suppliers, you have customers and you want to have

a financier involved for example, and let us say a bank through which the customer takes a loan and then it gives money to supplier.

Then customer pays monthly payment and all this stuff has to be together because the supplier if the customer fails to provide let us say the down payment or customer fails to make proper payment then supplier might intervene and make sure that the service gets stopped or something. So all these things you know is usually done by you know multiple different systems the one that is between supplier and bank.

One that is between supplier and financier and one that is between supplier and customer usually are separate systems. But now with the blockchain you can all put them all together in the same system. There will be everybody will know what is going on what kind of transactions are going on and then the supplier can easily make decisions based on the customer's compliance with its obligations.

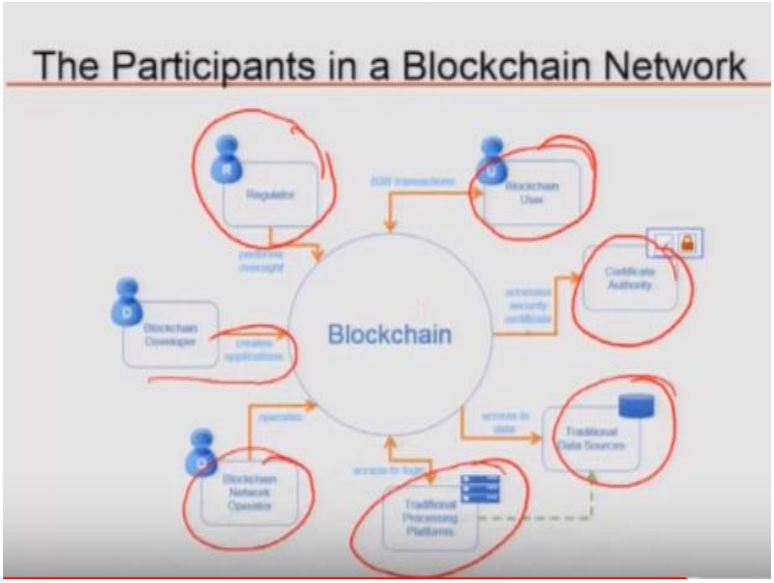
Financers similarly can know what the whether the supplier is providing the goods to the customer and so on so forth. Supply Chain Visibility and Supply Chain Provenance, right. So supply chain is often like for example, in Walmart, the let us say the food that comes from many different sources right? So meat get packaged by various companies at various plants.

And they get supplied to Walmart in their grocery section. Now the question is that suppose some particular batch of meat turns out to be bad imported by multiple customers, then one has to know where that meat came from and what are the other Walmart stores which has the same batch of meat and then they have to be taken off the shelf and corresponding payment and reimbursement and all that stuff has to be done by the supplier.

So usually, this is also tracked very manually in normal scenario. But with a blockchain implementation all that stuff will be in the same blockchain and then all the necessary visibility as to where something is coming from how to attribute it to particular supplier. And whether the supplier is giving credit to the store for returning the meat or throwing out the meat because it was the fault of the supplier.

All that information can be actually gathered from the blockchain. And it cannot be tampered with by any of these parties. And that is a good thing to have. Similarly, the supply chain provenance, like if you want to know where something came from, whether it involves child labor or not, all that stuff can be all tracked if every step of the process puts in all the information on a single blockchain. So these are some of the applications we are talking about.

(Refer Slide Time: 18:52)



So who are the participants in such a blockchain network, right? So in case of a bitcoin we saw that everybody is similar, right? So some of them distinguished themselves as miners because they have more computation power, but everybody has the almost the same ability to do and things on the blockchain right, accepting that some of them may become miners, same thing with Ethereum.

But we also saw yesterday that because of the inequality that has happened over time, so therefore, it is not really the same, but at least as far as the technology is concerned they are at the same role and responsibility. Here actually, it is quite different. So we have the blockchain. So blockchain developer creates applications. This is also true in Ethereum that you can be a smart contract writer.

So you are a blockchain developer. And then, blockchain network operator is the one who maintains the blockchain network, which means that all the entities that maintain the blockchain, do the consensus everything that has to be maintained by some entity. So that is a network operator. You have the blockchain user. For example, if it is a

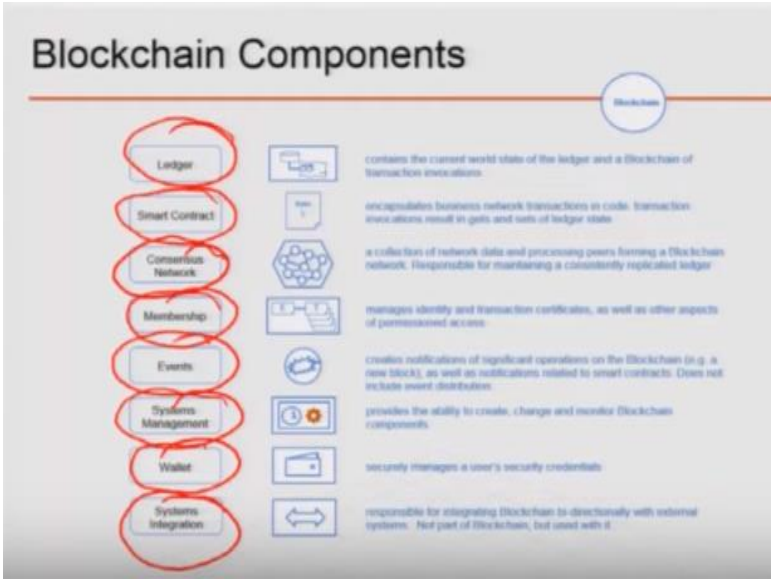
supply chain blockchain, then the blockchain user would be all the entities that are involved in the supply chain, the customer at various steps and so on.

Now in a permission blockchain, you also need to identify users with some digital certificate. So there has to be a Certification Authority involved. And this could be an internal Certification Authority or it could be a regular, you know digital certificate provider CAA, that kind of entity. Now also blockchain might be used to interact with the legacy traditional data source.

So that will be actually the blockchain might actually pull data from the traditional data source to have the information that is required to actually do execute some transaction or it can also send information back to traditional data source and then the traditional processing platforms that was part of this traditional data source based IT system that the company already had, could also have this thing integrated with the blockchain.

And then the regulator, so in case of this, this is the supply chain, for example, or some kind of a money lending application over the blockchain. Then a regulator can also look at all the transactions he has been, the regulator will be permissioned into looking into the blockchain. And then therefore, they can check the regulatory compliance much more easily than today when there is huge amount of paperwork involved. So that is the vision of this kind of Hperledger based blockchain applications.

(Refer Slide Time: 21:57)



So what are the components? Components is, obviously there has to be a shared ledger, which contains the current state of the ledger and the blockchain of the transaction invocation. So the state in this case is not really on the blockchain, but it is in a store that everybody has a copy of. So everybody knows the state of the blockchain.

But the blockchain itself has enough information in a hashed form that will make sure that the integrity of that state information is not compromised. And because of the replication, it cannot be easily compromised anyway. Smart contracts are the actual programs that will run to make transactions happen. And they actually have the business logic, right.

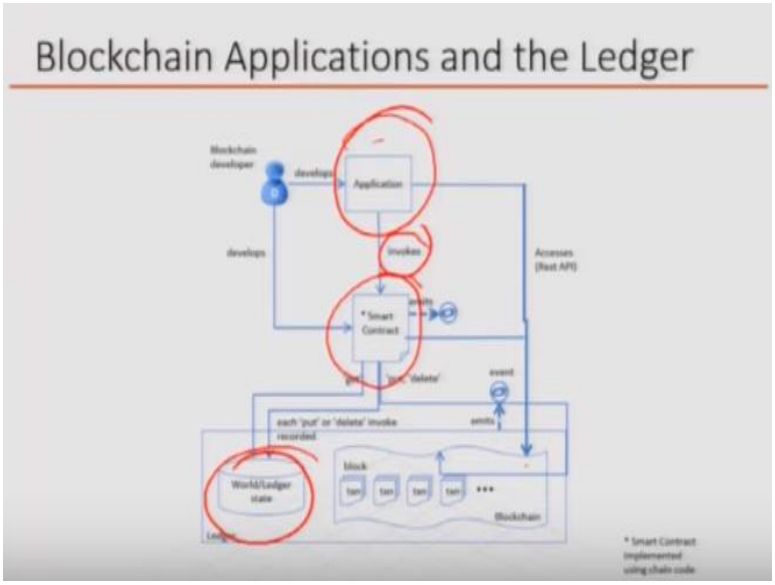
So by invoking multiple different transactions in the smart contracts, a particular business process, maybe automated. Consensus network, so since it is a blockchain, there has to be a consensus. And then the consensus network basically is responsible for that membership. Of course, this is a membership service is basically certification or identification for each of the participants that has to be there.

Events. So blockchain transactions may actually create certain events and those events might be also used for triggering other transactions. So there is a notion of events and then the system management because there is a network operator who can create change monitor various blockchain components. User wallets in this case, since we are not talking about cryptocurrency blockchain, it is not about money in the wallet.

But wallet actually contains the user's security credentials, which could be digital certificate, it could be username, password, or whatever the information is. And then systems integration is this basically the integration with the external systems, the systems that are legacy systems, systems that are not participating directly in the blockchain. So in a blockchain like Hyperledger, these are the components.

And with the very well defined and different roles and responsibilities, which is quite different from the blockchains that we have seen so far.

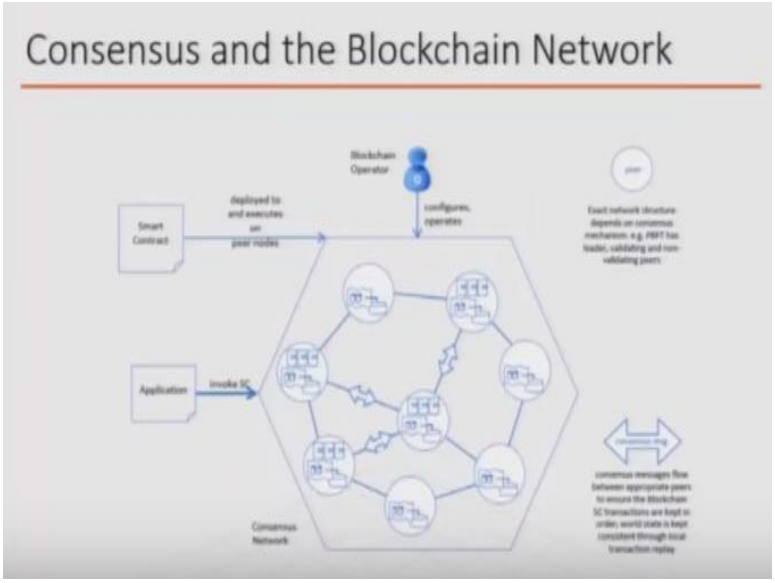
(Refer Slide Time: 24:18)



So the blockchain applications actually invokes smart contracts. So an application as we saw is like dapps, right, a distributed application, it has ability to also query the blockchain. And this access has to be provided through what we call rest API's. And then, the blockchain developer develops both the application and the individual smart contracts that together make the application work.

And then there is a state of the ledger. And that is a separate database, but everybody has a replica of the blockchain and this state information at all the different nodes. And that is how the entire system is configured.

(Refer Slide Time: 25:11)



So when we come back, we will talk more about the functioning of this blockchain. So far we are only talking about who are the participants who writes the application, who writes the smart contracts, what is in the blockchain versus what is in the state ledger, state part of the ledger. And then we talk about roles and responsibilities. But when we come back, we will talk about little bit more on how the entire Hyperledger blockchain normally functions.