Introduction to Blockchain Technology & Applications

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

Lecture - 25

Welcome to the seventh week of the blockchain technology and applications course. We are recording in a very strange situation. The whole India is going through a lockdown and our staff who actually to our studio recording are unable to come to work. So we are going to record this ourselves. And therefore, you will see that you would not see the instructor, but you will hear us and you will also see the slides as we go through them.

So with that in mind, I would request your indulgence with this form of presentation where the instructor is invisible, but hopefully that will not take away from learning. So in the past few weeks, we have been talking about cryptocurrency blockchains. Then we talked about a non cryptocurrency blockchain namely Hyperledger. And we discussed the differences between permissioned and permissionless blockchain.

And in case of permission blockchain like Hyperledger, we have seen that we have to have some kind of an identity and therefore, the blockchain had an Identity Service. And so as a result, the huge burden of making consensus among the nodes that are permissionless that are kind of anonymous is you know fulfilled by a very computationally expensive process, namely proof of work.

And in case of Hyperledger we saw that, that is no longer required. And in fact, Hyperledger has a notion of validation first and then it has the ability to order the transactions. And then it has the ability to actually you know put the information in the ledger after making sure that the transactions do not conflict. And that is how the Hyperledger blockchain worked. Now today I am going to talk about two different block chains.

One is specifically designed to work in a particular technological situation that is arising out of the extensive use of the Internet of Things or IoT devices, which are autonomous devices, which communicate with each other. And therefore, they often rely on each other on gating services and therefore, and the shared resources. And therefore, there is a notion of payment in terms of getting some services done by one device from the resources of other devices.

And to create such a payment in a way so that the all the payments and all the requests for resource usage or request for computational resource borrowing, one has to actually create what we call transactions and these transactions will obviously have a cost associated with it. And because of that cost, we have payments.

And because we have payments, of course, we could have done payments offline, which would mean that we would actually have a separate offline channel through which the owners of the devices could actually bill each other and have settlements.

But that is not very effective, especially given that the number of such devices and number of different owners could be daunting. And therefore, a blockchain based solution was proposed in the form of a specific technology called IOTA. Now this technology relies on notions that are German to the blockchain. But as we will see that they are not really using exactly the blockchain technology as we have seen so far.

They are using a quite different data structure. They are using a quite different method of validation and consensus. And therefore, some people would consider IOTA is as not a really a blockchain framework, but because of the similarities with the underlying technologies that they use in terms of digital signature, hashing, validation, etc., consensus, so therefore, we would consider it as a specific, customized blockchain technology.

So when I say customized let me remind you that bitcoin for example, is also somewhat customized for bitcoin. But as we have seen that somebody could develop other blockchains, other kind of solutions on top of the bitcoin blockchain. We know that we can persist some information for timestamping, or making certain information permanent and verifiable with the help of bitcoin blockchain.

For example, an educational system might decide to have their students graduation certificates in the blockchain using a you know using a particular field that we talked about, where we use some kind of a proof of burn kind of transaction to persist information. We could also develop other tokens on top of the bitcoin blockchain. But in general, the bitcoin blockchain is mainly known for a specific cryptocurrency called bitcoin.

So in that sense, it is quite custom type developed blockchain technology. On the other hand, the Ethereum decided that, that is not very useful in the sense that if bitcoin does not become the currency of choice of people, then the bitcoin blockchain technology will also not find much use and therefore, it might not survive. But Ethereum is designed in a much more generic way so that using smart contracts, you could actually develop any kind of application.

So you can use it as a cryptocurrency application framework, but you can also develop voting applications, you can develop land record registration, you can develop solutions for medical information sharing and medical information integrity and security provider. It could you could develop solutions for certification, you can provide solutions for creating identities.

You can create solutions for doing providing certificates, like even the digital certificates to people. So in that sense, we know that Ethereum is a very generic blockchain framework, which can be customized by developing suitable DApps to solve many different types of problems. The Hyperledger on the other hand is also pretty generic. So it is not designed with any specific application or any domain in mind.

And therefore, you can develop many different kinds of solution. Even you can develop a some kind of a digital coin mechanism for as a currency on top of Hyperledger. So the one that I first want to talk about, as I already mentioned is the particular blockchain technology developed for Internet of Things ecosystem. I see it as a customized solution for solving problems arising in a very specific domain.

And therefore it has its own form and function that can also be, you know somehow molded into other applications. But it is not as easy to mold it into other applications as it would be for something like Ethereum or Hyperledger. So that is one important thing to remember. The other one that we are going to talk about is the Corda, which is also designed for financial players like banks, the exchanges and the various kind of financial you know players in the finance market.

And therefore, it is also quite customized and designed specifically for enforcing and executing the provisions of legal contracts that happened between financial Institutes. And therefore, their design and their architecture are very much customized with those kind of applications in mind. Having said that, that does not mean that they cannot be molded into something different, especially if they have the flavor of legal contracts and the contracts are to be executed over time.

But still, it is customized. So therefore, today's class, mostly will focus or this week's classes will mostly focus on this kind of customized blockchains.

(Refer Slide Time: 11:58)

Acknowledgements

- IOTA while paper https://iota.org/IOTA_Whitepaper.pdf
- IOTA blog https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4
- https://public-rdsdavdrpd.now.sh/

So let us first talk about Iota. So Iota is a blockchain technology, actually the underlying blockchain technology is called Tangle. Tangle is the basic data structure and basic you know protocol by which the transactions between autonomous agents that are running inside various devices, Internet of Thing devices happen and the overall system is done by the IOTA Foundation.

The name IOTA already has the Internet of Things in it. So you can imagine the reason for its creation. So most of the thing that I am going to talk about today are in the IOTA white paper which is quite widely available. And then certain blogs, for example there are blogs on the Tangle. And then there are certain simulations I am going to show that is also from this particular site here.

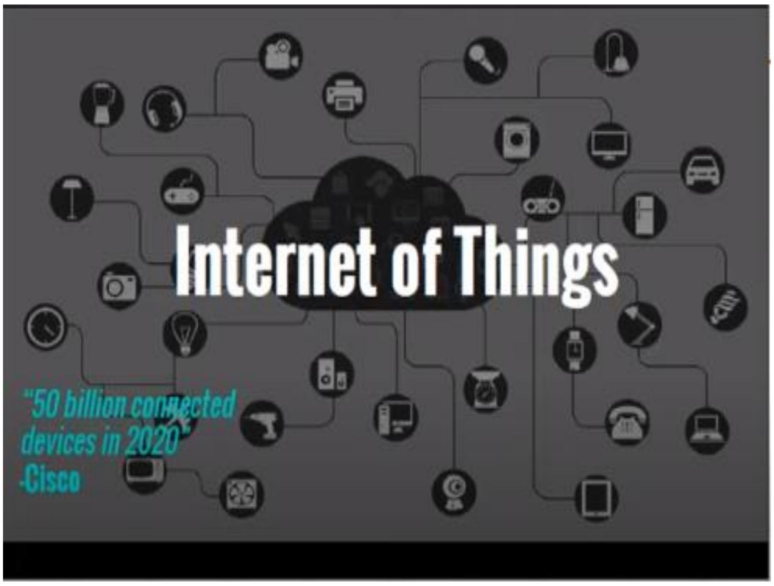
(Refer Slide Time: 13:31)

IOTA

Transactions, Confirmation And Consensus

So let us see. So we are not going to let me see where I am, okay. So let us talk about IOTA. And in IOTA, there are three basic concepts that we have to understand. One is the concept of transactions. The concept of transaction confirmation and consensus about a transaction being you know valid, no double spend has been has occurred. And the digital signatures associated with the transactions check out. And this basically are things that are has to be checked as part of the consensus.

(Refer Slide Time: 14:15)



So what is internet of things? So all of you probably know what Internet of Things are. So we talk about smart home these days, right? So smart home has smart you know thermostats, it has Smart TV, it may have a smart nowadays smart refrigerator, smart microwaves, it may have smart lighting, it may have smart you know smart grid components like rooftop solar panel, and various ways to control the various electrical equipments to save energy.

And all those things require a lot of sensors and lot of actuators and control. So in order for these things to work together to cooperate towards a goal, for example a smart HVAC system or heating and cooling system would be to have sensors in each room. And then based on a certain goal of let us say, minimizing the expenditure on energy, the different room temperature sensors and room, you know ducts and vents has to be opened.

The temperature sensor has to send data to a controller, the controller may actually separately control the needs of various rooms and open the vents with larger aperture or shorter aperture, this kind of stuff. So that what that means is that all these devices communicate to a controller, maybe they also communicate with each other in order for achieving certain goal.

And I would call it a computational goal or kind of information technology goal, which might be associated with the cost optimization and other requirements.

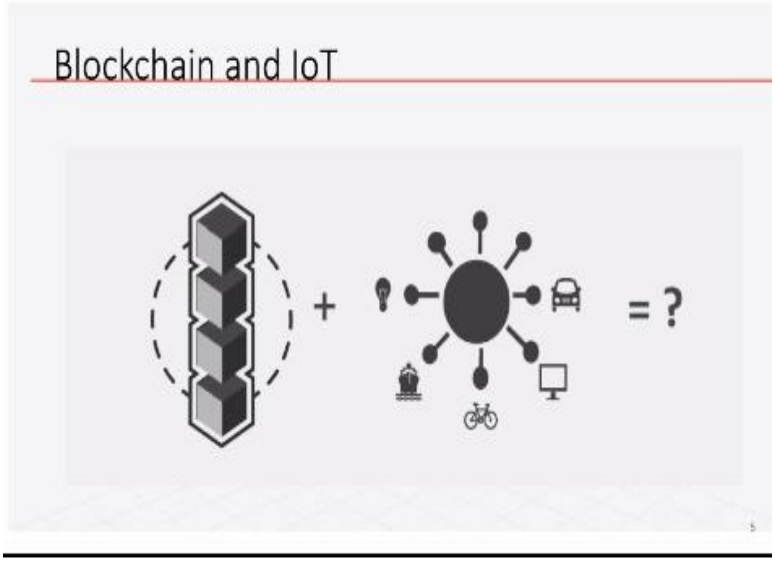
Similarly, you can talk about smart grid. Smart grid is the power grid, which is more and more having lots of communication between various devices.

Now these devices are not as simple as the smart home devices, they are often quite complex devices. They have many controllers at various locations of the grid, and there may be a overall supervisory control. And all these things together, they actually make a whole smart grid. And similarly, you can have a smart transportation, you can have various kinds of other you know device cooperation based infrastructure.

For example, vehicles like smart vehicles, they actually talk to each other, in order to avoid accidents, to understand the location of each other, especially around corners. They actually may talk to the infrastructure on the side of the road, they can even talk to infrastructure within the within the cars, these kind of things. So Cisco had earlier predicted that there will be 50 billion connected devices in 2020.

Now this is an older prediction. Now that we are in 2020 we probably have such numbers because the smartphones themselves are often part of the Internet of Things and then we have you know smart grid, we have smart manufacturing systems, we have smart transportation, all kinds of smartnesses that we talk about this requires many devices and sensors.

(Refer Slide Time: 18:21)



Blockchain and IoT

Now so what is the role of a blockchain in all this? So as we go forward with the technology of Internet of Things, it turns out that many of these devices are not necessarily very computationally resourceful. So but they need to do some computation, especially if AI is thrown into the picture for them to actually learn from the environment and then decide on certain control actions etc.

So then they can actually borrow resources, computational resources, storage resources, bandwidth etc., from other devices and therefore, they may have to transact with other devices. So note that there is no human intervention involved when they do that. So now the question is should now these devices are often not owned by the same company or same person.

And therefore, why should a device owned by another entity, you know serve some purpose for a device that is under the control of a different entity. So there has to be some kind of business relationship. In order to have that business relationship, what they have to do is they have to request a service and in return of that service they might have to pay.

So now for example, a cars that are electric vehicles, and they need charging. So there are roadside charging stations. They go to the charging station and get charged. So they have to pay. Now this payment could be done in traditional manner by keeping track of the amount of resources with the timestamp, you know like how we use credit cards and have the transaction log and have monthly billing or periodic billing of the owner of that particular device or particular infrastructure, you know.

And then bill comes to the user, in which case the user is the owner of the device. And then they can actually pay by banking and cheque and whatever. That is an old school method. But in this method, there are several problems. One problem is that these transactions you may get over built or you may actually somehow some transaction may be missing and you may be under built.

So and then somebody the owner, who is keeping all this transaction data going to him from his device might actually tamper with the transactions and over bill you. So these are some of the human problems, but the bigger problem could be that if we are having billions of such devices, obviously not all these devices are owned by the same entity. And many of these devices are, you know maybe in neighboring locations.

But they are owned by entities that are not even familiar with each other in the real world familiarity sense. So therefore, it is arguably a good thing if this devices can complete the monetary part of the transaction also unto themselves and we do not have to involve human in human beings to do the billing and other activities. Now how could device pay another device?

And the only way the device can pay another device is to have some kind of a digital currency. So obviously, when you think about digital currency in today's world, we think about cryptocurrency. So if you have cryptocurrency, that you have put in the wallet of a device, then the device as it needs, it can negotiate with another device completely autonomously and make the payment and get done with the transactions.

And then eventually that cryptocurrency that goes to the wallet of the other device, that can be either used for it to actually spend on acquiring resources for its other computational reasons or other activities. Or eventually its owner could actually somehow encash it through some exchange. And that is where the IOTA cryptocurrency or IOTA coins come in to help, come to help.

Because now if you could create a cryptocurrency system, then we can actually have this thing completely autonomous without any human intervention. Also all this transactions that happens, transaction would mean that I am requesting some resource and I am going to pay this amount and somebody else is using that amount for doing another transaction to some of its other neighboring devices and stuff like that.

And this kind of information of the transactions could also be persisted in a blockchain so that later on some auditing and other kind of AI based usage of that transaction history to optimize the location of the devices, optimize the amount of resources available to the devices, etc., can be also done by the owning entity for all the devices. So therefore, blockchain seems to be a good solution to do this.

And as I said that if it was if all the devices were owned by one entity, then you probably would not need a blockchain and you could probably do this either free of cost for device owned by you helping another device that is also owned by you or it could be done through some centralized you know server, in which all the data, transaction data is persisted etc.

But here we are talking about entities that do not trust each other, do not know each other and they are still doing this completely autonomously. Now the question then would be that why cannot I use bitcoin? Or why cannot I use Ethereum, the Ethereum Mainnet to do all this transaction. And ideally, you could. But the problems are that first of all these cryptocurrencies are pretty expensive.

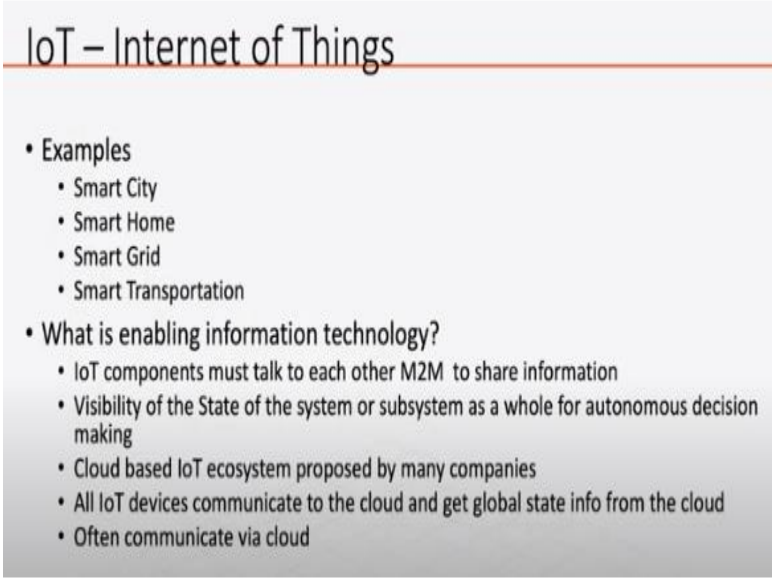
So that is one issue. But the second issue is that the, in order to interface these devices with such blockchains, they have to become nodes in the blockchain, this devices because you do not want any human intervention. And therefore, you want them to become nodes of this blockchain.

You could probably do a little better and you could probably have a sort of like a mediator which actually mediates for multiple different devices and then be part of this node, but then the granularity of the transaction history etc., will be lost, because any kind of manipulation of the transactions of these group of devices can be done by this mediator.

So the other thing is that the if obviously these such devices are resource constrained, so they cannot become nodes to this blockchain, which actually are or have millions of, you know transactions and blocks. And then finally, the other issue is that the transaction speed for bitcoin and Ethereum are not enough. So if you have billions of devices, and they need computational help from other devices, we are talking about a timescale of milliseconds.

Whereas these things actually have timescales of seconds to minutes, so they do not match properly. So therefore, it makes sense to actually consider a different blockchain solution. And that is what IOTA was trying to solve.

(Refer Slide Time: 27:10)



IoT – Internet of Things

- Examples
  - Smart City
  - Smart Home
  - Smart Grid
  - Smart Transportation
- What is enabling information technology?
  - IoT components must talk to each other M2M to share information
  - Visibility of the State of the system or subsystem as a whole for autonomous decision making
  - Cloud based IoT ecosystem proposed by many companies
  - All IoT devices communicate to the cloud and get global state info from the cloud
  - Often communicate via cloud

So going back to what I was already telling you about this internet of things, I already mentioned that smart city, smart home, smart grid, smart transportation, these are places where this IoT ecosystem thrive. But so what are the enabling information technology? So first of all, as I mentioned, IoT components must talk to each other machine to machine or M to M to share information, request resources, make payments, etc.

The state of the entire system or a sub system a group of devices as a whole has to be somehow visible to somebody, right? Obviously, each device may not keep track of the entire state of the entire ecosystem, because they are resource constrained, but somebody has to keep track of the state and then make autonomous decisions. It may be done together by all the devices, but not by some of the individual devices.

Now people have actually talked about or have implemented cloud based IoT ecosystem. For example, Azure IoT by Microsoft is one example. And if you do a search on Google as your IoT, then you will find out that they actually provide similar solutions. So they will allow to connect all your devices to an application hosted on Azure and that application will get data from each of the IoT devices.

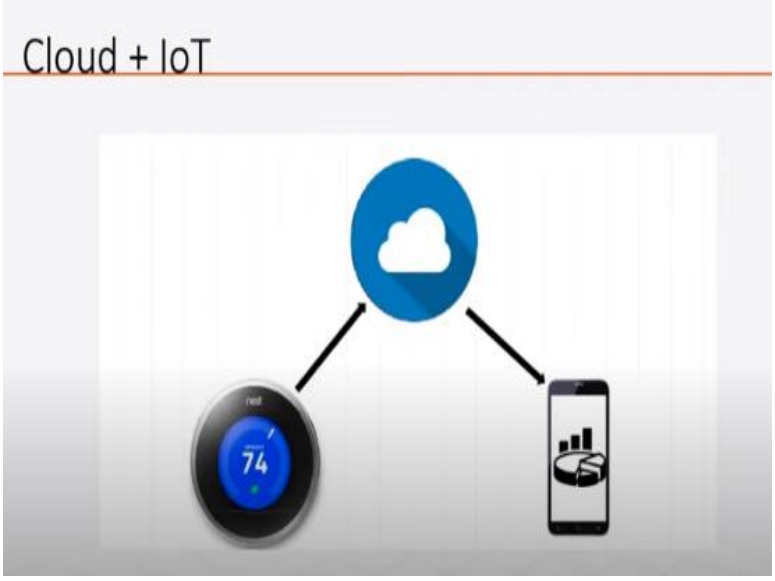
And then your application can infer the entire global state and make decisions and send the decisions back to the individual devices to adjust maybe, for smart valves, they can ask them to adjust the luminosity or adjust to turn them off. It can actually reduce the speed of a turbine. It can reduce the speed of a ceiling fan or it can reduce the temperature of a refrigerator or it can change the air condition setting etc., etc.

So often this things are communicating via the cloud. Now as I said before, this cloud based solution would work well, if you own all the IoT devices. For example, in your smart home, if you have multiple devices, you can actually use Microsoft Azure IoT or many other such cloud based offerings and have everything control via the application hosted in cloud.

But if you are going to not own all these devices and there are you know hundreds of different entities that own all these devices, then you cannot be trusted to have access to all those devices, state information as well as controlling them, right. So therefore or resource sharing decisions, you know on a single cloud. In that case, the cloud has to be managed by multi party.

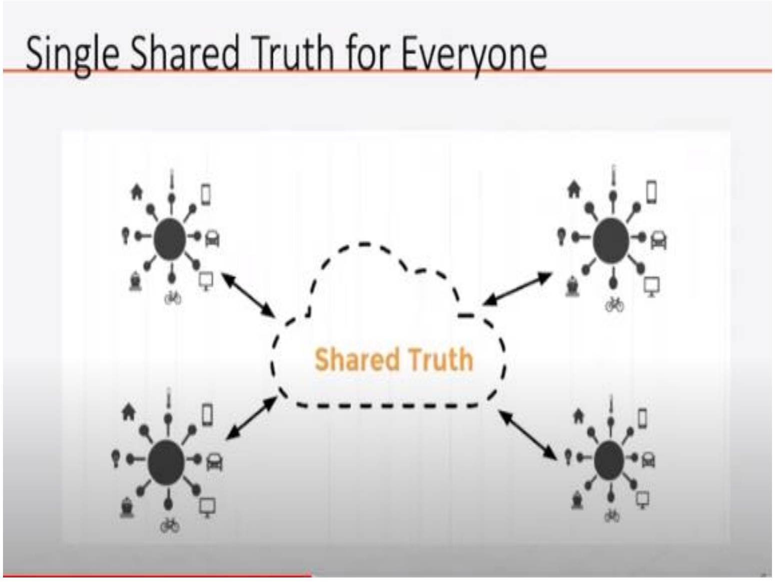
And that would basically give us bring us back to the situation of a blockchain which is basically a decentralized application rather than being hosted in a centralized place like a cloud.

(Refer Slide Time: 31:04)


Cloud + IoT

So this is kind of the scenario I was talking about. So if you have a thermostat, and if you have a smartphone to control that thermostat remotely, then this thermostat might be uploading all the information to the cloud. And then your smartphone is also interacting with the cloud. And the smartphone, when it wants to control the thermostat, it tells the cloud then the cloud then tells in the thermostat to actually change its setting. So that is the kind of scenario we are talking about.

(Refer Slide Time: 31:39)



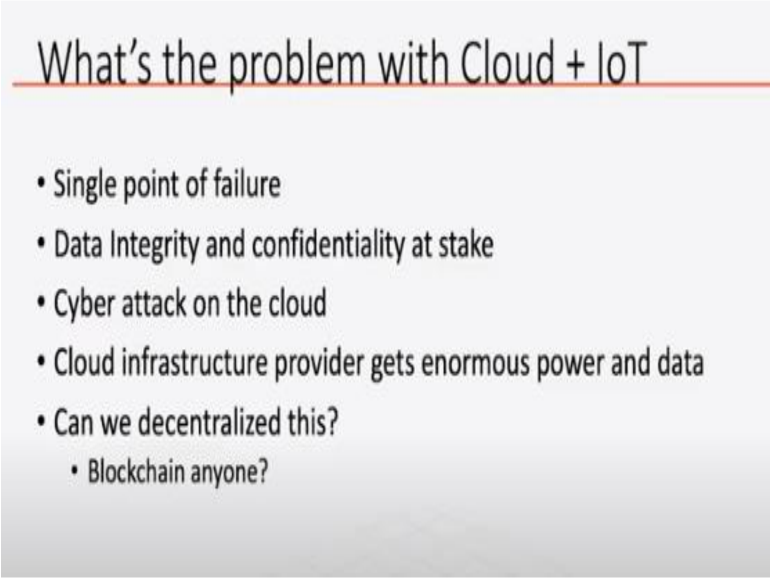
Single Shared Truth for Everyone

So what we in all this kind of cloud based solution, or if you want any other kind of solutions, in all these cases, all the devices should have the single shared truth about everything, right. Now it may or may not store the single shared truth in itself or in a cloud, but it has to be accessible to them, right. So you may actually have the shared state of the entire system with all the devices, current state etc., in the cloud.

That does not mean that each of the devices is looking it up. But if they want to look it up, they can actually look it up. And that is the whole idea of having this having a solution for this IoT, you know system control and decision making. If the shared truth is different at different points of the system, then they will make inconsistent decisions. And that is not good for you.

And we know already from this class that the blockchain is a repository of single shared truth, because as we have seen that through consensus mechanism through validation we always have the shared truth that is true, that is known to be true by everybody who is participating in the framework or in the system. Right. So that is the, another way of looking at the need for a solution where blockchain seems to fit well.

(Refer Slide Time: 33:25)



What's the problem with Cloud + IoT

- Single point of failure
- Data Integrity and confidentiality at stake
- Cyber attack on the cloud
- Cloud infrastructure provider gets enormous power and data
- Can we decentralized this?
    - Blockchain anyone?

So I already discussed this that the cloud based IoT, you know decision making and control mechanism has several problems. The cloud is a single point of failure. And in that sense it is not just a failure in terms of that if the cloud crashes then the entire system cannot be cannot proceed. But also the cloud is a point where somebody is managing the cloud and therefore data integrity maybe questioned.

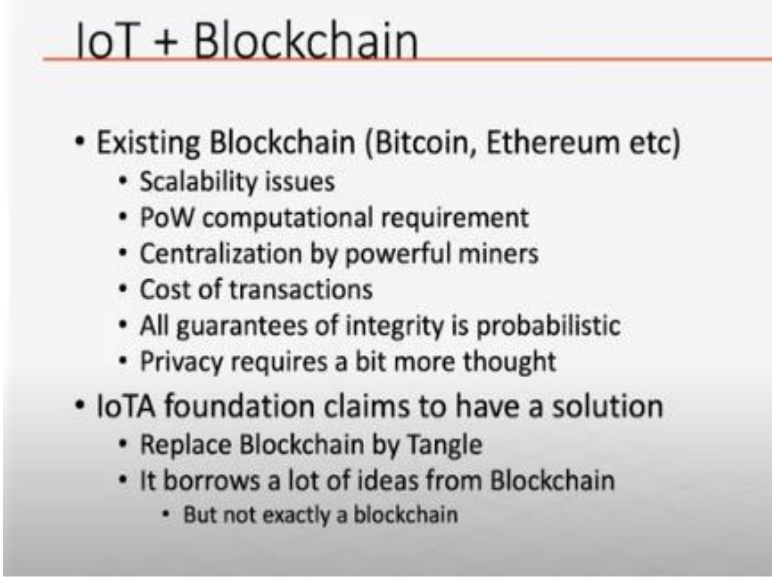
Like so some device's owning entity might say that the information that is kept in the cloud about its devices may have been tampered with. Or he or she might not even want that the all the information about this device be visible to the owner of the cloud or it may be made visible to all the other stakeholders in the system, which is not necessarily desirable.

So integrity and confidentiality could be at least a question. If not compromised, it may be questioned. And there is no way to argue that, that has not happened without an explicit mechanism to prove integrity and confidentiality. And again, that brings us to blockchain where these things could be actually arranged to be proven, or by construction, it has to be trusted. The cyber-attack can happen on the cloud.

Obviously, then again, the integrity and confidentiality would be at stake. And then also if a DoS attack happens or denial of service attack happens, then it may be even worse, and the cloud system would actually stop working. And therefore the entire the IoT ecosystem, the so called smart home or smart transportation will stop working.

So in that sense, the cloud infrastructure provider, like let us say Microsoft Azure will get enormous power and data over all the entities that are in the participating in that smart, whatever smart transportation, smart home, smart building, whatever. So we want to decentralize this. And certainly, decentralization after doing this class should bring to your mind the idea of using a blockchain.

(Refer Slide Time: 36:14)



IoT + Blockchain

- Existing Blockchain (Bitcoin, Ethereum etc)
  - Scalability issues
  - PoW computational requirement
  - Centralization by powerful miners
  - Cost of transactions
  - All guarantees of integrity is probabilistic
  - Privacy requires a bit more thought
- IoTA foundation claims to have a solution
  - Replace Blockchain by Tangle
  - It borrows a lot of ideas from Blockchain
    - But not exactly a blockchain

So let us consider existing block chains like bitcoin in Ethereum. I have already hinted that these are not necessarily the best solution for the particular problem we are trying to solve. Scalability is an issue, right? If we are talking about 50 billion devices, of course not all devices would be using the same infrastructure. But still, if you have a smart transportation, we could think about hundreds of thousands of smart devices.

They need to interact, they need to make this they have a shared single truth. They need to have a decision making process and of course these blockchains are may not scale for that. The proof of work computational requirements of course, none of this smart devices are computationally endowed enough to actually take part in that.

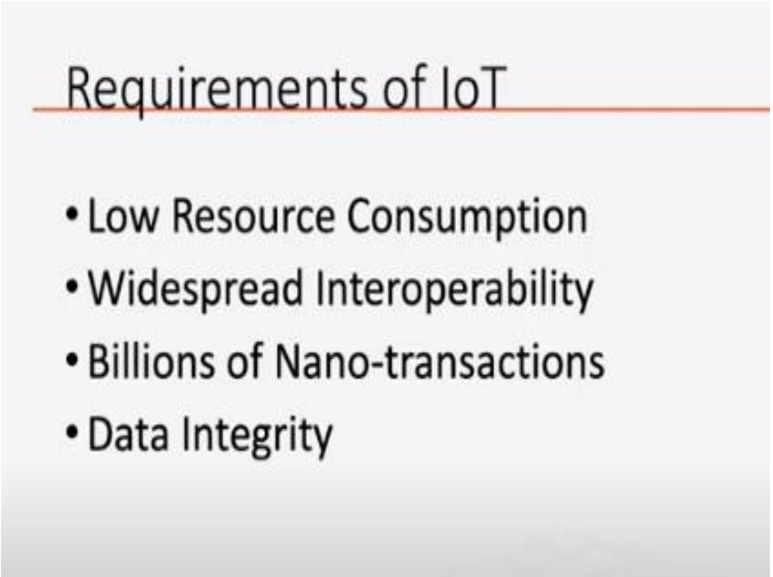
And the so therefore, there is a centralization tendency in bitcoin and Ethereum and we discussed this in the context of Ethereum when we talked about Ethereum that even though the decentralization and democratization was the goal of bitcoin and Ethereum, but turns out that you know 90% or even more percentage of the transactions, the money etc., are either held by a very few of the nodes.

And that basically would mean that it is going back to the centralized solution kind of thing which we do not want and that is why we said that cloud is not the most desirable solution to this problem. The cost of transactions of course, will be very high because all this cryptocurrencies are valued at a very high value.

And the guarantees of integrity is obviously probabilistic, which we cannot avoid even in this case, but that is a that is an issue. And then privacy would require more thought because as it is, bitcoin or Ethereum are not encrypting any of the transactions or any of the state information, and therefore everybody can see everything in those blockchain all the past history, and transactions and etc.

In our case, we may not want that kind of thing. So IOTA foundation came up with this notion of IOTA and they replaced the blockchain by this kind of a structure called Tangle and it borrows a lot of ideas from the blockchain, but it is not really a blockchain and as we will see very soon.

(Refer Slide Time: 39:24)



Requirements of IoT

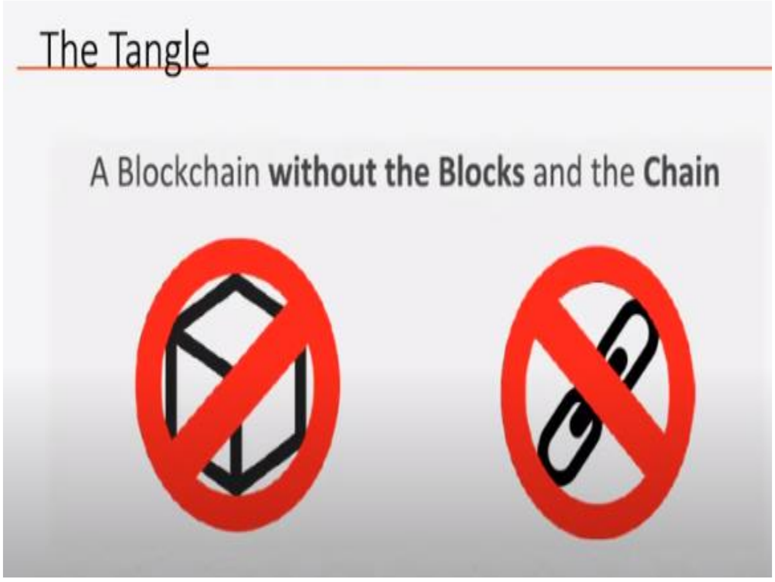
- Low Resource Consumption
- Widespread Interoperability
- Billions of Nano-transactions
- Data Integrity

So requirements of the IoT devices to be part of something like a blockchain is that the resource consumption for participating in the blockchain other than its own actual functionality has to be low, right. And then there has to be interoperability, right. So you cannot have for, you know some custom solution for specific manufacturer of IoT devices.

It has to be completely interoperable among all devices, among all manufacturers, etc. And the number of transactions is mind boggling. And that is one of the reason why bitcoin Ethereum etc., cannot cope with this is there will be billions of nano transactions. And then data integrity is important as with any of these things, so we do not want the data to be left just in a database, all the transaction data.

But it has to have some integrity mechanism against any kind of manipulation of the data.

(Refer Slide Time: 40:41)

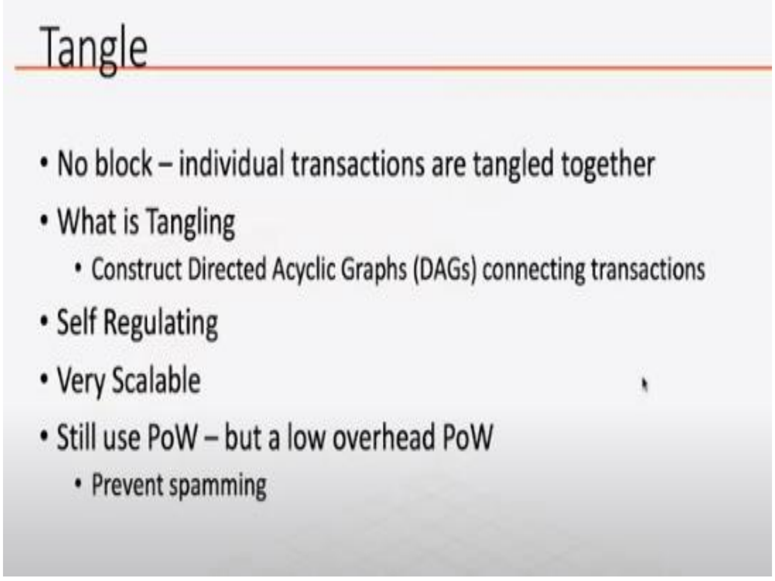


The Tangle

A Blockchain **without the Blocks** and the **Chain**

So as I said that IOTA is actually introducing this structure called Tangle, which is a blockchain without blocks and without chain, right. So what could that be?

(Refer Slide Time: 41:00)



Tangle

- No block – individual transactions are tangled together
- What is Tangling
  - Construct Directed Acyclic Graphs (DAGs) connecting transactions
- Self Regulating
- Very Scalable
- Still use PoW – but a low overhead PoW
  - Prevent spamming

So in Tangle, we have no notion of a block. So all the individual transactions actually are called are actually nodes of a data structure or a graph. So visualize bitcoin blockchain or Ethereum blockchain as a chain of nodes, right? So each node contains a block and the block contains many transactions. And then we have a chain of those. That is what we see as bitcoin or Ethereum etc.

Whereas here, we are only talking about individual transactions as nodes. And they are connected with each other through a graph structure. And we call we say that they are tangled together. And the idea is that transactions has nodes and they are connected by a directed acyclic graph. So what is a directed acyclic graph? All of you know what is a graph. Graph is a set of nodes and edges. Edges is what connects the nodes.

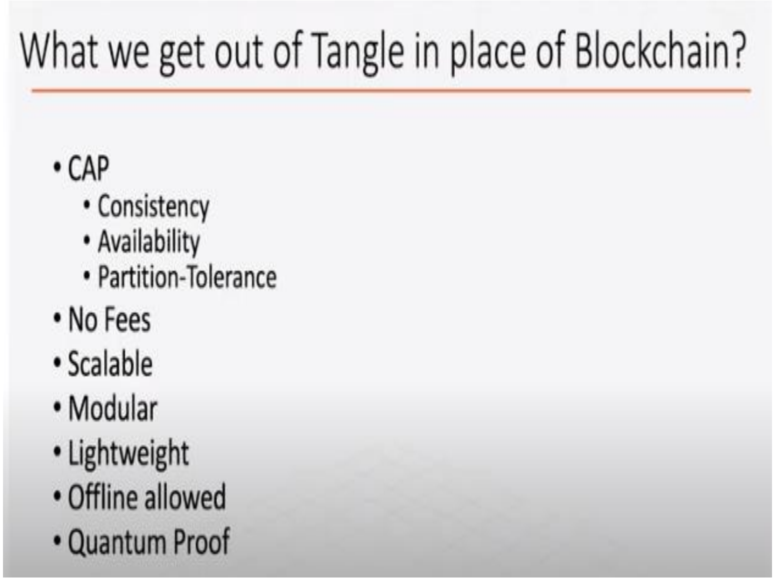
Acyclic graph is a graph in which nodes are there, edges are there, but there is no cycle, right. And then a directed acyclic graph is a directed graph which means that from node A to B if there is an edge, then there will be an arrow from A to B and but does not mean that B to A you can go because the arrow is unidirectional. If there is a way to go from B to A also then there should be edge or a path from B to A.

So unlike undirected graph where having an edge between A to B means that I can go from A to B and come back from B to A, directed graph are directional. So you cannot just go like that. So this is the kind of graph we are talking about. So instead of a chain, as in case of regular blockchain, we have a graph which is directed acyclic graph. Blockchain, the bitcoin blockchain also is directed, it is a directed chain, right.

So coming, starting from Genesis block, it is unidirectional, right. So this block, then Genesis block, then the next block and next block and so on. Here, it is a directed acyclic graph, but it is a directed graph. So tangle is self-regulating. We will see what that means. It is quite scalable. And it still uses proof of work, but the proof of work is not so actually this should be corrected.

We meant the low overhead and not the long overhead. Low overhead proof of work. And the proof of work is mostly used not for consensus but to prevent spamming. And we will see why that is.

(Refer Slide Time: 44:26)



What we get out of Tangle in place of Blockchain?

- CAP
  - Consistency
  - Availability
  - Partition-Tolerance
- No Fees
- Scalable
- Modular
- Lightweight
- Offline allowed
- Quantum Proof

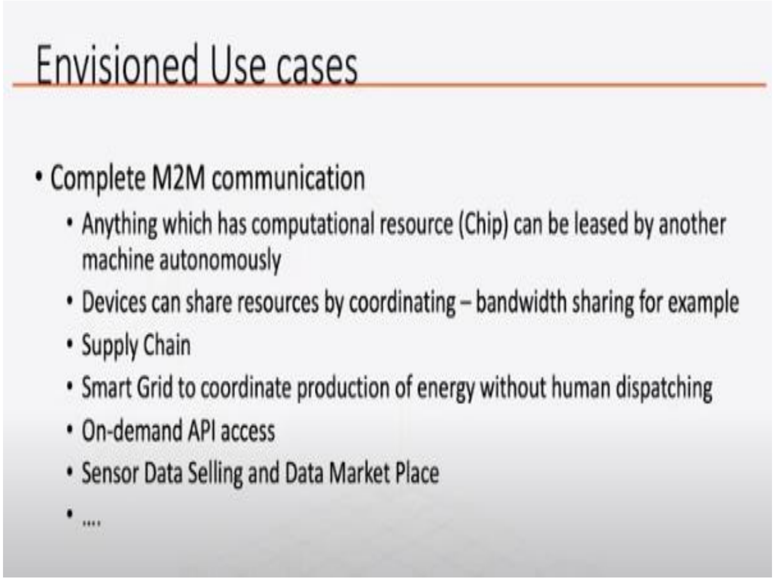
So what we get out of Tangle instead of using a traditional blockchain, right. So first of all there is this notion of Brewer's CAP theorem, which requires a distributed system to have consistency, availability and partition tolerance. So consistency is basically obtained by some kind of a notion of a consensus that the data at each node or notion of the shared state space at each node is the same consistent view.

Availability means that it should be available. The service or whatever service it is providing should be available all the time, which means there has to be some notion of fault tolerance of some kind and partition tolerance, and that is the P of the cap. Partition tolerance means since it is a decentralized system, so if some part of it becomes offline, even then the system should be able to work.

And we will see that CAP theorem of Brewer is actually pretty much fulfilled or satisfied by IOTA. There is no fees involved in this tangle. And then it is scalable. It is modular. It is modular in the sense of partition tolerance. We will see that it is quite lightweight. And offline transaction is allowed. Actually modular, offline allowed partition tolerance, these are actually different facets of the same thing.

And then the cryptography to users is actually more quantum resistant cryptography, then what we saw in case of a bitcoin or Ethereum.

(Refer Slide Time: 46:24)



Envisioned Use cases

- Complete M2M communication
    - Anything which has computational resource (Chip) can be leased by another machine autonomously
    - Devices can share resources by coordinating – bandwidth sharing for example
    - Supply Chain
    - Smart Grid to coordinate production of energy without human dispatching
    - On-demand API access
    - Sensor Data Selling and Data Market Place
    - ....

So what are the use cases for this? So as I said, the use case that is more close to my mind is that borrowing computational resource from one machine by another. So if I want to have a computation, I do not have the computational resource. I offload that to another machine which has the computational resource and instead I pay. So bandwidth sharing, for example, I could, I may need to urgently send some information.

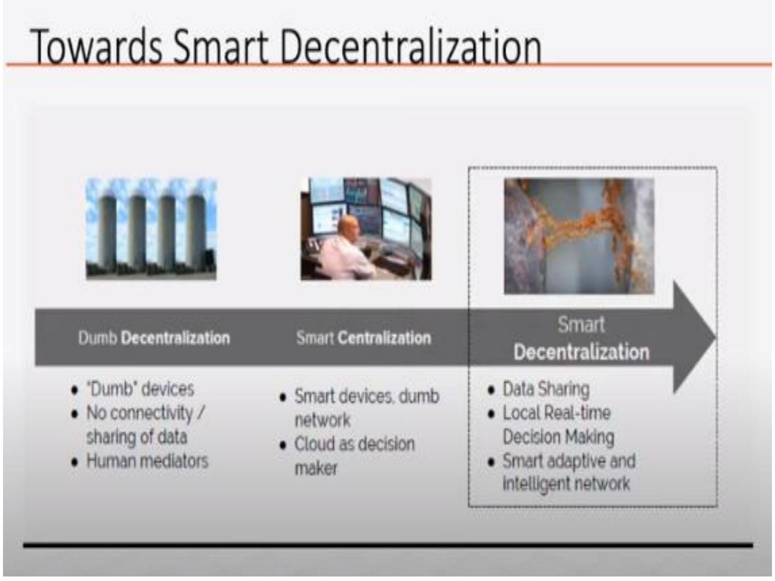
And I do not have the bandwidth. So I ask a neighboring node to actually use its bandwidth to deliver or broadcast or communicate that information, which is same as computational resource sharing. It can also be used to keep track of supply chain, in case of smart grid to coordinate production of energy without human dispatching, on demand API access.

So I have a device which needs to use some API let us say for example, in most cases, I can envision if this devices are also using some kind of a machine learning based decision making, then they might not have the ability to call on an API directly on their own resources for let us say, calling a machine learning model, but they can ask another higher resource device to do that for them.

And then you can also do various kinds of data, business data marketplace. Devices collect a lot of data. And you may want to monetize that data, which is not happening that all that much now but it is going to happen lot more. So devices, which are collecting, let us say solar irradiation data in a smart solar panel system.

This data can be actually monetized and people actually do sell this data but not autonomously, like what is envisioned here. But more by dumping that data in a database and then the owner of the database can sell that data to researchers and other companies that make solar related products. So this is the kind of things that we envision as the users of the IOTA system.

(Refer Slide Time: 49:15)



Towards Smart Decentralization

Dumb Decentralization

- 'Dumb' devices
- No connectivity / sharing of data
- Human mediators

Smart Centralization

- Smart devices, dumb network
- Cloud as decision maker

Smart Decentralization

- Data Sharing
- Local Real-time Decision Making
- Smart adaptive and intelligent network

So decentralization, so few words about decentralization. So it turns out that in the old days, you have an industry and you have devices, but devices do not communicate with each other. They actually or communicate very locally. So they are not connected through a network. They may directly hardware to a controller, so they can send some data to a controller but not send that data elsewhere.

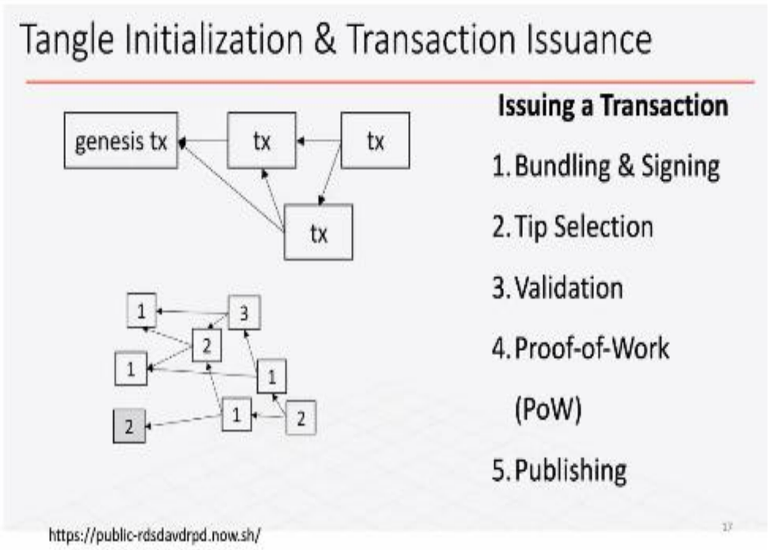
And most of the time, the human operators will use that whatever data they are seeing on let us say, an HMI interface or human machine interface will then intervene to actually use the data collected by the device. So smart centralization came when smarter devices started appearing in the market, which can send its sensed information which can be sent actuation information.

And there the network does not have to be very clever. It is only a mediator through which this information flows. And all the information may actually go to a cloud and the cloud may do all the necessary computation for decision making and then send the actuation information to the devices. So that is a very centralized solution, or smart centralization.

So dumb decentralization was not very smart. So this is basically I would say, industry you know 2.0 or between industry 2.0 to industry 3.0. Smart centralization is more like industry 3.0. And then we are talking about smart decentralization where devices share data. There are local decision making, which is real time. And then smart adaptive and intelligent network. And this is actually what we are envisioning, as industry 4.0.

And this is where we will see this kind of a situation, the use cases that we were talking about in the previous slide, and this is where the IOTA could be very useful.

(Refer Slide Time: 51:47)



Tangle Initialization & Transaction Issuance

Issuing a Transaction

1. Bundling & Signing
2. Tip Selection
3. Validation
4. Proof-of-Work (PoW)
5. Publishing

https://public-rdsdavdrpd.now.sh/

17

So let us now dive into Tangle, right. So in Tangle, there is this directed acyclic graph which looks like this. So you have, this graph starts with a node called the genesis transaction. And the genesis transaction actually, is where a pot of money, they are called the IOTA or IOTA coins, they are created. And then they are distributed through this transaction to a number of entities to in order to bootstrap the system.

So certain devices might actually be given some amount of IOTA, and IOTA, unlike bitcoin or Ethereum there is no notion of mining. So the first genesis, we create a pot of money, and that is all the money that it will have through its, you know life cycle, however long that life cycle goes, because money will keep changing hands and that is how the entire system will run.

And therefore, there is no way. Of course, one can also purchase from one of these devices or you know some of this through fiat currency through an exchange which accepts IOTA to fiat currency exchange, but that is all but there is no new IOTA coin that will be created. And then when transaction starts getting created, say devices want to make transaction they have to choose at least two previous transactions and validate them and then they add themselves into this graph.

So for example, this transaction cannot obviously have two transactions to validate because it before it, only genesis transaction was available. So it basically validates the genetic this genesis transaction. And when I say validate it basically at this point, it only can validate the signature and stuff like that, there is not much to validate here. The genesis transaction might have given some money to various devices.

And it may might want to check that is actually not conflicting or something. But then a new transaction come in and this transaction has now two transactions which both of which it can validate. And that is what these two arrows mean that this transaction validated these two transactions.

Now another transaction comes almost concurrently and then this transaction chooses to validate this transaction which already has been validated by this transaction, but there is no harm in this guy validating this transaction and he also validates this transaction. So this is how the Tangle grows. As transaction come they look for two unvalidated transactions so far and then they validate them and then they attach them to those two transactions.

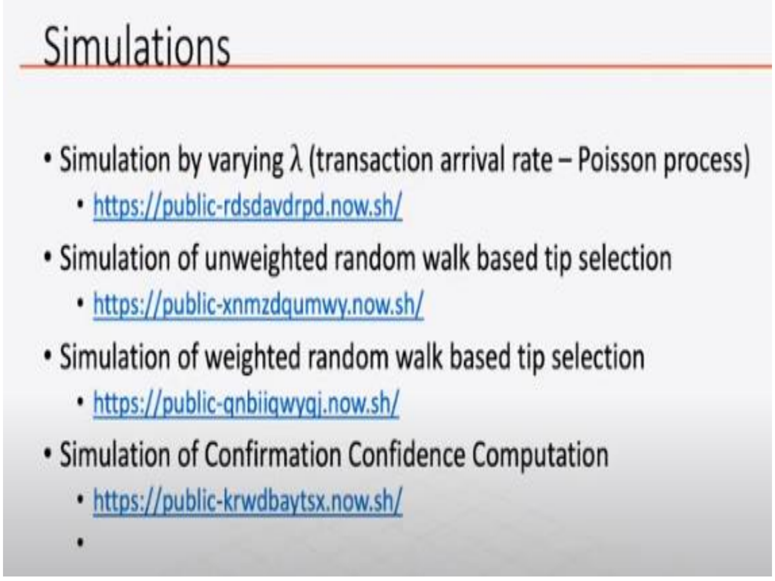
Now the transactions that they validate which are yet in not validated by anybody else are called the tips of the Tangle. So all the other transactions which are basically nodes in this graph, which has been validated by at least one transaction is called is an internal node whereas the nodes are transactions that have not been validated yet by any other new transaction are called the tips.

So and the transactions are actually bundled and signed by digital signature which is the done by the issuer of the transaction. And then, the as the new transaction comes in, it has to first do a tip selection. And we will talk about how this is done, the tip selection, and then we will talk about the validation, how they validate the two transactions or in some cases one transaction that it has to validate.

Now it also has to do a small proof of work. And this is because the, for a transaction to actually go into the tangle, it has to complete a small proof of work. And this proof of work is there in order to stop spamming. So what is spamming? Spamming means that a device may decide that I will create some meaningless transactions and just make the Tangle bigger, right? So it might go rogue, and it can start doing such things.

So we do not want that to happen. So therefore, we have to put some computational burden on the transaction created so that they do not start pumping out meaningless transactions. And then once the transaction is has passed all this then it will be published in the sense that it will be part of the Tangle and then anybody who has a copy of the Tangle, can see that **this is** this transaction has already made into this.

(Refer Slide Time: 57:26)

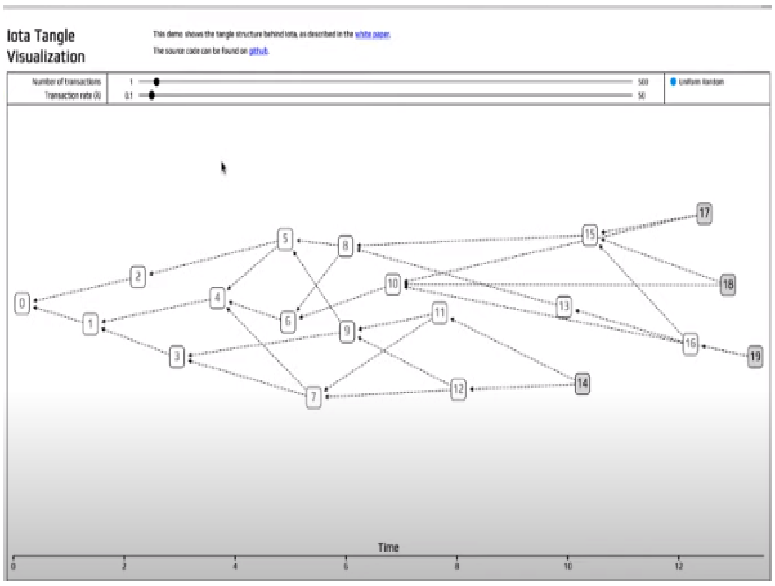


Simulations

- Simulation by varying λ (transaction arrival rate – Poisson process)
    - https://public-rdsdavdrpd.now.sh/
- Simulation of unweighted random walk based tip selection
    - https://public-xnmzdqumwy.now.sh/
- Simulation of weighted random walk based tip selection
    - https://public-qnbiiqwyqj.now.sh/
- Simulation of Confirmation Confidence Computation
    - https://public-krwdbaytsx.now.sh/
    -

So there are several simulations that I want to show you. So here is the simulation of how a Tangle actually starts growing.

(Refer Slide Time: 57:44)



Iota Tangle Visualization

This demo shows the tangle structure behind iota, as described in the white paper.

The source code can be found on github.

Number of transactions 1 500

Transaction rate (λ) 0.1 50

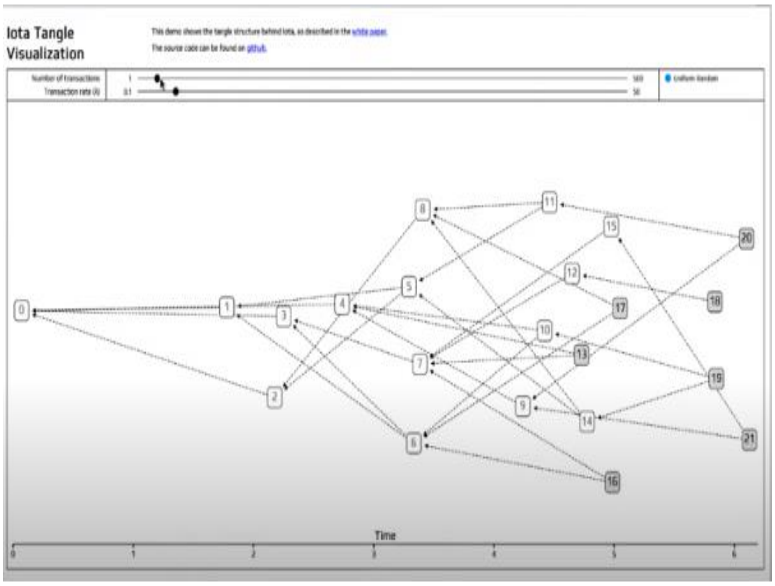
● Uniform Random

I do not know what is happening here. Okay, so here in this simulation, let us say the number of transactions is just one, right. And then I have a transaction rate, which is the rate at which transactions are created. You have many devices, each device may do its own transaction with another device, or you know they might just not do anything.

So here the transaction rate we have considered here is 0.1, which means that every 10 seconds, one transaction comes in. Now I increase the number of transactions from one to two, right? So the first transaction will find zero as unvalidated yet so it will validate it and do its proof of work and gets added. So now I have I add another one. Now 2 comes in and starts validating.

So it could have validated zero also but it decided to validate only 1. So here I do it another time. This is randomized simulation. So in this time it decided to validate zero. So now I have 3, now 4, 5, 6, 7 and this is how the tango starts growing.

(Refer Slide Time: 59:37)



Iota Tangle Visualization

This demo shows the tangle structure behind Iota, as described in the white paper.

The source code can be found on github.

Number of transactions 1 — 500

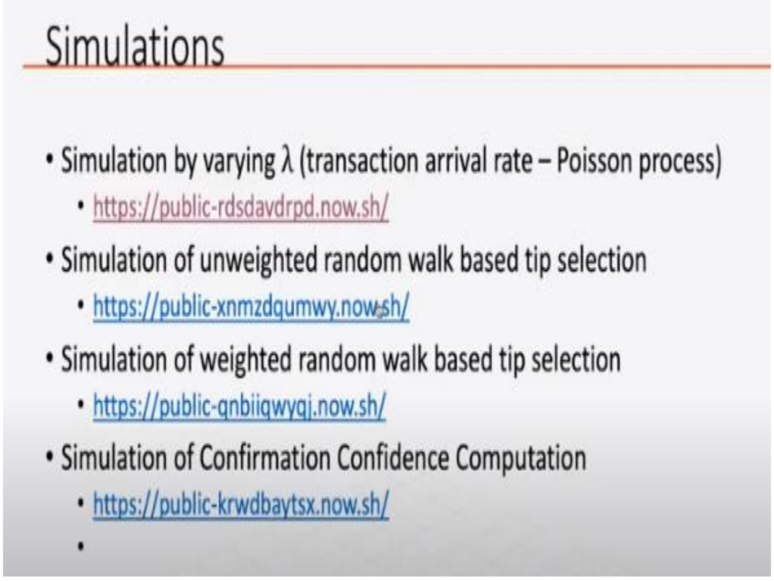
Transaction rate (λ) 0.1 — 50

● Uniform Random

Now if I change the rate and I make the transaction rate very high, then the shape of the tangle will also change because more transactions that come in at the same time, if they come one by one, then they will find few tips. But if many transactions come in together then number of tips or invalidated transactions, they will find many. So there will be a lot of different variety of transactions to choose from for them to attach themselves to the transaction.

So the shape of their Tangle will depend on two factors. One is the number of transactions and the rate at which transaction come and this is how the transaction will grow.

(Refer Slide Time: 1:00:28)



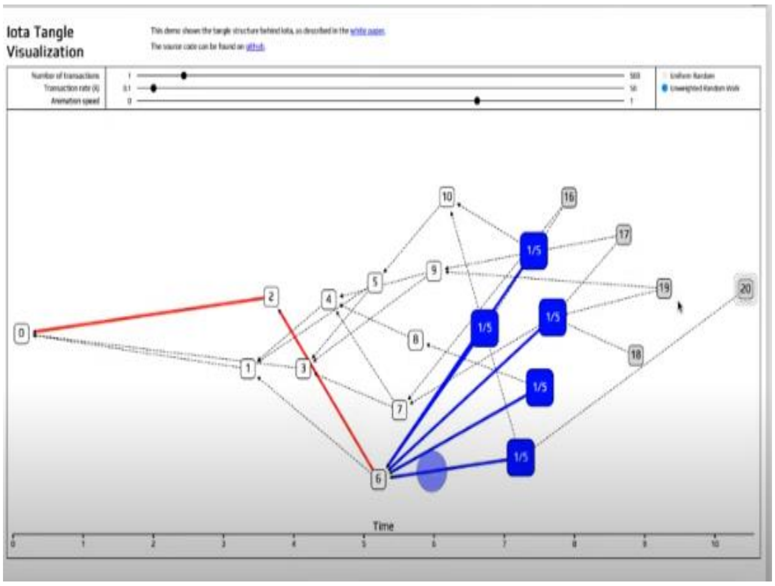
Simulations

- Simulation by varying λ (transaction arrival rate – Poisson process)
  - https://public-rdsdavdrpd.now.sh/
- Simulation of unweighted random walk based tip selection
  - https://public-xnmzdqumwy.now.sh/
- Simulation of weighted random walk based tip selection
  - https://public-qnbiiqwyqj.now.sh/
- Simulation of Confirmation Confidence Computation
  - https://public-krwdbaytsx.now.sh/
  -

Now the second thing is that, how does it choose which tip to attach to, right? So there are let us say I have five tips and I only need two tips to select to connect myself to the Tangle by validating them. So there are a number of different possibilities. So first thing we would like we will look at is what is called an unweighted random walk based tip selection.

So what happens there is that when I am a new transaction, by the way I have access, I have access to the entire tangle that has been made so far.

(Refer Slide Time: 1:01:08)



Iota Tangle Visualization

This demo shows the tangle structure behind Iota, as described in the white paper.

The source code can be found on github.

Number of transactions 1 — 500

Transaction rate (λ) 0.1 — 50

Animation speed 0 — 1

○ Uniform Random

● Unweighted Random Walk

So here, I have the animation automated, so the animation is happening. Now what you are seeing here is that what when a new transaction is coming, it starts from the genesis, it does a walk from the genesis block. And what it does is that in the in this unweighted mechanism, for a random walk, it basically gives equal probability. So it is in zero and it has right now three paths from zero.

So it gives equal probability and chooses one of them. Then it once it chooses 1, it comes to this node there it has, let us say 1, 2, 3 again probability. So each has one-third probability. Then it comes to this one. And this 1 has also two at least I see two outgoing, so it will have a half of probability of adding to the next one. So this way it will walk all the way from genesis to the whichever tip it ends in, after which it cannot proceed, because there is no more path. So then it chooses that tip.

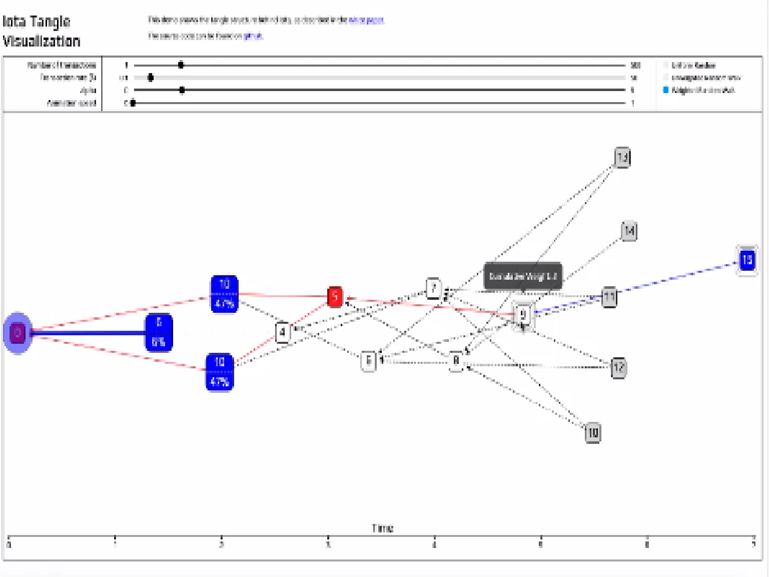
And then it does the same thing again, so that it can choose the second one. So this is what is called the unweighted random walk. So unweighted random walk is a process by which the tip selection happens. But in this case, the tip selection creates something called lazy transactions, lazy tips. Lazy tips are tips that basically goes and does not validate some new tips.

So a new transaction comes in and it does not do all the work. To find some new tips, it goes and does validate some already validated old transactions. And that is not desirable because we want that all the transactions to be validated. Now if every tip comes and validates, let us say zero, then every new transaction comes and validates zero, zero has already been validated several, by several node several transactions.

So it does not make sense to do that. So therefore, we have to have a way to penalize the new transactions that does this. So therefore, equal weight towards all directions at every intermediate node, while doing the random walk towards a tip is not a good idea, because then the lazy tips will also get validated with very good probability. So you want to reduce the probability that if a tip is lazy, it should not be allowed to be validated.

And therefore, if it never gets validated, the transaction never makes it to the permanent record. So that is what we want to do. So therefore, what we do is we do a weighted random walk based tip selection.

(Refer Slide Time: 1:04:23)



So weighted random walk based tip selection basically assigns different weights to the different directions, when it is on an intermediate path. So you see that here it is doing equal number of probabilities, equal probabilities. But now you see, there is a difference 33, 33, 33 and then as it grows more you will see we saw just 45,27, 27 and so on and so forth, right. So the question is that how does it decide what is the split, right.

The split has to be some algorithm right. So it cannot randomly say this is 23rd, 232% that is 38% and so on. So I have to have let us reduce the animation speed here. So you can have a better look at the numbers. So increase it a little more. So here you see 42, 42, 16. So when it comes it obviously will come towards 42, 73 and 27. So it will certainly high chance it is going here and so on and so forth.

And this is based on the notion of a cumulative weight. The cumulative weight of a node is based on how many transactions have already validated a particular transactions, and then that plus one. So we will discuss this lot more. And then based on the all the cumulative weights of all the nodes that are that you branch out to, you can then split the probability based on the in proportion to the cumulative weight of the nodes that you are connected to.

So here you see that this guy has a cumulative weight of 10, this has a 10, this has a 6. This guy has a 6 cumulative weight, this has a cumulative weight of 4. And this guy has a cumulative weight of 1, this guy has a cumulative weight of 4. So why is it has a cumulative weight of 4? Let me stop the stop this and look at this. So what is the cumulative weight here?

The cumulative weight here now is 2, because it has been only it has been validated by 1 and nobody else. Now 8 has been validated by 14, 13 and it has been validated by 10. So 3 validated it. So it has 4 cumulative weight. This guy has a cumulative weight of 7, because 2 have validated it, but those two have been validated by others. So 4 and so it has 4, and this guy has been validated by, so this is cumulative weight 4.

This is cumulative weight of 2. So 4 and 2 six. And then plus one is cumulative weight of 7. So this is 7, and let us say this is 5. So the probability between these two will be in the 7:5 ratio. So that is how the your tilting your path in the tip selection towards the nodes that have a higher cumulative weight because they have been already been validated by many more different new transactions.

So then finally, I want to show this animation which is about the what is called the confirmation, confirmation weight or confirmation score. So or confirmation confidence. So what is the confirmation confidence? Confirmation confidence is basically say the genesis node. It has been validated by couple of transactions right after they came after the genesis node.

But those nodes have in turn been validated by other nodes and those nodes have been validated by other nodes. And one thing I forgot to tell you is that when I validate a transaction, I have to make sure that whatever transaction that guy has validated is also valid. So therefore I basically do an entire history of the nodes. The node I am validating or the transaction I am validating has validated some other transaction which in turn validated other transactions.

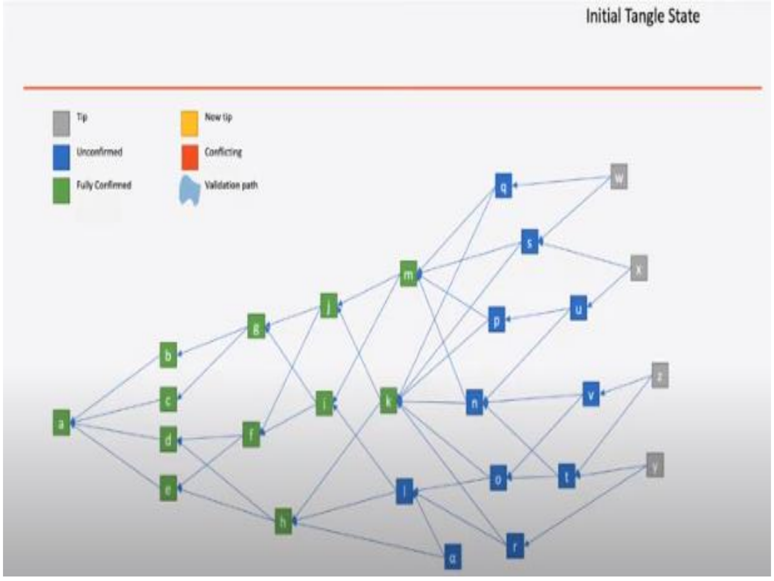
So every time I validate a transaction, I will not only validate the that particular transaction but any transaction that this transaction has validated and in the transitive manner. So therefore, the genesis node has been validated after some time. The genesis node has been validated by all the current transactions which has been attached to it. So the confidence that the transaction recorded in the genesis transaction is very high.

Whereas something that is in the tip which has not or close to the tip, it has been only validated by maybe one or two other transactions and not by very many others. So then I will say that the that one has not been the confirmation confidence is not very high. Now why do we need this confirmation confidence? That is because I may decide that say I put a transaction and I may want to do the result of the transaction.

So I got some money out of this transaction. I am a device and I got some IOTA coin, because I gave some resources to you and then I want to spend that resource for getting another resource. So I put another transaction. But that transaction, you know may or may not be trusted by others, because the previous transaction on which you depend on to put this transaction on is not necessarily very high of very high confidence.

So I have to wait until the high confidence increases. So now we will we will go back to some more illustrative example.

(Refer Slide Time: 1:11:11)



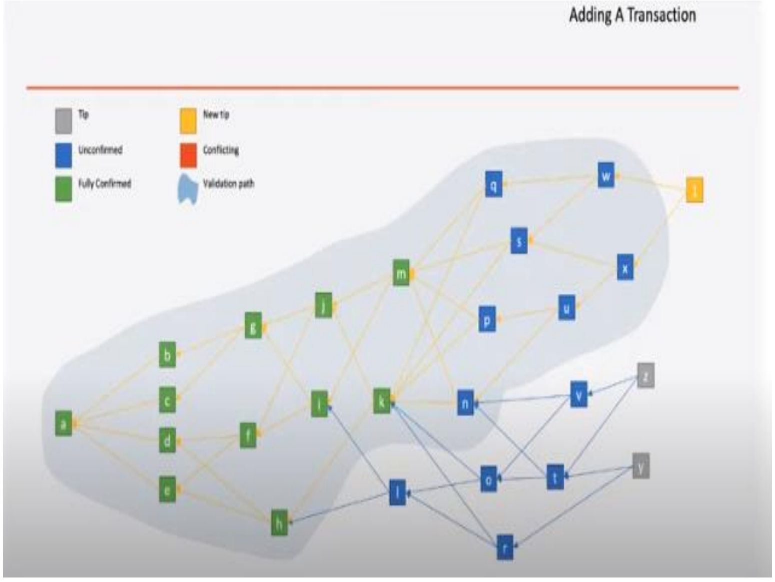
Initial Tangle State

So in this picture, so I have let us say this is the Tangle state in which I am looking at this. When I look at this and I see that some of the transaction nodes are painted green, and then the some are blue and some are gray. So the gray ones are tips. They have not been validated by anybody yet. So obviously, we cannot have any confidence in their confirmation because they have not been confirmed by anybody.

But the green ones for example b, b has been confirmed by g, g has been confirmed by j, which then in turn had to confirm b; j has been confirmed by m and m in turn confirm g and that in turn confirmed b. And then m has been confirmed by q. And that means in that process has confirmed v and w has confirmed q which in turn that process confirmed b.

So b has been confirmed many times and therefore, I would say that b is of high confidence. Whereas, or after a certain high confidence is reached, I will say that this is fully confirmed, whereas this blue ones, they have been only confirmed by few and therefore, they are not completely confirmed yet.

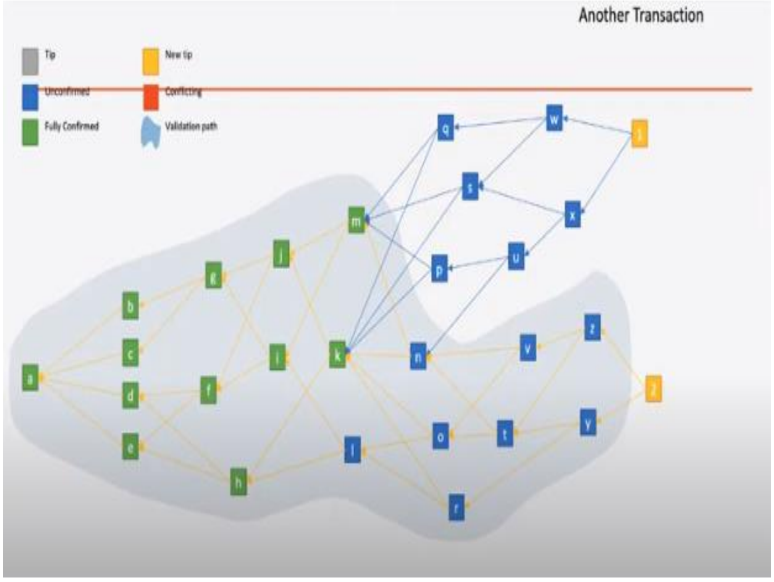
(Refer Slide Time: 1:12:45)



Adding A Transaction

So when I add a new transaction now let us call it 1, which confirms w and x. And in the process, it conforms all the ones that are in this shaded region, because they somehow in turn has been confirmed by either x or w, right.

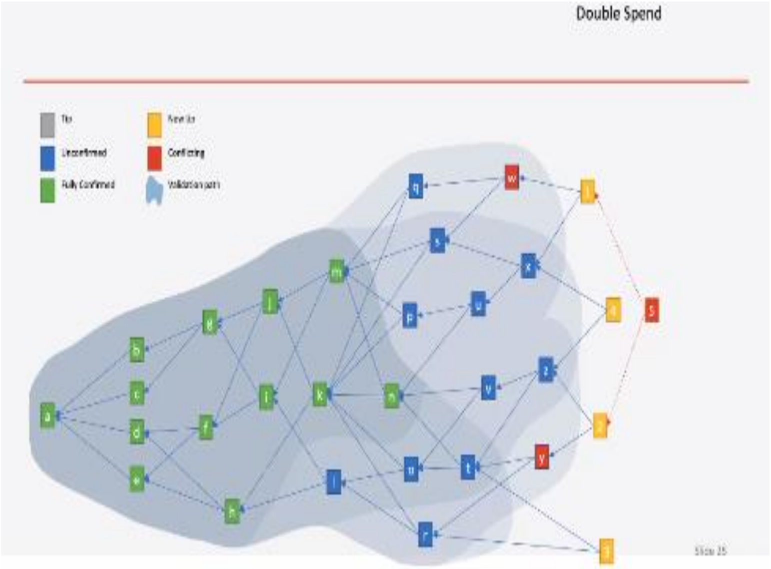
(Refer Slide Time: 1:13:11)



Another Transaction

So now another transaction I and 2, which actually confirm z and y. In that case, what I will do is I will have this ones that had confirmed indirectly by z or y I will consider them as having a higher score of confirmation confidence.

(Refer Slide Time: 1:13:36)



So this way, I will keep doing this and if you take them to overlap, then you will see that the node n has been now added into green because it has reached the enough number of confirmations. So in my first picture if you look at n, n was blue, right. So only m and k were Green. But then after one and even after one has been added n is still blue, but then n has been now confirmed another time by addition of 2 and therefore n will now turn green.

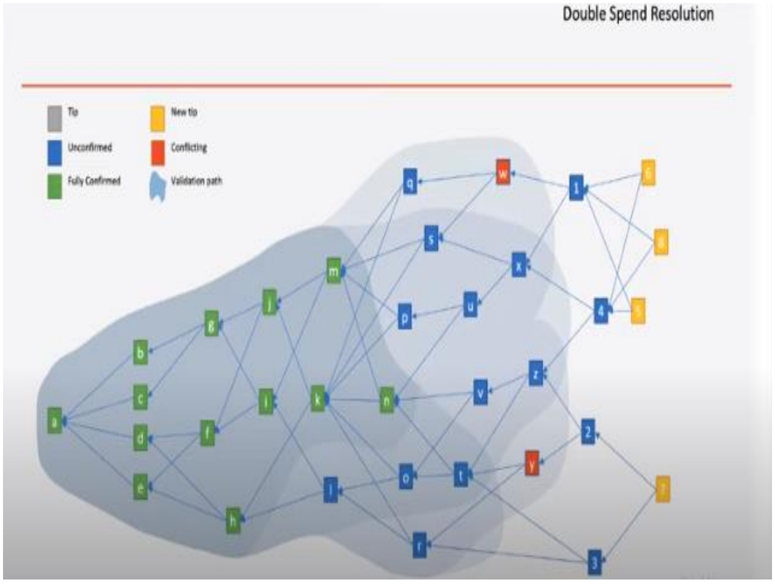
Now one issue is that. So this way if more and more new transactions come in, things get more and more confirmation, and therefore, their confirmation levels go up and eventually more ones turn green. Now there is one issue that can happen, which is the problem of double spending. Let us say w is spending a coin that it has gotten and from a previous transaction and y is doing the same thing.

And then 2 confirm z and y and 1 confirm w and x. So 1 did not know the existence of y similarly 2 does not know the existence of w. So they are double spending, but still has been confirmed at least by 1, one transactions. But this will not work very long, because soon after, as more and more transactions get added, some transaction will choose 1 and 2 together.

Or some successor of 1 and 2 together and at that time, they will they have to go to go through the entire history and then they will find a conflict w and y and therefore, w and y will no longer be in the path and anything that depends on w or only w may stay or y may stay. So that will depend on how people decide. So obviously 5 will obviously not continue to validate this.

So 5 will then choose 1 and 4 maybe. And then this part the part of with 2 will get orphaned. So this will keep happening.

(Refer Slide Time: 1:16:15)



Double Spend Resolution

Tip

Unconfirmed

Fully Confirmed

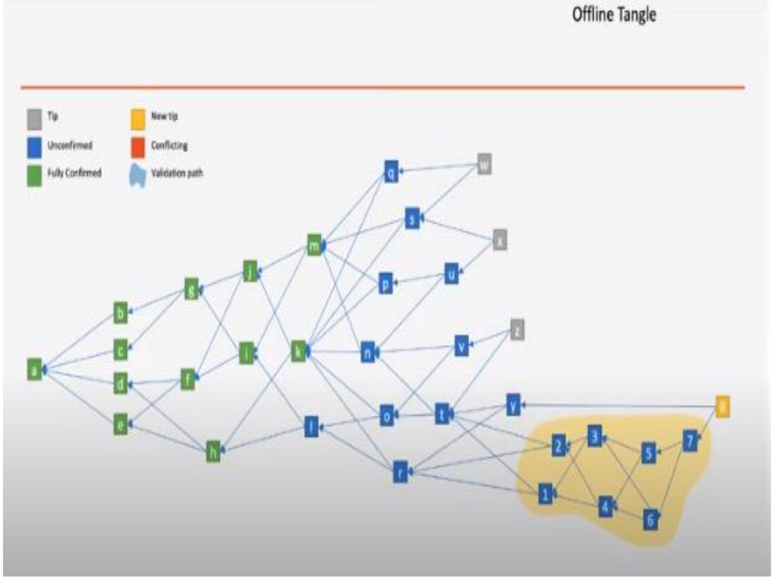
New tip

Conflicting

Validation path

So this is how the confirmation level of y will not increase anymore, because after a while everybody will flock towards the upper side and then the in the lower side y will not remain very active. This part will not remain very active and therefore y will actually lose in gaining any more confirmation confidence. So this is how the double spending is resolved in Tangle.

(Refer Slide Time: 1:16:50)



Offline Tangle

Tip

Unconfirmed

Fully Confirmed

New tip

Conflicting

Validation path

So then the one last thing I want to say is that suppose I have a part of the network that get segmented. So let us say I have a transaction. This yellow part that you are seeing is actually 1 and 2 started by having validation of t and r and but at that point they got disconnected from the rest of the network.

And then that does not stop its own partition of the network to keep transacting and in order to go back to the intertangled when the partition gets rejoined again, a new transaction has to come in to add to validate together the last transaction or tip of the offline transaction and tip of the online transaction together and then they will get connected.

Now if there is a double spend in this yellow region with the any of the nodes on the previously the online part, then after some time, that will be again be caught like we showed earlier between w and y. And that is how they then one of them will stop getting any more, stop growing and their confirmation confidence will stop growing, and therefore they will never become green. So that is the idea of having the offline Tangle.

So what we see from this is that the consistency in terms of resolving conflicting transactions, the availability in terms of having the ability to survive, making transactions in case of a network partition or becoming offline and the partition tolerance, that is if the network gets partitioned, the part of the network that is partitioned out, can still continue having the growth of transactions.

And later on resolving the consistency as it gets joined back in, all these things are satisfied. So CAP theorem in some sense holds for this Tangle framework. So that makes this one quite powerful. So this is all I am going to talk about IOTA because this is, you know one can of course go on having very long sessions on IOTA, going through how this proof of work works here, how the what the transactions look like, what the and then maybe having some more coding examples, etc.

But that is not the point of this class. The class is to just give you ability to see between different paradigms, even within the blockchain technology, the different paradigms, the difference between customized for a specific kinds of application versus more generic type of blockchain. And then the fact that the blockchain is not necessarily always a chain, but it could have a different structure.

But it uses very similar concepts of transaction, transaction validation, some form of consistency making and in this case, even further partition tolerance and availability. So all this together gives you a very good sense of a different paradigm which will help you to actually articulate when somebody asks what kind of blockchain I should use, here is my problem scenario and here is the here is the constraints and here is what I want to achieve.

Then you should be able to at least give him a good informed advise on what might suit his cause the best. But more than that, what you would be able to do is that, once you actually start programming, you know either in Ethereum or Hyperledger or any other blockchain framework forum or whatever, you will actually be aware of all the different paradigms.

So that you can see that whether you have made the right choice in terms of choosing the platform, choosing the architecture of the application, choosing the way you do consensus, etc. So that is what the goal is. And from that point of view, I think this is sufficient information that you need about the IOTA blockchain. So when we come back, we will be talking about the other blockchain that is the Corda.

And that probably is a very different paradigm. Not probably, that is for sure a very different paradigm, a quite a bit customized for financial applications. And that should give you a very different taste of a different paradigm. All right, so when we come back, we will see that. Thank you.