

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

Lecture- 19
Blockchain for Enterprise – Overview

Hello everyone I am Praveen Jayachandran from IBM research in India, I am delighted to be here to be teaching this online course on Block chain with Professor Sandip Chakraborty from IIT Kharagpur. Since it is the first lecture I am teaching for this course, let me start with the brief introduction about myself, I lead a team of researchers that are India research lab in Bangalore.

We been working with block chain technology for about 2 and half years, now let me tell you little about that journey itself. So, we been following this space for quite a while than the in 2015, we really saw the potential of the technology for various industries. And we were looking at some of the existing platforms and some of the solutions that were being built at the time.

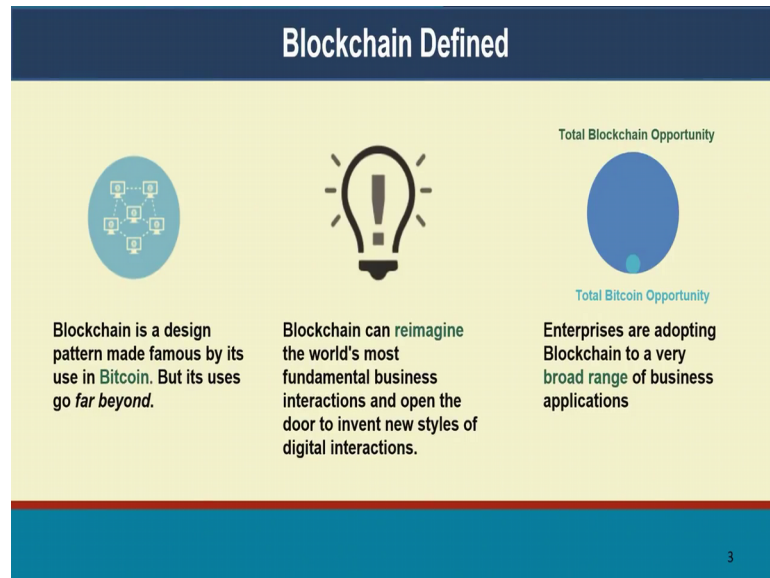
And we realise that none of them were really well suited for enterprise applications, they did not have the kind of security and privacy that, we wanted they did not have the kind of scalability throughput requirements that, we needed and many other enterprise requirements that we will talk about more than next few lectures. So, we at the time decided that we are going to build a platform of our own I was fortunate to be one of the first developers on that project.

And since then that project is grown manifold and we have contributed that to what is now hyper ledger fabric. So, we will talk about hyper ledger fabric at length over the next few lectures, and since then over the last couple of years my colleagues and I have also been involved with various clients building some of the first production grade enterprise block chain solutions, that are there are running out there with clients today.

So, along the way I want share a point of view of where enterprise is looking at ah about this technology and give you some of that perspective. So, with that let us get started. So, the first lecture is going to be just talking about what is the need for block chain and

enterprise, what are some of the requirements and a high level overview of that of this, from an enterprise stand point what the technology means for industries.

(Refer Slide Time: 02:20)

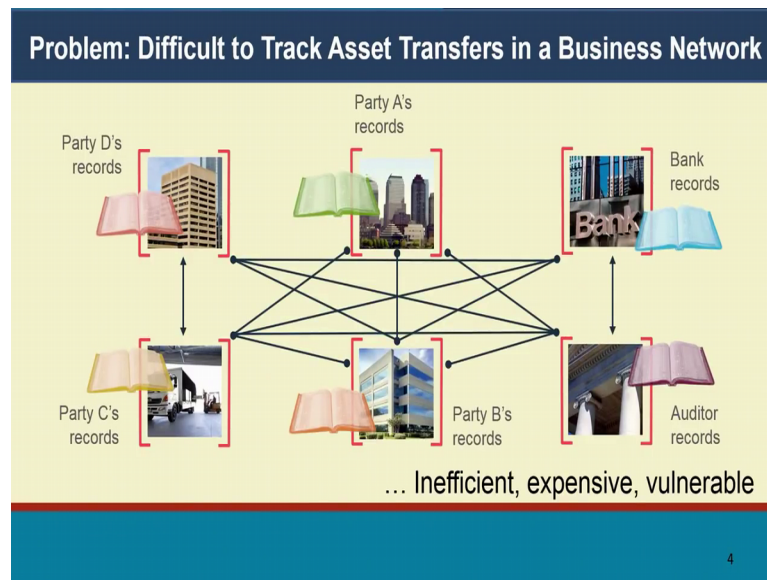


The slide is titled "Blockchain Defined" and is divided into three columns. The first column features a circular icon with a network of nodes and the text: "Blockchain is a design pattern made famous by its use in Bitcoin. But its uses go far beyond." The second column features a lightbulb icon and the text: "Blockchain can reimagine the world's most fundamental business interactions and open the door to invent new styles of digital interactions." The third column features a large blue circle with a small blue circle inside it, labeled "Total Blockchain Opportunity" and "Total Bitcoin Opportunity" respectively, with the text: "Enterprises are adopting Blockchain to a very broad range of business applications". A small number "3" is in the bottom right corner.

So, first of all I think with the last view like just you would have learnt about Bitcoin and I think it is been extremely popular, it is all over the media lot of start UPS in this space lot of venture capital funding for Bitcoin as well as block chain, but I want to highlight this difference you would have already heard about this we see Bitcoin, as just one application of the underlying technology itself.

And the technology is much more powerful than just the Bitcoin application. So, the overall opportunity for block chain expands to multiple industries its for financial services for supply chain for logistics, for health care there are host of applications, we will talk about those as well and all of those go much beyond just crypt crypto currency or Bitcoin that it is looking at. Now, I wanted to highlight that before we get into what really this means for enterprises.

(Refer Slide Time: 03:17)



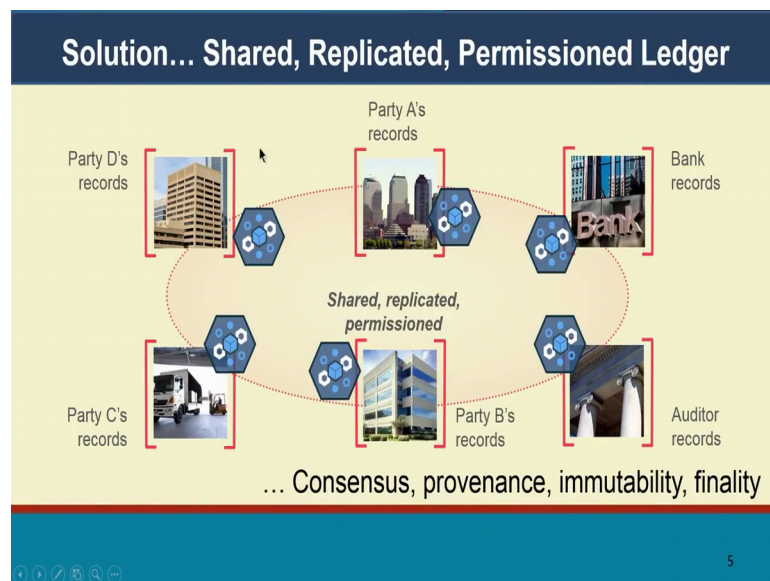
So, let step back may be 20 25 maybe even thirty years right when the internet was really picking up. At that time what the internet really did for enterprises was that it really made communication extremely simple right, it made it easy for people to digitize and automate their processes, and it made communication between a organisations very very simple. So, we moved away from pep having to use paper and having to use other physical modes of communication to mode digital modes. So, you could send messages, you can send the, you can have a protocol that part is execute between themselves.

So, what this meant was let us take a example right, let us take the how the payment system works today with banks, today if I am to send let say hundred dollars to a bank in the US, recipient may be a friend of mine in the US, then I instruct my bank in India to transfer that 100 dollars to my friends bank in the US.

And it is not really just these two banks that are involved, what ends of happening, there are probably 5 or 6s other banks in between that all get involved in this in this transaction. And all of these become point to point communications, what I mean by that is my bank in India talks to another bank B and then bank B talks to bank C and so, on. There are may be 5 or 6 hops and the money then finally, eventually reaches my (Refer Time: 04:46) my friend at the other destination. This becomes very inefficient very expensive and is also vulnerable, because there could be failures along the way, and then they have these failures have to then be manually reconciled correct.

So, we are looking at these many point to point interactions that are happening in the current enterprise echo systems. And this is true even for the let say the supply chain industry, you can think of it as let say there is a supply or who is supplying certain let say automobile parts to a manufacturer and there may be other logistics providers there may be a bank involved for finances, all of these become point to point interactions in today's world and that becomes very inefficient and expensive.

(Refer Slide Time: 05:30)



So, we want to move from this kind of very complex interactions point to point interactions, to this world where all of these enterprise users they are all doing business with each other today, we want to bring them altogether into one common platform, where they are able to share information in a secure manner right amongst all of these participants.

So, this is where the block chain really comes in. So, what the block chain provides is a mechanism by which multiple enterprises can come to a common shared platform, where they can exchange information with one another this is all business information, for executing their business processes. They can exchange business information amongst one another in a shared secure manner. And what happens is everyone in this equal system, whoever you need the to know about this piece of information, we will immediately get excess to this information.

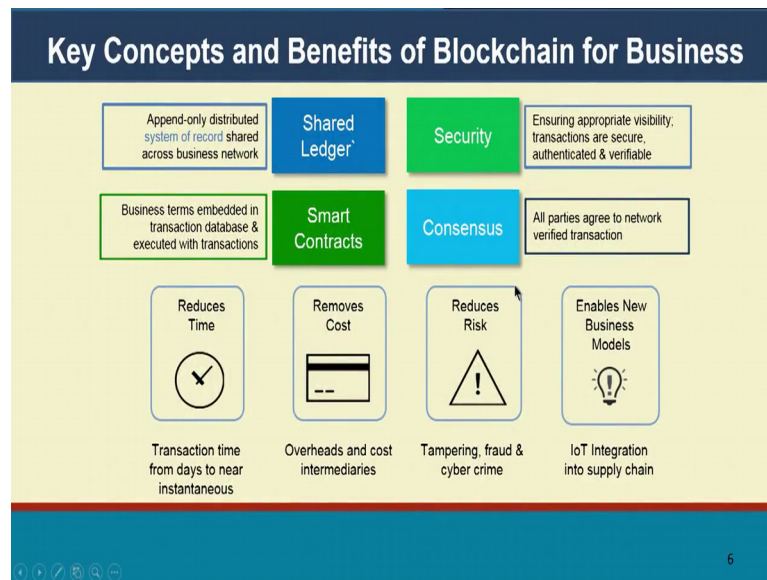
So, in some sense every node in this block chain network is going to store replicated copy of all the information that is getting transacted. So, think of each exchange of information being a transaction and, this transaction is going to get recorded on the block chain. So, all of these nodes are the participants of the block chain they are going to record it on what we call their ledger, these terms you would have heard in the Bitcoin context as well.

But I am going to introduce this from an enterprise context. So, all of these participants in the equal system are going to store this to these transactions you know completely immutable log it is an append only log. So, you can only add transactions to this ledger, you cannot tamper with previous transactions. And how these transactions get added on to the ledger is through a notion of consensus here.

This is so, the consensus is an important notion here, where all the parties agree that this is a legitimate transaction that needs to get added to the ledger and they all simultaneously in a consistent manner add the transaction on to the ledger. And what this completely auditable fully immutable log gives you is provenance. So, you have a full log of every transaction that is happened in the sequence system and everyone has this copy.

So, no one can cheat another party and say that this transaction did not happen, or I did not perform the transaction. So, none of that is possible it gives you a sense of immutability. So, no one can change this in the future and it also gives you finality. So, once the transaction is performed it is there for forever right, everyone can see that the transaction was performed. So, this is the overall system and this ensures that we can significantly reduce some of the inefficiencies that exist in multiple echo systems today ok.

(Refer Slide Time: 08:03)



So, what are some of the key concepts right? So, we talked about a shared ledger amongst all the participants in the network. So, this is an append only distributed system of record of all transactions that are being performed on the network by any participant. So, that is the shared ledger so, think of this as may be some of the distributed systems concepts that you might have studied in other courses and, how this ledger is maintained in a consistent manner across all the participants is through a notion of consensus.

So, this is a protocol that all the participants will perform, it is an exchange of messages and they all agree that this is a valid transaction that can be added on to the network. And apart from these notions there is also a notion of security some of these notions are not there in the Bitcoin block chain, where we want a ensure that only certain participants can see certain pieces of information, or they can only perform certain kinds of transactions.

And all of these transactions are secure, they are authenticated and their verifiable and there are many notions of privacy that, we are also introduction interested in we will look at some of those notion in subsequent lectures. And, we also want a make sure that this is auditable right may be even a regulator can come in and see that all of these transactions are performed by valid users, they are all authenticated proper transactions to be performed on this business network and they can admit these transactions.

This is very different from how Bitcoin taught about block chain and, another important aspect that we are interested, in is the notion of smart contracts. So, apart from exchanging information amongst participants in the network, we are also interested in executing business processes. And these are captured as what we call as smart contracts.

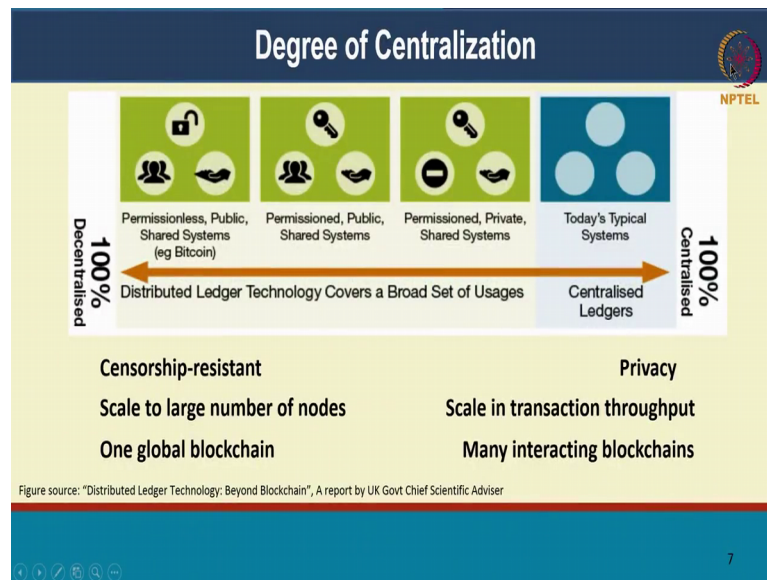
So, this is a let us say the logic or a piece of code written in traditional programming languages perhaps, that you can execute in a decentralised fashion. So, all of the nodes in the network will actually execute this transaction, they will compute the output state. And the output state will then get recorded on to the ledger, if this is a valid transaction.

In the Bitcoin world again just as a comparison, the Bitcoin executes a very static smart contract, this is exactly one smart contract and it does not have the ability for you to embed your own smart contract. And that smart contract in Bitcoin is just being able to determine who the owner of a particular Bitcoin is or who transferred how many Bitcoins to another person. So, that is the asset management in transfer is the only kind of thing that you can do in Bitcoin.

Whereas, we are looking for a much more richer set of transactions and business logic that we want to embed in to some of these transactions and, what do these all of these put together is what we call a block chain right. And it putting these together is really the big acknowledged advancement that we have come up with block chain together as a community, it helps reduce time for executing some of these transactions, what was previously very manual process is can now be automated.

Across organisations it helps remove cost it helps reduce risk and, it also enables new business models right, we will when we talk about some of the solutions that have been enabled by block chain, we will look at some of these new business models.

(Refer Slide Time: 11:19)



So, now again setting things in perspective of how you think about Bitcoin versus, how we want to look at enterprise block chain applications, you can think of the right hand end of this picture, as something that is 100 percent centralised right. So, here this is our typical old distributed systems where it is just one organisation that is the executing the entire a application or your system.

And it is a centralised system of record so, that is at one end of this spectrum. The other end of spectrum is where maybe Bitcoin and some of the other permission less systems belong, where it is completely decentralised, anyone can join the network anyone can execute transactions and anyone can see what is going on correct.

So, that is on the fully decentralised permissionless side, but for enterprise applications we need something slightly in the model, where we want some of the decentralization benefits, but with certain security privacy features with better scale and so, on. Let us here is the distinction in the Bitcoin world, they are look they were looking at completely censorship resistant right. So, no one should be able to prevent transactions from being executed right. So, in a government or regulatory authority should not be able to say this transaction is not valid. So, they were looking for complete censorship resistance.

They were looking to is really scale to very large number of nodes. So, Bitcoin today runs about 5000 or so, a full nodes right. So, we want a scale to a really large number of nodes and they were looking at one block chain for the entire world, in contrast for the

enterprise applications we are really interested in security and privacy properties. Instead of really scaling in a number of this number of nodes, we are really interested in scaling in the transaction throughput.

And the distinction is like if you take any enterprise today it probably is doing business with may be tens of other, other companies or may be even may be sometimes hundreds of other companies, it is very rarely that you are scaling even larger than that. So, we are looking to really scale in the transaction throughput and, we are also looking at many interacting block chains, we could think of one block chain application for one block chain network for particular application, there is a different block chain network for another application and the two need to talk to each other right.

So, we are looking at those sorts of synonyms. So, the requirements in some sense are very different and because of that the some of the way we design these block chain platforms, are also going to be very different from what Bitcoin did, but overall the underline properties remain the same, they still want immutability, finality, consensus amongst all the parties and we want to run this in a decentralised manner, where no single entity is in charge of managing the entire network.

(Refer Slide Time: 14:10)

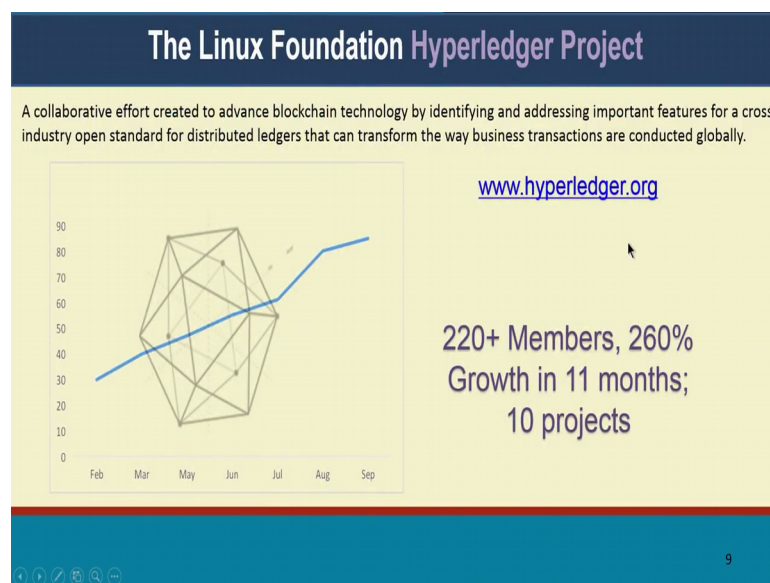
Permission-less vs Permissioned Blockchains		
	Permission-less	Permissioned
Access	Open read/write access to database	Permissioned read/write access to database
Scale	Scale to a large number of nodes, but not in transaction throughput	Scale in terms of transaction throughput, but not to a large number of nodes
Consensus	Proof of work/ proof of stake	Closed membership consensus algorithms
Identity	Anonymous/pseudonymous	Identities of nodes are known, but transaction identities can be private/anonymous/pseudonymous
Asset	Native assets	Any asset/data/state

So, I think I talked about some of these differences between permission less and permissioned block chain systems. So, the access is open in a permission less setting to everyone in the network whereas, in the permissioned setting we are only looking for

permissioned read write access, we can specify who can write a particular piece of data, who can read that data, those things we give you flexibility for that.

And the scale permission less is looking at scaling the number of nodes, the permissioned block chain is looking at scaling in the number of transactions. We talked about consensus the kinds of consensus algorithms, we use are going to be different between the two we will talk about that in detail, identity management is going to be different.

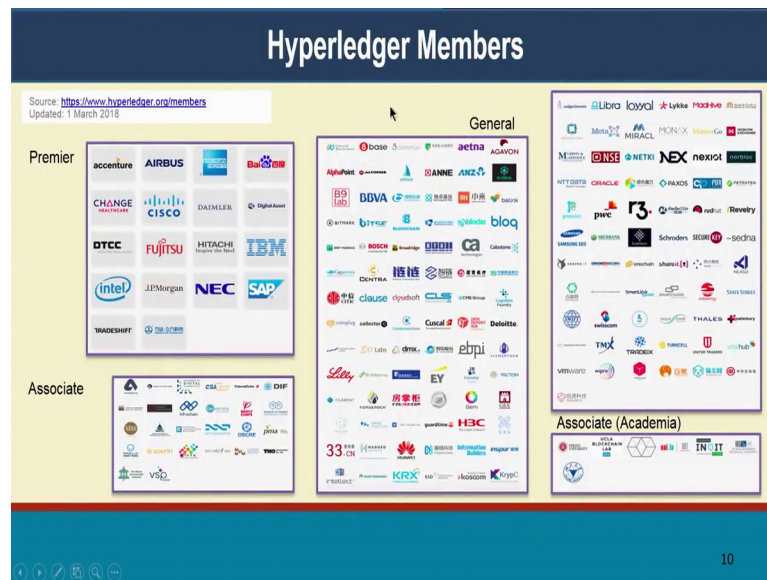
(Refer Slide Time: 14:54)



So, we will talk about all of these in greater detail over the next few lecture, with all of these going back to my initial story about how we started more than 2 years back. We started building this kind of new block chain platform specifically suited for enterprise applications, within contributed that to what is now the hyper ledger project, it is now governed by the Linux foundation, it is under the ages of the Linux foundation. And it is one of the fastest growing open source projects out there today right.

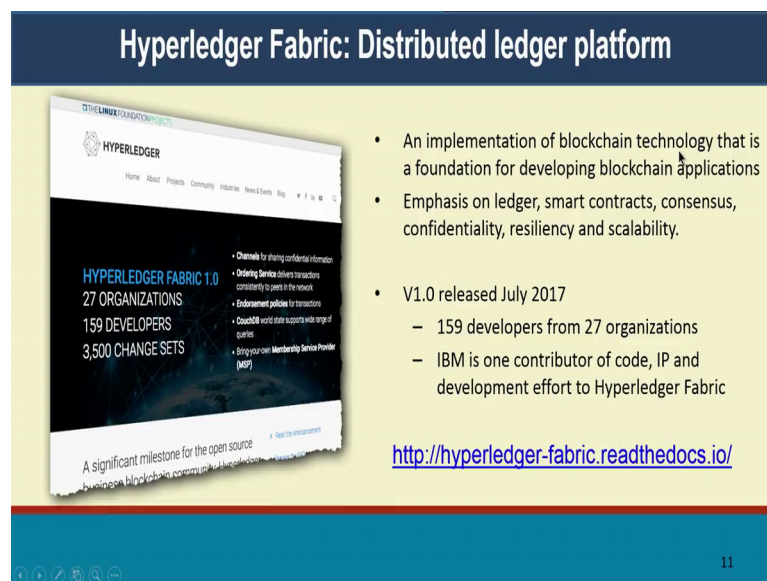
So, today we have over 220 plus members of this foundation these are all leading enterprise companies. So, in the next slide I have some of those names and its grown very quickly over a very short span of time right.

(Refer Slide Time: 15:33)



So, here is just the set of logos of all the various companies that are participate, that is that are now part of hyper ledger. So, this includes large technological firms the it includes large financial companies banks and so, on. It has a lot of start UPS it has even health care companies and industries specific companies who have joined this consortium, to help promote its mission in building the enterprise grade block chain platform right. And there are some mechanic make institutions set of all joined the consortium.

(Refer Slide Time: 16:10)



So, hyper ledger fabrics so, this is going to be the focus of the next few lectures in something that my team and myself have contributed to, it is it was released as a production grade of the hyper ledger fabric, was raised in July last year of version one of that of that platform. And it has a large number of organisations contributing to it. So, we get kind of get the best of experiences from around the world, and IBM is one of the largest contributors to this both in terms of code as well as IP, and we are we are fostering, this consortium.

(Refer Slide Time: 16:50)

Hyperledger Composer: Accelerating Time to Value

<https://hyperledger.github.io/composer>

- A suite of high level application abstractions for business networks
- Emphasis on **business-centric vocabulary** for quick solution creation
- Reduce risk, and increase understanding and flexibility

Business Application

Hyperledger Composer

Blockchain (Hyperledger Fabric)

- Features
 - Model your business networks, test and expose via APIs
 - Applications invoke transactions to interact with business network
 - Integrate existing systems of record
- Fully open and part of Linux Foundation Hyperledger
- Try it in your web browser now: <http://composer-playground.mybluemix.net/>

12

There are many other projects that are also part of the hyper ledger consortium one of them is hyper ledger composer we will look at this as well. So, this is a gives you a set of high higher level abstractions for business users, to come and develop applications on top block chain. So, instead of being a having to work with a (Refer Time: 17:08) details of the block chain platform.

We can level work at a level higher level of abstraction, where you can talk about business concepts directly and encode that to run on the block chain platform, it has many interesting features that you can model your business network, you can talk about it in terms of assets participants and transactions rather than having to talk about low level variables and functions and so, on.

And it is all exposed via APIs and you can automatically generate some of these APIs as well and, it also gives you the ability to integrate with the existing systems of record. So,

block chain in many of these enterprise applications block chain is going to be just one part of a larger applications. So, it might involve other databases or other places where you are storing data, you might have to bring that data on into block chain, or whatever is getting record on block chain you might want to extract that out and do your own analytics and visualization and things like that.

So, some for some of those capabilities are also part of composer and, composer is also fully open source open governed. And it is also under the Linux foundation hyper ledger project and this is easy link for you to go try it out quickly. So, they have a playground out there where you can go try out, but we will have a couple of lectures dedicated to looking at some of the details of hyper ledger composer.

(Refer Slide Time: 18:33)



The slide is titled "Fun Reading" and features the NPTEL logo in the top right corner. It contains a list of five items, each with a URL:

- What is the difference between Bitcoin and Blockchain (3 mins): <https://www.youtube.com/watch?v=MKwa-BqnJDg>
- Smart contracts, 1994 article by Nick Szabo: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/L_OTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
- Hyperledger resources page: <https://www.hyperledger.org/resources>
- Hyperledger publications: <https://www.hyperledger.org/resources/publications>
- Keynote talk by Brian Behlendorf, Executive Director of Hyperledger Project at LinuxCon 2017 (21 mins): <https://www.youtube.com/watch?v=pr4Hb0jb0Io>

At the bottom of the slide, there are navigation icons and the number 13.

So, for me personally I think some of the when I was back a student may be more than two one or two decades ago, some of the most interesting course is for me where the once that really hindered my curiosity. And they really made me explore and read a lot more than what the course material was really about. So, with that as a guiding force I am I am looking to this I am creating the section called fun reading at the end of a every lecture.

Where I will point you to some extra reading material that if you are interested you can go and look at it right. So, they I am trying to point you to certain directions, where you can go explore further, than what the lectures themselves give you. So, I am hoping that

at least some of you will go through some of these additional material, may be you pick and choose which topics you are most interested and you go there dwell in to that deeper. But at I would encourage all of you to at least look at some of these reading material they are all very good material overall.

So, these could be research papers these could be blogs these could be interesting start UPS that you could look at, it could be videos short ones that you can get a flavour of what this is about what that what the particular topic is about and so, on right. So, for this lecture there is interesting video on the difference between Bitcoin and block chain, which I have talked about a couple times during the course of the lecture itself.

So, this is a short YouTube video just three minutes, but it gives you a flavour of some of those differences and also encouraged you to read the original article on smart contracts, this was by nick Szabo back in 1994. So, imagine this was 15 years before bitcoin. So, people at that time were talking about being able to run pieces of code in a completely decentralised fashion. So, it was not like Bitcoin came up with these concepts sort of thing (Refer Time: 20:25), but there is lot of research that we went on behind the notion of Bitcoin and block chain itself.

So, this is one of those things it is an interesting it is a very short read it is just a philosophical statement that, we want be able to run these pieces of code in a decentralised fashion it is not sufficient if one person runs and it tells you that this is the output. And then there are resources for finding out about hyper ledger itself.

So, there is lot of material out there where you can read up on hyper ledger of the various projects that are out there, there are short videos that you can get your hand on to learn more about some of these projects. And there are lot of publications as well. So, lot of blogs and articles that have been written on the various hyper ledger projects, along with the hyper ledgers overall machine as well to build like the enterprise grade block chain, platform and also bring an intro probability amongst multiple platforms.

And Brian Behlendorf is the executive director of the hyper ledger project and, he gave a nice keynote at LinuxCon last year and it is just 20 minutes you can take a look at it tells you some of the motivations and the and the directions in which the hyper ledger project is planning to go right. So, with that thanks a lot that concludes the first lecture. So, see you at the next lecture.

Thank you.