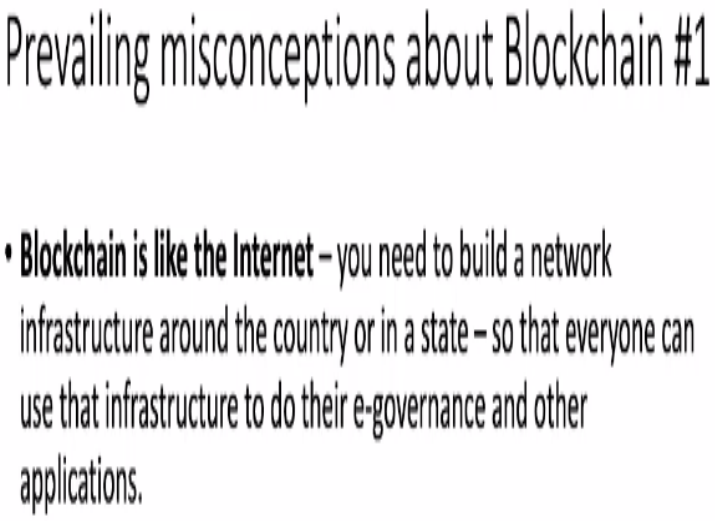
Blockchain Technology and Applications
Prof. Sandeep K. Shukla
Indian Institute of Technology – Kanpur

Lecture – 29
C3I Center

Welcome to the part 3 of the final week of blockchain technology and applications on NPTEL. So in this last part, I want to talk to you about some of the misconceptions I have seen while discussing about blockchain with various people including the government agencies and I want to dispel some of these myths, so that you know you are also aware of those misconceptions and you know how to address them when you discuss the blockchain.

(Refer Slide Time: 00:35)



So, I have written down some of the misconceptions that I have been hearing about. So first one is blockchain is like the Internet, you need to build a network infrastructure around the country or in a state, so that everyone can use that infrastructure to do their e-governance and other applications, and I have seen this in Tamilnadu government's brochure where they are claiming to be building a statewide blockchain through which they want to provide e-governance services. Now, the problem is that blockchain is not like the Internet.

You do not have to prebuilt a blockchain on which all kinds of data will be thrown in. You have seen that you know we did for example a blockchain solution architecture for say land records, another one blockchain solution for healthcare, and they are quite different. Their assets that are involved are quite different. The transactions are quite different. Some have multiple channels. Some require single channel. The rest APIs for accessing, making

transaction requests and so on are quite different.

So privacy requirements are quite different. So it makes no sense to build a blockchain, have nodes all over the state or region or the country and say that okay here is a blockchain, now you can build an application on top of this, it does not make sense. Each application needs to be considered in its entirety and what blockchain solution works for it will depend on the problem, its requirements, and then accordingly you have to create their solution.

There are multiple different platforms that are available when most of them are open source, so there is nothing hidden in that and you can always use them to build your application. So, this concept that you know we build a statewide blockchain or nationwide blockchain and then any kind of application will be built on top of it makes no sense.

(Refer Slide Time: 03:09)

Second misconception I keep hearing is that blockchain is secure, which means that they assume that tamper resistant data repository is same as secure, but we have seen in this course while discussing for example the Ethereum for example as soon as smart contracts came in, the number of vulnerabilities that were exposed were a very large right and we discussed some of the tools that people have developed to check the smart contracts for security vulnerabilities and so on.

So blockchain by itself by definition or by construction is not secure. What blockchain guarantees is that if you have a proper mechanism for transaction validation, if you have a proper mechanism for building consensus, then you can create this chain of blocks and then

when the chain of blocks is sufficiently long, then going back and changing one information or more information in a particular block is going to be so computationally expensive that you can assume that it is going to be computationally almost impossible.

So, therefore you are going to see data in the grid. Now in case of block chains that are not based on let us say proof-of-work kind of consensus mechanism where the computational cost is not prohibitive, but they have probably something else, for example proof of authority or proof of stake where somebody unless a large number of high stake individuals in the blockchain participants do not collude and want to attack, the integrity cannot be easily tampered with.

In case of permissioned blockchain, it is secured by way of the fact that identities of each participant is actually established and therefore any kind of tampering attempt will be actually figured out because it will take long time to actually go back in time and redo every transaction except the transaction that you want to say eliminate and not get caught, because your redo identity is associated with that identity. So integrity is something that is kind of part of the reason why blockchains are used but does not make it any secure, for example against DDoS attack.

Against exploiting software vulnerability in your smart contracts to do things which would be otherwise considered from the blockchains perspective this is legal because this is acceptable because transactions are going through according to the smart contract and everything, but the smart contract itself at the bug and therefore somebody is using it to do the bug. For example in the DAO attack, they used a bug in the security in the smart contract that allowed somebody to change the owner of an account and that is why the attack could happen. So, declaring that since I am doing blockchain I am secure is also a very wrong idea.

(Refer Slide Time: 07: 34)

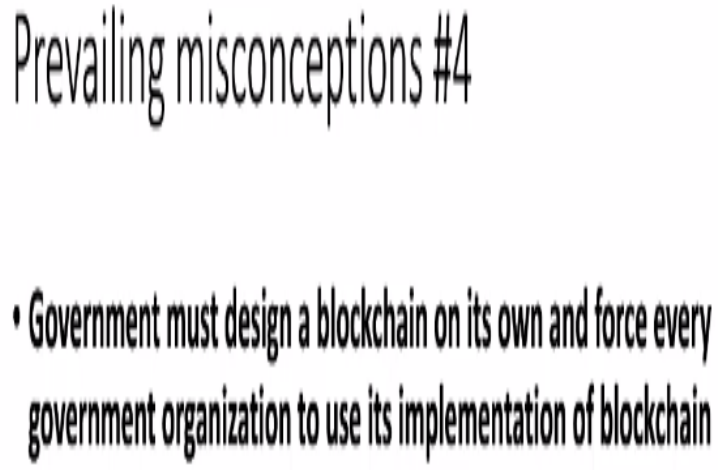
Now another misconception is that since I am using cryptography, no matter what cryptography I am using, it guarantees that the blockchain data integrity is kept. Now, this again depends on the cryptography and the strength of the cryptography you are using. Of course, if you are using a cryptographic hash function for example that is so far known as you know collision resistant like SHA256 or SHA-3, you can be more or less feeling comfortable about the data integrity.

But we do not know in the future nobody would come up with a way of finding collision like SHA-1 was considered pretty secure MD5 was considered secure, was used for some time, but then people found ways to do collisions in them. Similarly cryptographic signatures because you are using RSA for example or and some other public key cryptography, you can assume that if you are using the proper key size and everything, it is not possible to forge signatures, but we know that RSA 10 size of you know 1024 bit long keys are no longer considered very secure.

Also there could be other things like side channel analysis on your machine on which you are doing the cryptography and then the public/private key maybe leaked out. So all kinds of possibilities are there, so you cannot completely guarantee that cryptography is going to keep the data valid and data integrity intact, but you know if you are using strong cryptography, strong hashing function, collision-resistance hashing function for now you are okay. The other issue is that quantum computing.

So in the future if the data is kept for a long time if a particular blockchain is there for a long time and then the keys are still using let us say RSA and even the PKI is **is** RSA, then if quantum computing becomes a reality, RSA will be broken and then you will have a problem. So, all these things has to be always considered in the context of current time and what is best known about the cryptography you are using at that current time.

(Refer Slide Time: 10:41)



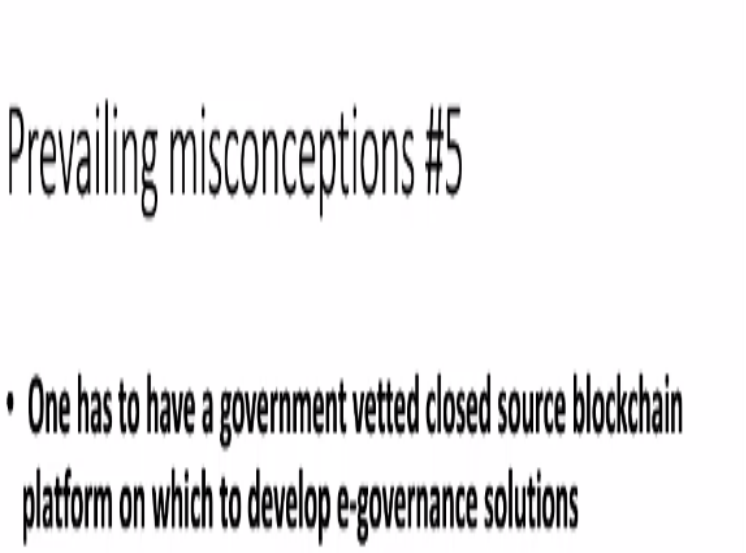
So, another one I heard is that from the government agencies that government must design a blockchain on its own and force every government organization to use that implementation of the blockchain. So, this actually was told to me by some government people saying that you know we want full control on the blockchain that people are using for e-governance, we do not want a foreign provenance blockchain, we do not want a freeware or open-source blockchain, we want to have our own and therefore we will have to force everybody to use it.

One example they were trying to give in support of this argument is that look at what WhatsApp has done to us, we have no way to force Facebook to give us the messages that are being exchanged on WhatsApp. So we should not be dependent on technology built by others, but this is a very wrong idea, the reason being that you cannot have an untrustworthy system to create people's trust. The whole point of doing blockchain based e-governance is to actually earn people's trust in a much better manner.

Now if you say that I am going to build a blockchain, I am going to build a cryptography in it, I am going to have a full control of the code and I want security by obscurity, then you are

going to be in for a surprise. First of all, people might suspect that the cryptography has been weakened or some form of some backdoor is there in the infrastructure for government to actually get the information before cryptography is applied to some data or before hashing is done on data that is the one problem with respect to generating citizen trusts, but the other issue is that indeed it is not something that government should control.

(Refer Slide Time: 13:20)



So same kind of misconception is that it has to be a government vetted closed source blockchain platform to develop all e-governance solutions, same thing, but the other problem is that there are multiple different varieties of blockchain right. So we have seen blockchain as evolved from blockchain 1, blockchain 2.0, blockchain 3.0 and now we are talking about blockchain 4.0. So this thing is an evolving technology.

If you make it a closed source blockchain now today, then tomorrow the blockchain will move to much better features and better ways of doing, building applications and then it will be missing out. Second problem is that where will you get the best programmers that are working on Ethereum or Hyperledger because these are open sourced and huge community of very good programmers are developing them. Where will you get that kind of developers in the government sector to build something that competes in performance, competes in feature set, competes in the ability to provide the guidance, everything is going to be difficult.

So it is best to do open source blockchain platform, because it is open source you can have the full you know authority and ability to actually look into the code, look for existence of any backdoor, you know check the cryptography implementation everything, right. So it is

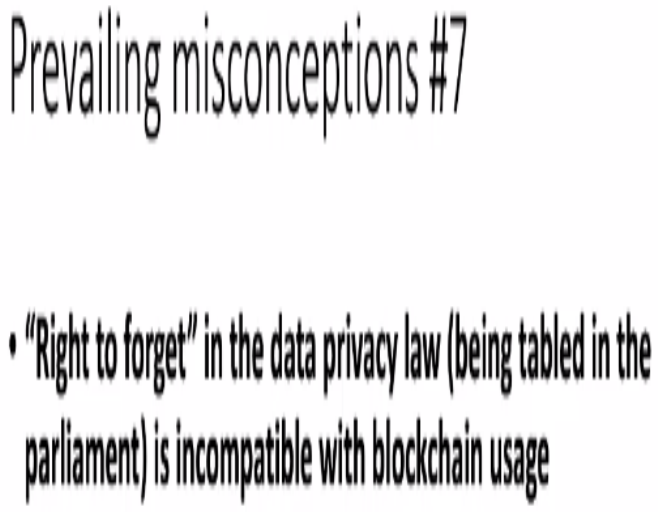
not a good idea to have a government vetted closed source blockchain platform for e-governance solutions.

(Refer Slide Time: 15:09)

Another misconception I keep hearing is that oh blockchain is an open ledger, it is open to everybody, so there will be no data privacy and that is again a wrong idea. First of all, you do not have to put the entire data on the blockchain even if it is open and public. You can put the hashes of the data because eventually you want to use blockchain to provide data integrity guarantees and not to float the data itself. In case you want to have the data transferred, there may be other ways to have the data transfer rather than using the blockchain as a conduit for data transfer.

So it is a total misconception or maybe the mindset that is stuck in blockchain 1.0 like bitcoin or Ethereum, where all the data is available to everybody in their public permissionless setup, then I can understand that misconception has arisen of that, but you know people should study the latest blockchain technologies, the distributed ledger technologies and get rid of this misconception.

(Refer Slide Time: 16:36)

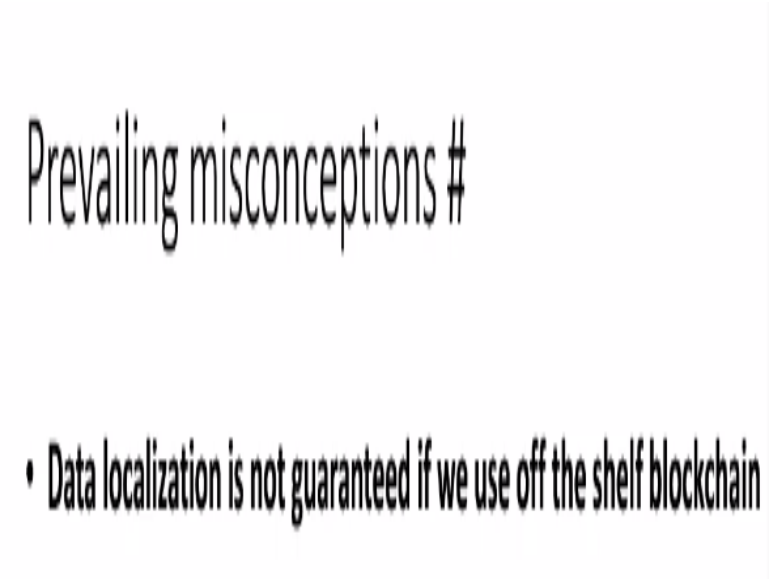


So the other misconception is that the right to forget in data privacy law is incompatible with blockchain usage. So, this is again the same kind of mistake. First of all, you do not put the data into the blockchain if there are personally identifying information or other kind of information that comes under the purview of the privacy law. So secondly you know the data in a permissioned blockchain, a particular change in the data is possible by basically making a transaction for doing that. So, therefore 2 things.

One is that you do not put e-governance blockchain in public permissionless setup, so therefore there is only permissioned entities that are going to look at the data, but even if that is a concern, you actually can put encrypted version of the data and this encryption has to be strong and forward secure which means that it should be encrypted with the quantum resistant cryptography and then there may be a proxy re-encryption scheme and other schemes to actually for the data principle to release the right to look at the data.

Then once your data has to be forgotten, then you actually destroy the ability to create re-encryption keys. So also in some cases, you only put the hash of the data in which case there is no concern about this right to forget because there is no way to reconstruct your data from the hash. So, again this is a mindset that is coming from knowing only about bitcoin and maybe Ethereum, but this mindset has to change because now you know we have come a long way from bitcoin type of blockchain to distributed ledger technology and where this kind of concerns can be easily addressed.

(Refer Slide Time: 19:00)



Another issue is that oh so if you put something in the blockchain, you do not know the ledger is replicated everywhere, so there is no guarantee that the data will be localized in the country, whereas government requires that all the data should be localized in the country which means that all the data should not leave the country's geographical boundaries. All servers in which data is kept should be within the geographical boundaries of the country because the data may be subpoenaed by the courts of the country.

If it is in another country, it cannot be subpoenaed by the extent laws of the nation. All these considerations are called data localization considerations. Now if you are using a Hyperledger instance or Corda instance or some permissioned private blockchain for providing e-governance with the proper APIs for people to access data, but through certain nodes that are exposing the rest APIs, then all the servers and everything are under your control under the control of the government.

So, there is no concern about data localization. So, this is again another misconception that has to understand how the permissioned private distributed ledger technology works and then this misconception will be addressed.

(Refer Slide Time: 20:47)

Prevailing misconceptions #9

• Government must regulate blockchain technology

Another misconception I heard a lot is that the government must have a regulation to regulate the technology. Now, that is actually again a misconception. You do not regulate a technology, what you regulate is the rules, what you regulate is how the data is used or how transactions take place. So, it is not the underlying technology that you need to regulate, you need to regulate the particular application domain in which if it is banking then banking regulations, if it is legal contracts then it is the company law or whatever be applicable laws are has to regulate that particular application.

Now, one situation is certainly important is that for example our transactions that is done over an IT system without any manual intervention, legal transactions or contract made on an IT system without manual intervention are acceptable or are proof of temper that one can generate from the blockchain, the investigation into a blockchain is that acceptable in a court of law in the country? These kind of blockchain related changes in IT law or IT Act associated with taking into account that the usage of blockchain at various sectors has to be made.

But that is not about regulating the blockchain technology is about, making laws more amenable for broader use of blockchain technology, so that is a facilitator of developing applications on blockchain technology other than regulating the blockchain technology. Regulating blockchain technology would mean that you go and tell that you cannot use this kind of blockchain technology in this kind of applications, you cannot use permissioned blockchain for this kind of applications or you have to use permissioned blockchain technology for this kind of application.

Those would be regulating the technology but that should be less to the particular domain and particular may be government agency would be using this and assuming that they are doing the right thing. There should be certain applicable policies related to, security related to, privacy related to availability, integrity, etc., and they have to choose the right blockchain technology for fulfilling those obligations. You do not have to actually regulate the blockchain technology.

(Refer Slide Time: 23:59)

Then another prevailing misconception I heard a lot is that oh it is all about cryptocurrency, it is immensely power consuming and therefore it is not environment friendly. Again these kinds of ideas are coming from the misunderstanding and the ideas that originated in bitcoin or blockchain 1.0 with proof-of-work. We have seen throughout these classes that is not the only type of blockchain, neither are they really applicable to most of the applications that we really want blockchain to be used in and therefore this concern is not a correct or valid concern.

So with that, I would like to close this week as well as the course. I am hoping that this course has given you a very good conceptual understanding of the blockchain technology, its evolution from blockchain 1.0 to 3.0 and the various ways the blockchain has evolved for making it applicable for various applications, what a blockchain technology based application give you and what are the advantages of using that particular application over a blockchain rather than a traditional centralized IT system.

Also, I hope that you understand the prevailing misconceptions regarding blockchain and how to dispel them, and finally I hope that by understanding at least 4-5 different blockchains in some details like bitcoin, Ethereum, Hyperledger, Corda, IOTA and having very cursorily seen something like that is the Algorand kind of blockchain, you have some idea that this field of blockchain technology has quite a bit of variety and because of this variety, it is able to fit into various different application domains.

Which application domain actually requires a blockchain based solution depends on what are its requirements, in terms of data integrity, in terms of availability, in terms of you know redundancy of data, in terms of who is allowed to participate, and in terms of whether the data that is kept in this decentralized ledger should be visible to everybody or not, all that considerations has to be factored in before you choose whether to first of all first you choose whether to really use blockchain or centralized system is sufficient for your requirements or if it is the blockchain that you want to do.

Then the question is what type of blockchain you need to use. So, these kind of perceptual understanding is what the goal of this course was and I hope that having gone through 8 weeks of lectures and quizzes and all that you are now comfortable and confident about that kind of abilities to advise as well as select yourself the right approach to developing an application with blockchain. With that, I wish my best to all of you for a more productive career in using blockchain technology in case you decide to do so.

For that also you have to learn more about at least one or two specific blockchain technology in detail how to build applications in those blockchain technology and how to deploy them, how to may be deploy them on the cloud, these kind of things that you have to figure out over time and hopefully this course was a suitable substrate on which you will be building a much more robust castle of knowledge, which will give you advancement in your career and your studies and research whatever is you are doing. With that, thank you all for listening for 8 long weeks and wish you all the best. Thank you.