

**Distributed Systems**  
**Dr. Rajiv Misra**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Patna**

**Lecture – 27**  
**Block Chain**

(Refer Slide Time: 00:17)

**Introduction**

- A **blockchain is essentially a distributed database of records** or public ledger of all transactions or digital events that have been executed and shared among participating parties.
- Each transaction in the public ledger is **verified by consensus of a majority of the participants** in the system. And, once entered, information can never be erased.
- The blockchain contains a certain and verifiable record of every single transaction ever made.
- To use a basic analogy, it is easy to steal a **cookie from a cookie jar**, kept in a secluded place than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people.

*Handwritten notes:*  
- Distributed Consensus  
- Distributed Ledgers  
- Search Function  
- Distributed Consensus  
- Impossibility Results - Possibility

Technology introduction; block chain is essentially a distributed database of records or a public ledger of all transactions or digital events that have been executed and shared among participating parties. So, in a blockchain we can also say that it is kind of distributed consensus. So, a blockchain is basically categorized in a distributed consensus its nothing, but essentially a distributed databases of records; so, for the operations which are called as ledgers. So, it is a distributed ledger implementation. So, bank also maintains the ledger of different people a, b, c having different money values in their accounts and the bank maintains the ledger centrally how this particular ledger is to be made in a decentralized manner. So, this is to be achieved using a distributed consensus and blockchain is the technology which will basically maintain this kind of distributed ledger or a distributed records.

So, a blockchain is essentially a distributed database of records or a public ledger of all the transactions or digital event that have been executed and shared among the participating parties. So, it is not only one is not maintained at centrally located place,

but it is to be maintained in a distributed manner how it is all done through a blockchain that we are going to discuss this new technology which is also called a disruptive tech technology. In this part of their discussion involves the concept of distributed consensus which will basically see that there are different impossibility results and how due to this impossibility this particular technology which is called a blockchain is going to make it possible to see in this part of the discussion.

So, each transaction in a public ledger is verified by a consensus of majority of the participant in the system that is why it is called basically the distributed consensus. So, the distributed ledger will be implemented with the help of the distributed consensus of the participating parties. So, a blockchain contains a certain and verifiable records of every single transaction ever made. So, to use a basic analogy it is easy to steal a cookie from a cookie jar kept in a secluded place then stealing a cookie from a cookie jar kept in a market place being observed by thousands of the people meaning in the sense there are 2 models of security the existing model of security employs a particular security provision to secure some resources from unauthorized access and this particular security mechanisms have to be implemented in a very strong manner and it requires a lot of overheads and it has to be maintained centrally.

The other model says that it is a decentralized security model. So, the un-trusted people set up un-trusted people will be given the access to these resources and resources are being basically monitored by the un-trusted people and this is another model of security. So, if let us say that cookie is placed over here and it is being secured nobody can take the security will ensure it similarly the cookies are put in a public. So, public is watching. So, then also basically; they will witness and nobody can steal then in that case. So, this is another model and we are going to see how this particular model will be useful to implement the distributed consensus and how the blockchain is going to implement it.

(Refer Slide Time: 04:57)

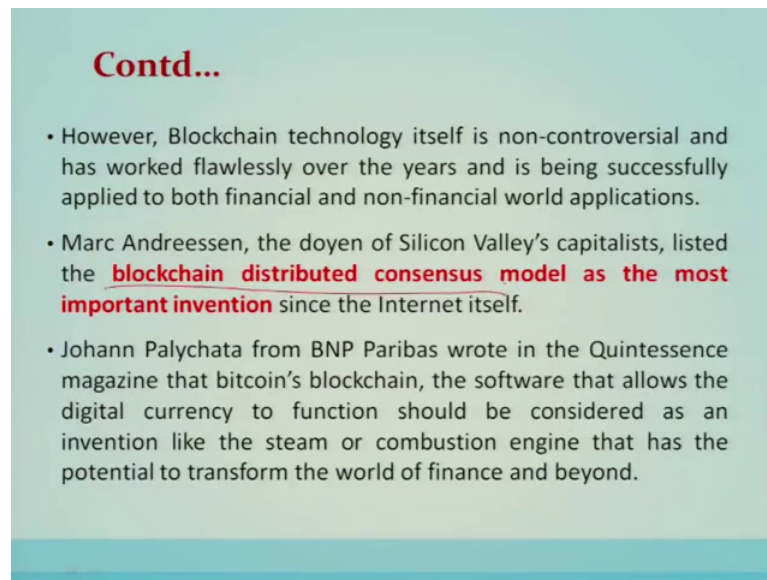
**Contd...**

- **Bitcoin is the most popular example** that is intrinsically tied to blockchain technology.
- It is also the most controversial one since it helps to **enable a multibillion-dollar global market of anonymous transactions without any governmental control.**
- Hence it has to deal with a number of **regulatory issues** involving national governments and financial institutions.

So, Bitcoin is the most popular example of a blockchain technology it is a disruptive technology means the way the banks are operating with the help of a of a single centralized secure system, it is going to basically provide an alternative wherein identities are also anonymous and the technologies which are called as the distributed consensus is basically used in the in the blockchain technologies. So, we are going to see and we have already seen that Bitcoin has successfully implemented with the help of a blockchain all security provisions which is otherwise possible only through the centralized banks now is possible using the blockchain technology to realize it.

So, it is the most controversial that is a bit Bitcoin. Since it helps the enable the multibillion dollar global market of anonymous transactions without any governmental control hence it has to deal with the number of regulatory issues involving the national and financial institutions.

(Refer Slide Time: 06:21)

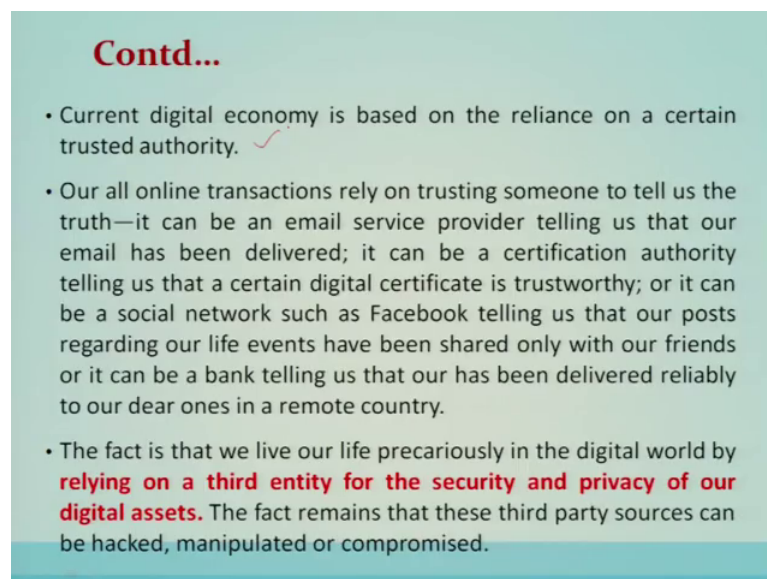


**Contd...**

- However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications.
- Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the **blockchain distributed consensus model as the most important invention** since the Internet itself.
- Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond.

Blockchain technology itself is non controversial is what flawlessly over the years and is being successfully applied to the financial non financial applications. So, blockchain distributed consensus model is the most important invention.

(Refer Slide Time: 06:41)



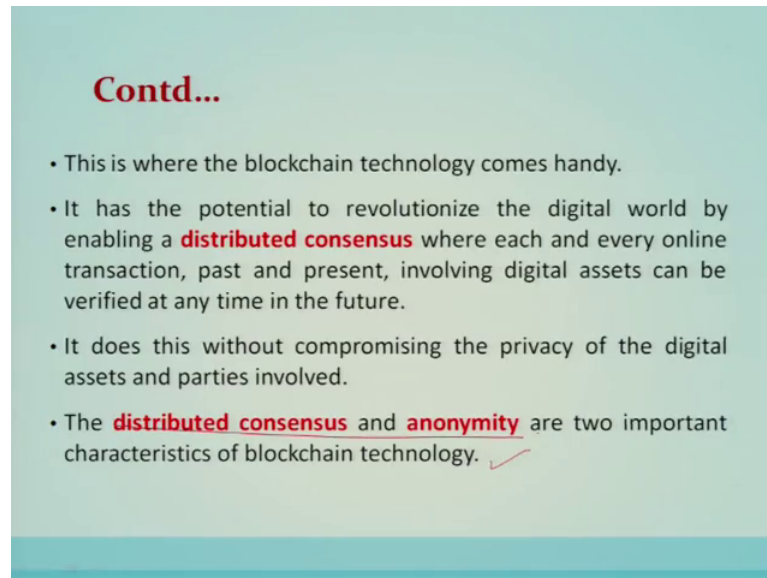
**Contd...**

- Current digital economy is based on the reliance on a certain trusted authority. ✓
- Our all online transactions rely on trusting someone to tell us the truth—it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our has been delivered reliably to our dear ones in a remote country.
- The fact is that we live our life precariously in the digital world by **relying on a third entity for the security and privacy of our digital assets**. The fact remains that these third party sources can be hacked, manipulated or compromised.

So, that is why we are discussing this particular that is technology that is called a blockchain technology which is not only going to be used in a financial institution, but as well as non financial institutions wherever there is a centralized system.

So, current digital economy is based on the reliance on trusted authority. So, wherever such kind of scenarios are there this particular blockchain technology will going to solve the problem, I believe in our inner life precariously in a digital world by relying on the third entity for security and privacy of our digital assets and blockchain technology comes into an handy.

(Refer Slide Time: 07:22)

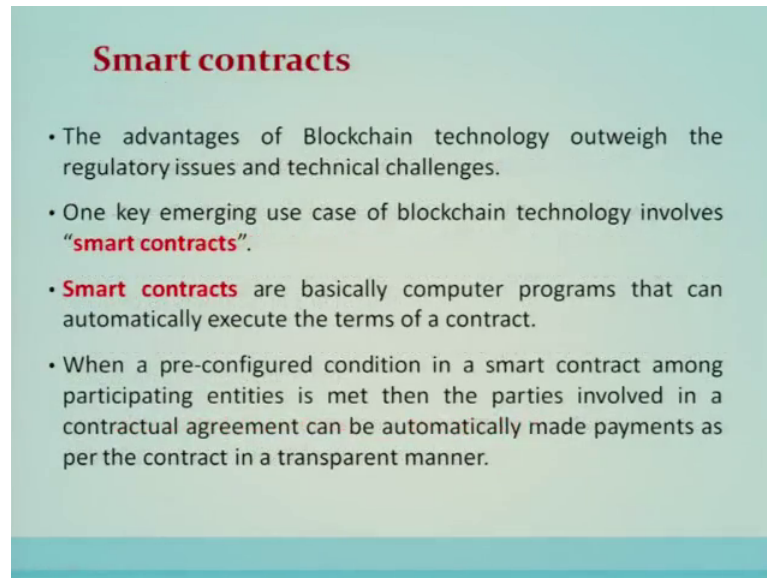


**Contd...**

- This is where the blockchain technology comes handy.
- It has the potential to revolutionize the digital world by enabling a **distributed consensus** where each and every online transaction, past and present, involving digital assets can be verified at any time in the future.
- It does this without compromising the privacy of the digital assets and parties involved.
- The **distributed consensus** and **anonymity** are two important characteristics of blockchain technology. ✓

So, it has a potential to revelation as the digital world by enabling a distributed consensus we are each and every online transaction passed prison involving the digital assets can be verified at any time in the future. So, the distributed consensus and anonymity are the 2 important characteristics of a blockchain technology that we are going to see here in this particular discussion.

(Refer Slide Time: 07:50)

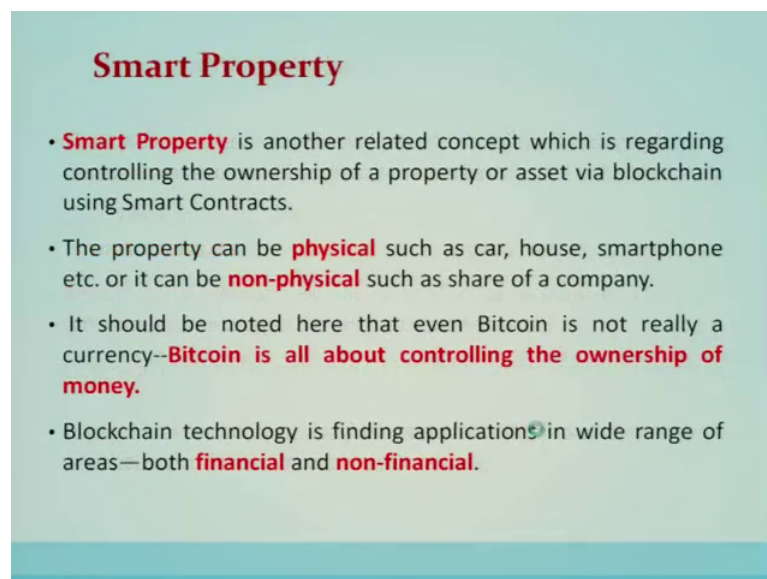


**Smart contracts**

- The advantages of Blockchain technology outweigh the regulatory issues and technical challenges.
- One key emerging use case of blockchain technology involves “**smart contracts**”.
- **Smart contracts** are basically computer programs that can automatically execute the terms of a contract.
- When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner.

Now, another application is in the form of digital smart contracts. So, the advantage of block chain technology outwits the regulatory issues and technical challenges one key emerging use case of blockchain is smart contracts.

(Refer Slide Time: 08:07)



**Smart Property**

- **Smart Property** is another related concept which is regarding controlling the ownership of a property or asset via blockchain using Smart Contracts.
- The property can be **physical** such as car, house, smartphone etc. or it can be **non-physical** such as share of a company.
- It should be noted here that even Bitcoin is not really a currency—**Bitcoin is all about controlling the ownership of money.**
- Blockchain technology is finding applications in wide range of areas—both **financial** and **non-financial**.

Smart property is another related concept controlling the ownership of the property or I said why are the blockchain using smart contracts is another non financial kind of application.

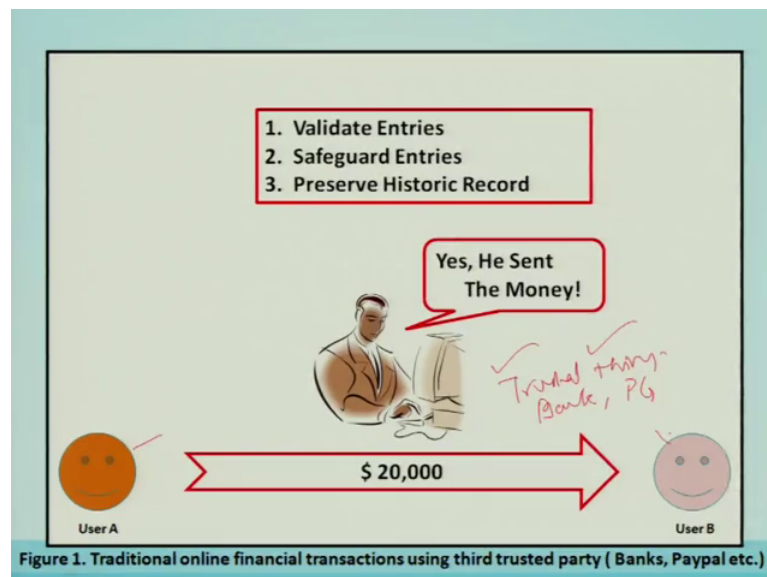
(Refer Slide Time: 08:20)

### Financial and Non-Financial Applications

- **Financial institutions and banks** no longer see blockchain technology as threat to traditional business models. The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications. In a recent interview Rain Lohmus of Estonia's LHV bank told that they found Blockchain to be the most tested and secure for some banking and finance related applications.
- **Non-Financial applications** opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved.

So, financial and non financial application financial institutions in bank no longer see the blockchain technology is a threat with a traditional business model non financial application opportunities are also endless.

(Refer Slide Time: 08:34)



So, let us see this particular example in a traditional system here the bank has to say that or has to verify the flow of the transaction from A to B, yes, he has sent the money. So, that is being done in a traditional transactions where this is the trusted third party that is a bank or a payment gateway which basically both these partners they trust or everyone



else trust and that is the existence of the bank is involved transactions which is happening how this is to be broken up how 2 people can communicate or can transact without using the third party of a blockchain technology.

(Refer Slide Time: 09:08)

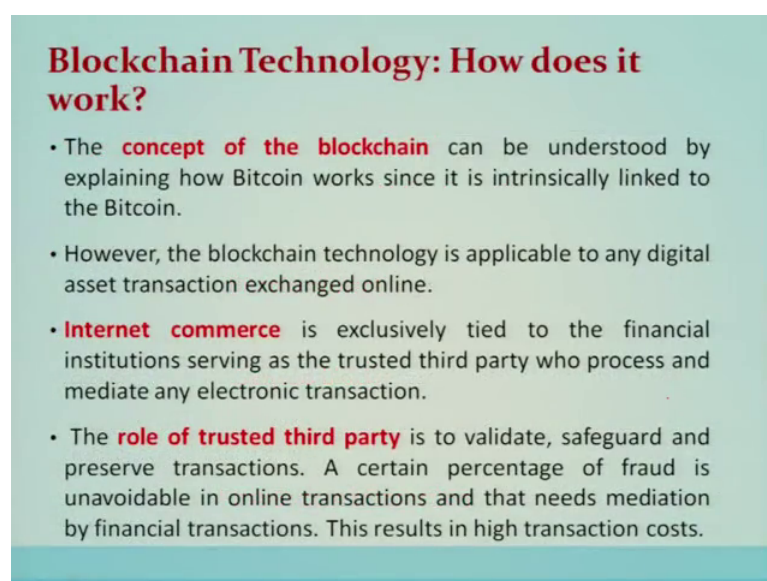


**Contd...**

- Every industry in today's digital economy is also facing disruption due to the emergence of blockchain technology.
- Blockchain technology has potential to become the new engine of growth in digital economy where we are increasingly using Internet to conduct digital commerce and share our personal data and life events.
- There are tremendous opportunities in this space and the revolution in this space has just begun.
- In this lecture, we will also focus on few key applications of Blockchain technology in the area of Notary, Insurance, private securities and few other interesting non-financial applications.

So, in this lecture we will also focus few key applications of the blockchain technology such as in the area of notary insurance private securities and other film interesting non financial applications.

(Refer Slide Time: 09:39)



**Blockchain Technology: How does it work?**

- The **concept of the blockchain** can be understood by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin.
- However, the blockchain technology is applicable to any digital asset transaction exchanged online.
- **Internet commerce** is exclusively tied to the financial institutions serving as the trusted third party who process and mediate any electronic transaction.
- The **role of trusted third party** is to validate, safeguard and preserve transactions. A certain percentage of fraud is unavoidable in online transactions and that needs mediation by financial transactions. This results in high transaction costs.

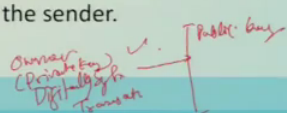


So, this is the blockchain technology the concept of the blockchain is understood by explaining how the Bitcoin works; since it is intrinsically linked with a Bitcoin.

(Refer Slide Time: 09:52)

**Contd...**

- **Bitcoin uses cryptographic proof** instead of the trust in the third party for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature.
- Each transaction is sent to the "**public key**" of the receiver digitally signed using the "**private key**" of the sender.
- In order to spend money, **owner of the cryptocurrency** needs to prove the ownership of the "**private key**". The entity receiving the digital currency verifies the digital signature – thus ownership of corresponding "**private key**"—on the transaction using the "**public key**" of the sender.



The diagram shows a box labeled 'Owner (Private Key)' with an arrow pointing to 'Digital Transaction'. Another arrow points from 'Digital Transaction' to 'Public Key'.

So, Bitcoin uses cryptographic proof initial initial of the trust in the third party of 2 billing parties to execute the an online transaction over the internet. So, each transaction is sent to a public key of the receiver a digitally signed; using a private key of the sender in order to spend the money owner of the cryptocurrency needs to prove the ownership of the private key the entity receiving the digital currency verifies the digital signature, there is the ownership of the corresponding private product key on the transaction on the transaction uses using the public key of the sender whenever the owner has a private key it use; it will digitally sign the transaction and this particular transaction is broadcast on the receiving side this particular using public key this particular transaction is verified and if it is verified that he is the owner who want to do a transaction then basically the process of chaining the transactions will basically involve that we are going to see.

So, each transaction is broadcast to every node in a in a Bitcoin network and is recorded in a public ledger after verification.

(Refer Slide Time: 11:22)

**Contd...**

- Each transaction is broadcast to every node in the Bitcoin network and is then recorded in a public ledger after verification.
- Every single transaction needs to be verified for validity before it is recorded in the public ledger. Verifying node needs to ensure two things before recording any transaction:
  1. Spender owns the cryptocurrency—digital signature verification on the transaction.
  2. Spender has sufficient cryptocurrency in his/her account: checking every transaction against spender's account ("public key") in the ledger to make sure that he/she has sufficient balance in his/her account.

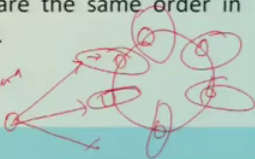
So, every transaction needs to be verified for validity before it is recorded in a public ledger verifying mode needs to ensure 2 things before recording any transaction spender owns the cryptocurrency it has to digitally sign and spender has sufficient cryptocurrency in his account checking every transaction against the spenders account to make sure that he has sufficient.

(Refer Slide Time: 12:01)

**Contd...**

- However, there is question of **maintaining the order of these transactions** that are broadcast to every other node in the Bitcoin peer-to-peer network.
- The transactions do not come in order in which they are generated and hence there is need for a system to make sure that **double-spending of the cryptocurrency** does not occur.
- Considering that the transactions are passed node by node through the Bitcoin network, there is no guarantee that orders in which they are received at a node are the same order in which these transactions were generated.

*Distributed System* *Broadcast*

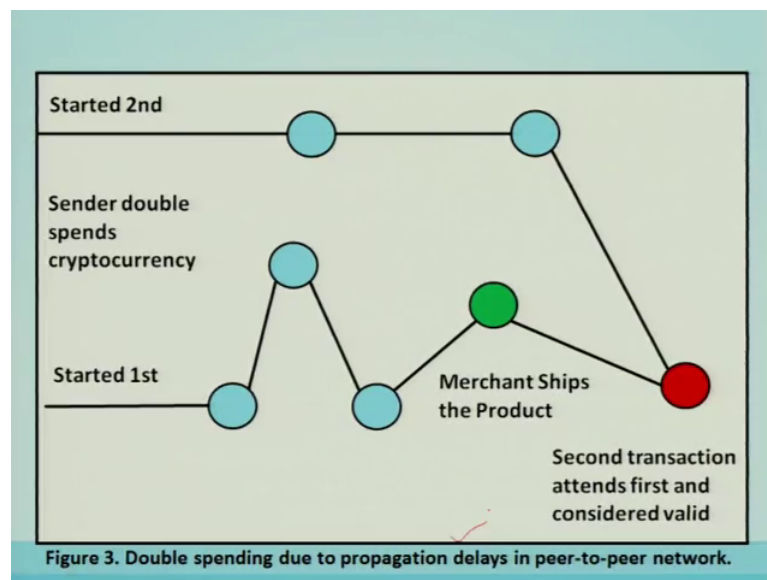


Is now the question of maintaining the order of these transactions because to every other node in the in the peer to peer network the transition do not come in the order in which

they are normally generated by because of delays in the network. Hence there is a need of for a system to make sure that double spending of a crypto currency does not occur believe there are various peers and if it is the message is broadcast it may happen that this particular transaction may reach earlier than other transactions

So, the ordering is not basically guaranteed at all the peers, but what happens is majority of the peers of this particular ordering is basically taken care and the double spending of a cryptocurrency currency can be avoided in using the distributed consensus though double is pointing due to the propagation delays in a peer to peer network I explained well spending means.

(Refer Slide Time: 13:08)



So, they are going 2 transactions are started looser and it may. So, happen that they are being received at different instant of time, but it will be basically ordered using the distributed consensus.

(Refer Slide Time: 13:34)

**Contd...**

- This means that there is need to develop a mechanism so that the entire Bitcoin network can agree regarding the order of transactions, which is a daunting task in a distributed system.
- The Bitcoin solved this problem by a mechanism that is now popularly known as **Blockchain technology**.
- **The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain.**
- The transactions in one block are considered to have happened at the same time.
- These blocks are linked to each-other (**like a chain**) in a proper linear, chronological order with **every block containing the hash of the previous block.**

Hence only one transaction will be basically used and double spending will be avoided using this particular concept of distributed consensus.

So, Bitcoin solve this problem by a mechanism that is now properly known as blockchain technology. So, the transaction in one block are considered to have a happened at the same point of time these blocks are linked to each other like a chain in a proper linear and chronological order with every block containing a hash of the previous blocks.

(Refer Slide Time: 14:07)

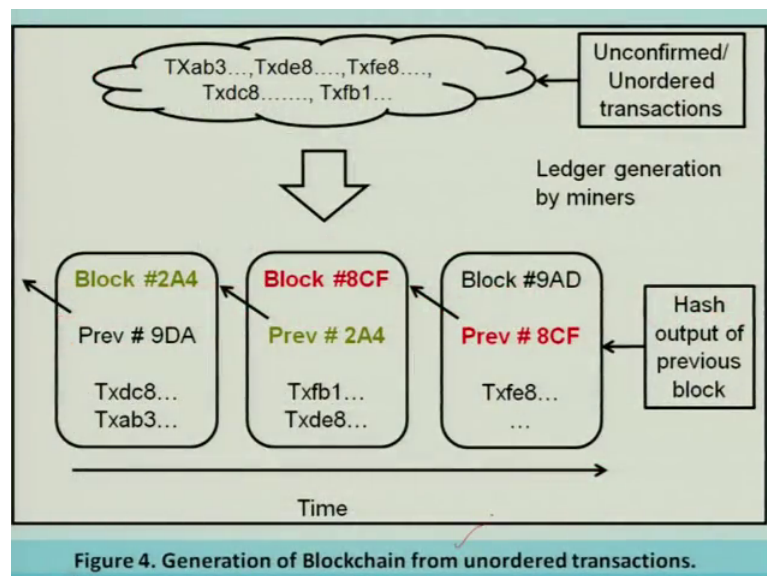


Figure 4. Generation of Blockchain from unordered transactions.

So, this particular timestamp is maintained in the form of a blockchain that is shown over here Bitcoin solves this particular problem by introducing a mathematical puzzle.

(Refer Slide Time: 14:17)

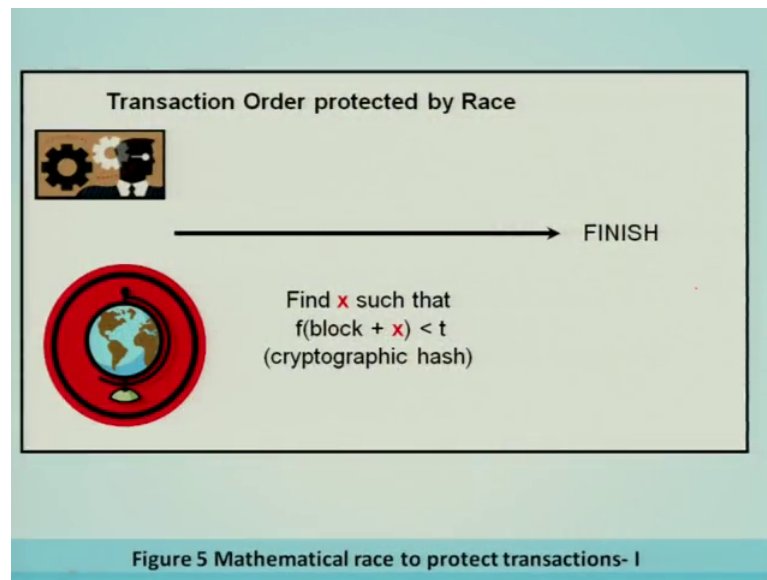
**Contd...**

- **Bitcoin solves this problem by introducing a mathematical puzzle:** each block will be accepted in the blockchain provided it contains an answer to a **very special mathematical problem**.
- This is also known as **“proof of work”**—node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle.
- For instance, a node can be required to find a **“nonce”** which when hashed with transactions and hash of previous block produces a hash with certain number of leading zeros.
- The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.

So, each block will be accepted in the blockchain provided it contains an answer to a very special mathematical problem which is also called a proof of work loading a block need to prove that it is; it has put enough computing resources to solve a mathematical puzzle.

So, for instance a node can be required to find out nonce which when hashed with the transactions in hash or previous blocks produces a hash with a certain number of leading 0s; as I mentioned earlier that finding out this particular nonce is a computationally very expensive it requires lot of CPU and the energy resources and the one the node which is called a minor who calculates first we will get the incentive for this particular purpose.

(Refer Slide Time: 15:19)



So, the transactions transaction order is protected by the race here the mathematical race to protect the transactions.

We small probability that more than one block will be generated in the system at a given time first node to solve the problem broadcast the blocks to the rest of the network.

(Refer Slide Time: 15:27)

**Contd...**

- This mathematical puzzle is not trivial to solve and the complexity of the problem can be adjusted so that on average it takes ten minutes for a node in the Bitcoin network to make a right guess and generate a block.
- There is very small probability that more than one block will be generated in the system at a given time. First node, to solve the problem, broadcasts the block to rest of the network.
- Occasionally, however, more than one block will be solved at the same time, leading to several possible branches.
- However, the math of solving is very complicated and hence the blockchain quickly stabilizes, meaning that every node is in agreement about the ordering of blocks a few back from the end of the chain.

And that is accepted occasionally; however, more than one blocks will be solved at the same time leading to several possible branches; however, the matter of solving is very



complicated and hence the blockchain quickly stabilizes meaning that every node in the agreement about the ordering of the blocks a few back from the end of the chain.

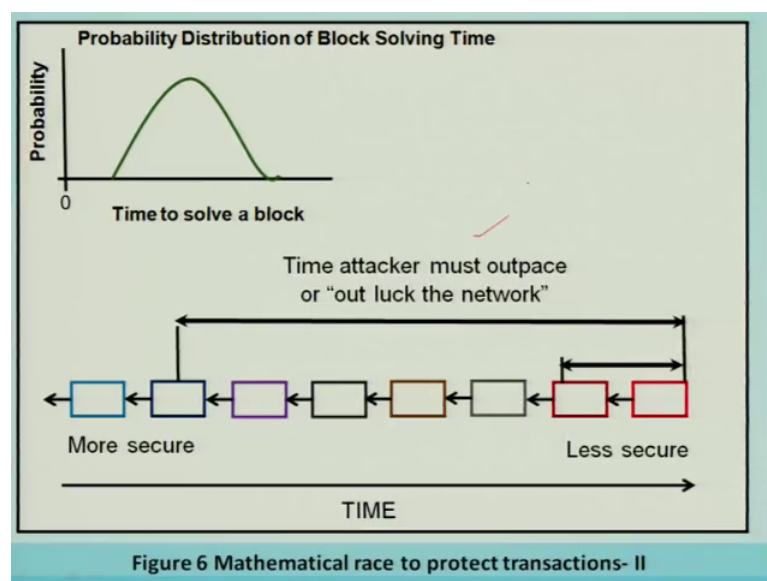
(Refer Slide Time: 15:56)

**Contd...**

- The nodes donating their computing resources to solve the puzzle and generate block are called **"miner nodes"** and are financially awarded for their efforts.
- The network only accepts the longest blockchain as the valid one. Hence, it is next to impossible for an attacker to introduce a fraudulent transaction since it has not only to generate a block by solving a mathematical puzzle but it has to at the same time mathematically race against the good nodes to generate all subsequent blocks in order for it make other nodes accept its transaction & block as the valid one.
- This job becomes even more difficult since blocks in the blockchain are linked cryptographically together.

So, the nodes donating their computing resources to find out the nonce are called minor nodes and they are financially awarded to obtain the nonce and basically continue in forming the longest proof of work chain. So, network only accepts the longest blockchain is the valid one hence it is next to impossible for an attacker to find out that.

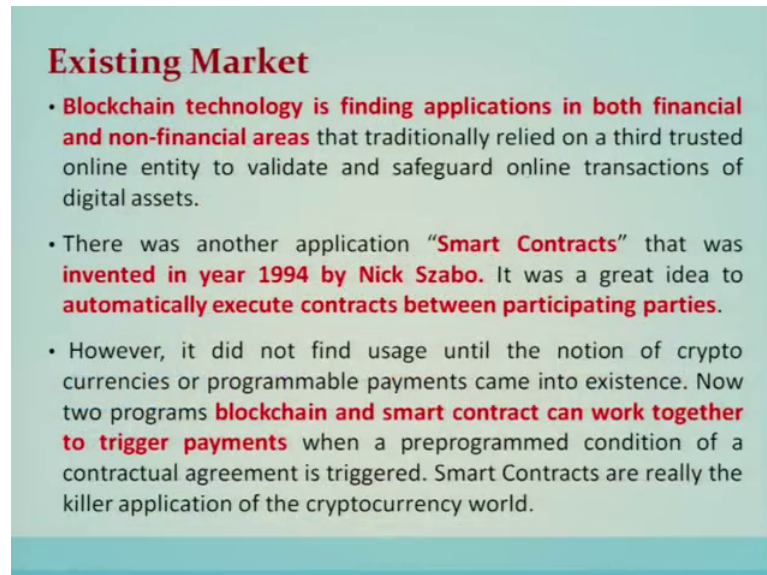
(Refer Slide Time: 16:29)





This particular example shows that the attacker must outpace or out of luck the network effort.

(Refer Slide Time: 16:42)

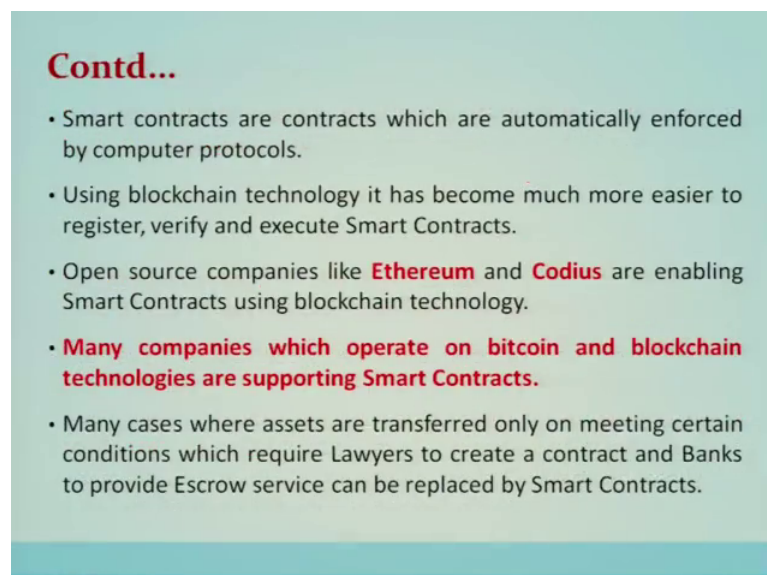


**Existing Market**

- **Blockchain technology is finding applications in both financial and non-financial areas** that traditionally relied on a third trusted online entity to validate and safeguard online transactions of digital assets.
- There was another application "**Smart Contracts**" that was **invented in year 1994 by Nick Szabo**. It was a great idea to **automatically execute contracts between participating parties**.
- However, it did not find usage until the notion of crypto currencies or programmable payments came into existence. Now two programs **blockchain and smart contract can work together to trigger payments** when a preprogrammed condition of a contractual agreement is triggered. Smart Contracts are really the killer application of the cryptocurrency world.

Which is becoming impossible as the chain length increases the existing market blockchain technology is finding application both in financial and non financial areas.

(Refer Slide Time: 16:55)



**Contd...**

- Smart contracts are contracts which are automatically enforced by computer protocols.
- Using blockchain technology it has become much more easier to register, verify and execute Smart Contracts.
- Open source companies like **Ethereum** and **Codium** are enabling Smart Contracts using blockchain technology.
- **Many companies which operate on bitcoin and blockchain technologies are supporting Smart Contracts.**
- Many cases where assets are transferred only on meeting certain conditions which require Lawyers to create a contract and Banks to provide Escrow service can be replaced by Smart Contracts.

That we have already discussed there are some open companies like Ethereum and Codius are enabling smart contracts. So, they are all already available in the literature.

(Refer Slide Time: 17:09)

### Contd...

- Also, there are a number of blockchains in existence to support wide range of applications—not just cryptocurrency. Currently there are three approaches in Industry to support other applications and also to overcome perceived limitations of Bitcoin blockchain:
- **Alternative Blockchains** is a system of using the blockchain algorithm to achieve distributed consensus on a particular digital asset. They may share miners with a parent network such as Bitcoin's--this is called **merged mining**. They have been suggested to implement applications such as **DNS, SSL certification authority, file storage and voting**.
- **Colored Coins** is an open source protocol that describes class of methods for developers to create digital assets on top of Bitcoin blockchain by using its functionalities beyond digital currency.

So, there are alternative a blockchain in the system of using blockchain algorithm to achieve distributed consensus on a particular digital asset they may share miners with a current networks such as Bitcoins and this is called a merged mining that coins is an open source protocol that describes the class of methods for developer to create digital asset on top of Bitcoin blockchain by using its functionalities beyond the digital currency.

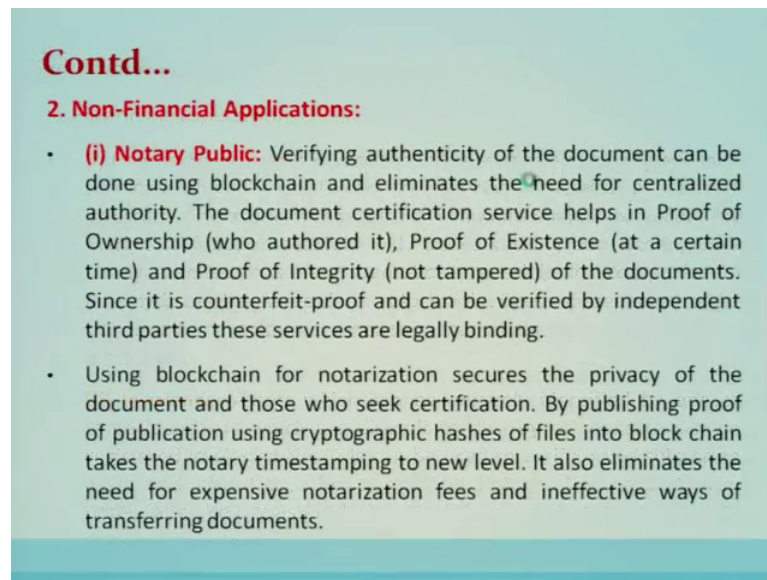
(Refer Slide Time: 17:38)

### Applications of Technology Compelling Use Cases in both Financial and Non-Financial Areas

#### 1. Financial Applications:

- **(i) Private Securities:** It is very expensive to take a company public. A syndicate of banks must work to underwrite the deal and attract investors. The stock exchanges list company shares for secondary market to function securely with trades settling and clearing in a timely manner. It is now theoretically possible for companies to directly issue the shares via the blockchain. These shares can then be purchased and sold in a secondary market that sits on top of the blockchain.
- **(ii) Insurance:** Assets which can be uniquely identified by one or more identifiers which are difficult to destroy or replicate can be registered in blockchain. This can be used to verify ownership of an asset and also trace the transaction history. Any property can potentially be registered in blockchain and the ownership, transaction history can be validated by anyone, especially insurers.

(Refer Slide Time: 17:41)



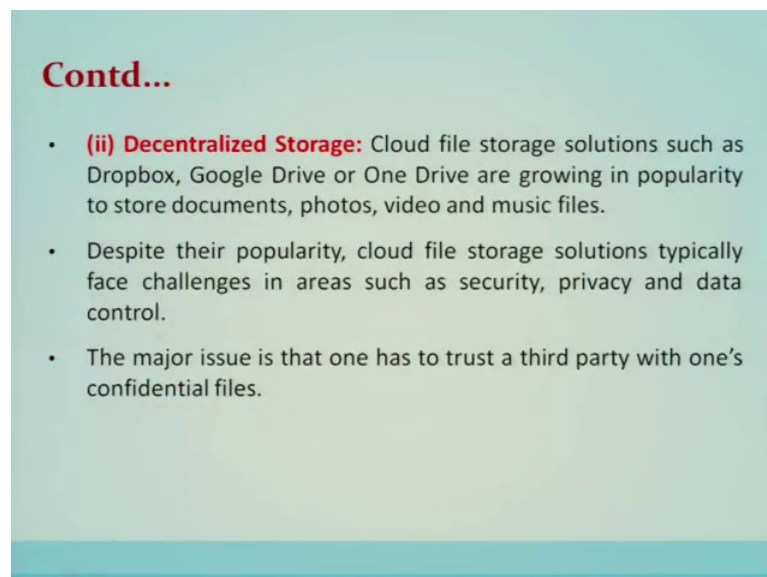
**Contd...**

**2. Non-Financial Applications:**

- **(i) Notary Public:** Verifying authenticity of the document can be done using blockchain and eliminates the need for centralized authority. The document certification service helps in Proof of Ownership (who authored it), Proof of Existence (at a certain time) and Proof of Integrity (not tampered) of the documents. Since it is counterfeit-proof and can be verified by independent third parties these services are legally binding.
- Using blockchain for notarization secures the privacy of the document and those who seek certification. By publishing proof of publication using cryptographic hashes of files into block chain takes the notary timestamping to new level. It also eliminates the need for expensive notarization fees and ineffective ways of transferring documents.

We various applications, we have already touched upon in the beginning another application is about the decentralized storage cloud file storage solutions.

(Refer Slide Time: 17:43)



**Contd...**

- **(ii) Decentralized Storage:** Cloud file storage solutions such as Dropbox, Google Drive or One Drive are growing in popularity to store documents, photos, video and music files.
- Despite their popularity, cloud file storage solutions typically face challenges in areas such as security, privacy and data control.
- The major issue is that one has to trust a third party with one's confidential files.

Such as Dropbox, Google drive and one drive are growing popularity to store documents photos videos music files despite their popularity cloud file storage solution typically face challenge in the area such as security privacy and data control the major issue is that one has to trust the third party with ones confidential file.

(Refer Slide Time: 18:08)

**Contd...**

- **(iii) Decentralized IoT:** The IOT is increasingly becoming popular technology in both the consumer and the enterprise space. A vast majority of IOT platforms are based on a centralized model in which as broker or hub controls the interaction between devices, However, this approach has become impractical for many scenarios in which devices need to exchange data between themselves autonomously. This specific requirement has lead to efforts towards decentralized IoT platforms.
- The blockchain technology facilitates the implementation of decentralized IoT platforms such as secured and trusted data exchange as well as record keeping. In such an architecture, the blockchain serves as the general ledger, keeping a trusted record of all the messages exchanged between smart devices in a decentralized IoT topology.

Hence there is another solution which is called decentralized IOTs; IOTs are increasingly becoming popular technology in both consumer and enterprise space vast majority of IOT platforms are built on centralized model in which as broker or hub controls the interaction between the devices; however, this approach can become impractical in many situations and need to exchange data between themselves autonomously.

(Refer Slide Time: 18:44)

**Contd...**

- **(v) Internet Applications: Namecoin** is an alternative blockchain technology (with small variations) that is used to implement **decentralized version of Domain Name Server (DNS)** that is resilient to censorship. Current DNS servers are controlled by governments and large corporations, and could abuse their power to censor, hijack, or spy on your Internet usage. Use of Blockchain technology means since DNS or phonebook of the Internet is maintained in a decentralized manner and every user can have the same phone book data on their computer.
- **Public Key Infrastructure (PKI) technology** is widely used for centralized distribution and management of digital certificates. Every device needs to have root certificate of the Certification Authority (CA) to verify digital signature. While PKI have been widely deployed and incredibly successful, dependence on a CA makes scalability an issue.

So, blockchain technology facilitates this decentralization of IOT in IOT platforms. So, there are many applications.

(Refer Slide Time: 18:47)

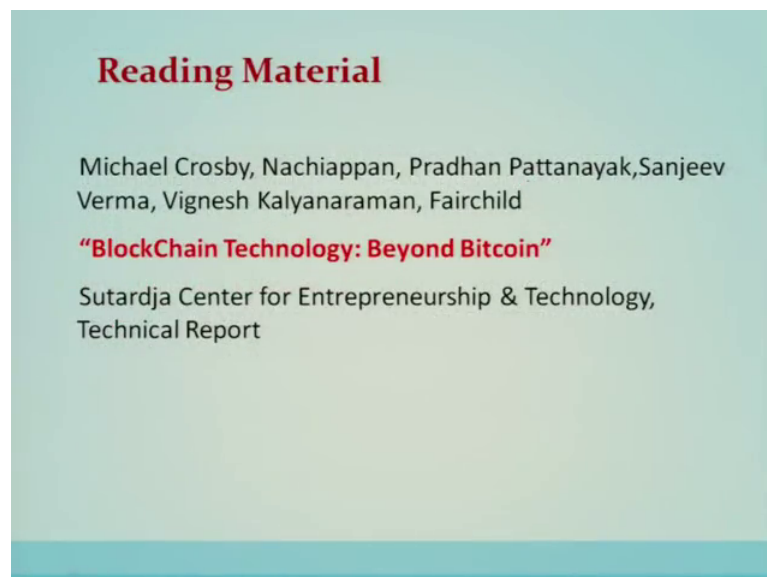


**Risks for Adoption**

- Blockchain is a promising breakthrough technology.
- There are vast array of applications or problems that can be solved using Blockchain based technology.
- That spans from Financial ( remittance to investment banking ) to non-financial applications like Notary services. Most of these are radical innovations.
- As it happens with adoption with radical innovations, there are **significant risks of adoption**.

Which is basically we have summarized in the form of these particular slides. So, there are reading materials available blockchain technologies beyond point.

(Refer Slide Time: 18:56)



**Reading Material**

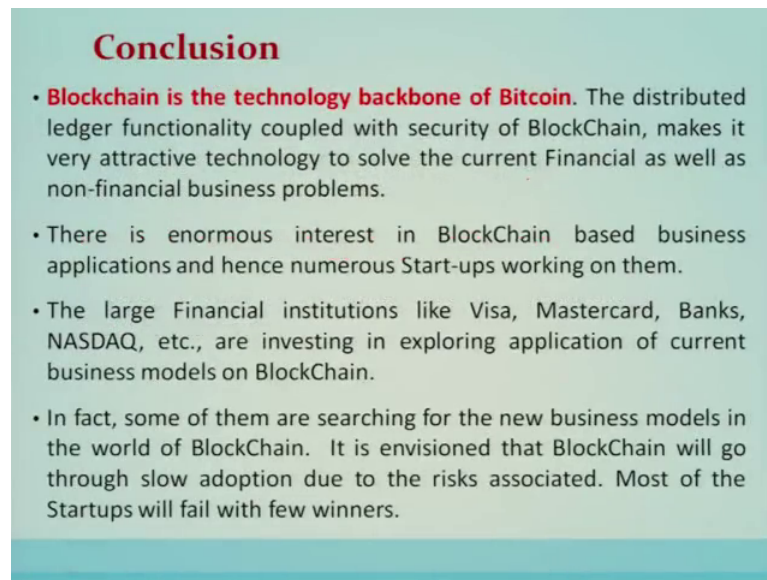
Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, Fairchild

**“Blockchain Technology: Beyond Bitcoin”**

Sutardja Center for Entrepreneurship & Technology,  
Technical Report



(Refer Slide Time: 19:02)



### Conclusion

- **Blockchain is the technology backbone of Bitcoin.** The distributed ledger functionality coupled with security of BlockChain, makes it very attractive technology to solve the current Financial as well as non-financial business problems.
- There is enormous interest in BlockChain based business applications and hence numerous Start-ups working on them.
- The large Financial institutions like Visa, Mastercard, Banks, NASDAQ, etc., are investing in exploring application of current business models on BlockChain.
- In fact, some of them are searching for the new business models in the world of BlockChain. It is envisioned that BlockChain will go through slow adoption due to the risks associated. Most of the Startups will fail with few winners.

So, that you can refer conclusion blockchain is the technology backbone for of Bitcoin the distributed ledger functionality coupled with security of blockchain makes it very attractive technology to solve the current financial as well as non financial business problems there is enormous interest in blockchain; these business applications enhance numerous startups working on it, we have to financial institution like these are must record or investing in exploring applications of the current business model or blockchain. In fact, some of them are searching for the new business models in the world of blockchain; it is envisioned that blockchain will go through slow adoption due to the risk associated most of the start of will fail with few winners.

Thank you.