Advanced Financial Instruments for Sustainable Business and Decentralized Markets

Prof. Abhinava Tripathi
Department of Management Sciences
Indian Institute of Technology, Kanpur

Week 9
Lesson 26

In this lesson, we start the discussion with centralized and decentralized ledgers. We also make a comparison between these two forms of ledgers. Then we introduce the concept of blockchain. We also discuss some key properties of the blockchains. Then we discuss the historical evolution of blockchains. Next we discuss the key characteristics of blockchains. Then we discuss permission vs permissionless blockchains and compare and contrast between them.

In this video, we will introduce the concept of centralized ledger. To begin with, the concept of a blockchain backed ledger has revolutionized the process of maintaining transaction records and verifications of the same. Particularly those domains where data immutability i.e. ability to alter data in an unsecured manner is paramount of importance and where the necessity to issue data integrity and subsequently identifying data tampering is at the core in various processes. Now based on this, ledgers can be classified based on the types of entities that can modify the ledger. In this backdrop, the ledger technology is classified as either centralized ledger technology, centralized ledgers and decentralized ledger technology as we will see shortly.

In the first case or centralized ledger technology, the data is transferred to a central node. This node has control over the entire ledger system as it is the only node capable of adding the data to the ledger. The ledger must be stored in a central repository and if necessary, access to it can be severely restricted. In contrast to this, a decentralized ledger or DLT will have numerous nodes that are able to control and update the ledger's data. So, in centralized ledger, CLT will have this key node affecting the access to data while in DLT, there will be multiple such nodes who have access and control and so on. So, thus in contrast to centralized ledger, the decentralized ledger will have numerous nodes that are able to control and update the data, creating a network of centralized ledgers, multiple such nodes and at each data update, all nodes will receive a new copy of the ledger, allowing them to remain in sync.

So, let us define these centralized ledgers. These central ledgers are like physical books or digital files used by individuals or organizations to record and aggregate economic transactions in a very centralized manner as opposed to decentralized ledgers used in distributed ledger technology as we discussed. Ledgers have been used since the earliest days of civilization to record and confirm the ownership of assets and the legal entity of individuals as well as their legal status and political rights. Here, the popularization of

double entry bookkeeping in the 16th century has revolutionized the use of ledgers in banking and accounting, which played a crucial role in expanding the economic system. The technique of recording every entry to an account along with the corresponding and opposite entry like asset liability, credit debit, in different accounts credit debit has significantly improved the accuracy of ledger records.

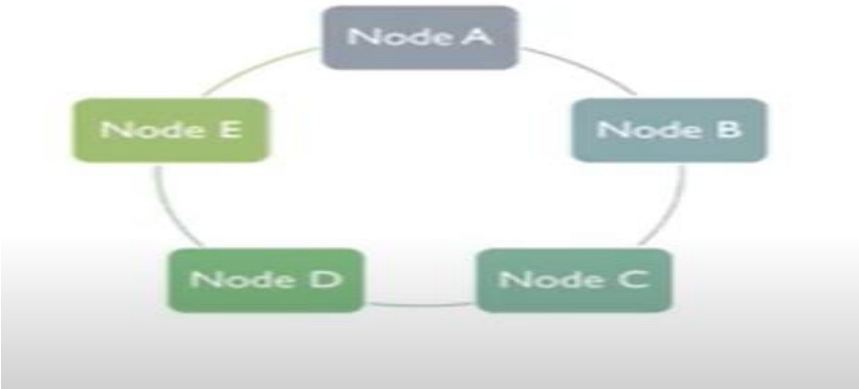
Traditionally, a central ledger is managed by the accounting department of a business to record all economic activity that the company is involved in for the purpose of financial analysis, tax reporting, and more. Although efficient, this approach has disadvantages. Relying on a central authority to manage all the bookkeeping makes the ledger vulnerable to any mistakes made by the authority either deliberate or accidental. More recently, the ledger technology has become the focus point for industry, academia and research due to its potential to change the way in which things are organized and the way collaboration takes place within various domains, such as supply chain, finance, healthcare, energy, telecommunication among others. Here ledger is the system of record for a business record, like asset transfer between participants, anything in the world that has a financial value needs a ledger.

A centralized ledger is administered and controlled by a single entity such as a business governed body or a financial institution. All the data is stored in a single location in a centralized ledger system and access to that data is controlled by authorized individuals or institutions. Now, these centralized ledgers are commonly employed in traditional financial systems like banks, where a central authority keeps and maintains the financial transaction data. For example, if you think of a bank, it might employ central ledger to maintain customer account balances of its clients, transaction histories and other financial information. While centralized ledgers can provide high levels of accountability, they can also have some downsides. For example, relying on a central authority to manage all bookkeeping makes the ledger vulnerable to any mistakes or some kind of cyber attacks in modern world, mistakes by that authority that are by just by chance or some kind of cyber attack or malicious attacks, they can be deliberate or accidental. For example, in the case of banks, the transactions that are posted on the centralized system, if the controlling authority shuts down abruptly, all the transactions will be terminated and cannot be processed. This can lead to a misrepresentation of transactions in the bank statement and it will affect all the bank's clients.

To summarize this video, we introduced the concept of centralized ledger, where a central authority keeps records of all the transactions happening in a system such as banks, which is of some financial value.

In this video, we will introduce the concept of decentralized or distributed ledger. To begin with, a distributed ledger or decentralized ledger is a type of database that is shared or replicated and synchronized among the members of the decentralized network. The

distributed ledger records the transactions such as the exchange of assets or data among the participants in the network. For example, here there are multiple nodes that are participants in this network that share the data. This distributed ledger technology is a more recent evolution of the concept of ledger that aims to decentralize the process of bookkeeping and remove the central authority which acts as a simple point of failure.



For example, Bitcoin's blockchain is one of the most successful examples of a decentralized or distributed ledger. Here, participants in the network govern and agree by consensus on the updates to the records in the ledger. So, the participants agree and govern and no central authority or third-party mediators such as financial institutions or clearing houses involved, like a central bank or some central counterparty. Every record in the distributed ledger has a timestamp and unique cryptographic signature, which makes this ledger and sort of auditable and immutable history of all transactions in the network. So, some unverified party or malicious attack cannot change the data or transaction records. Often this word decentralized and distributed are used interchangeably.

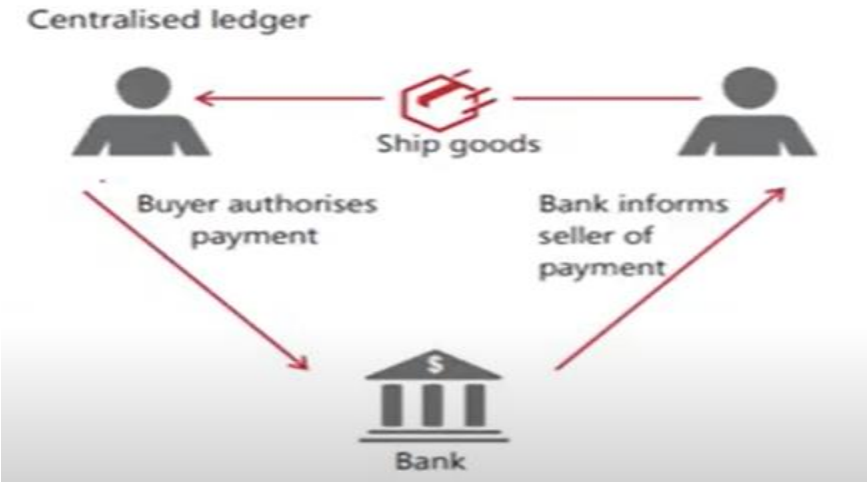
Decentralization here refers to the distribution of control or authority across multiple nodes, across multiple nodes like here. A distributed ledger, which is also known as shared ledger, it is a list of shared and synchronized data that are geographically spread across multiple sites. A distributed ledger is a database that is shared, synchronized and maintained by multiple participants like this multiple participants on board in a network. Blockchain is an example of a technology that is both decentralized in terms of control and authority and distributed in terms of ledger or database. Now here, the data is exactly replicated and synchronized across all the locations across all the locations ABCD and so on.

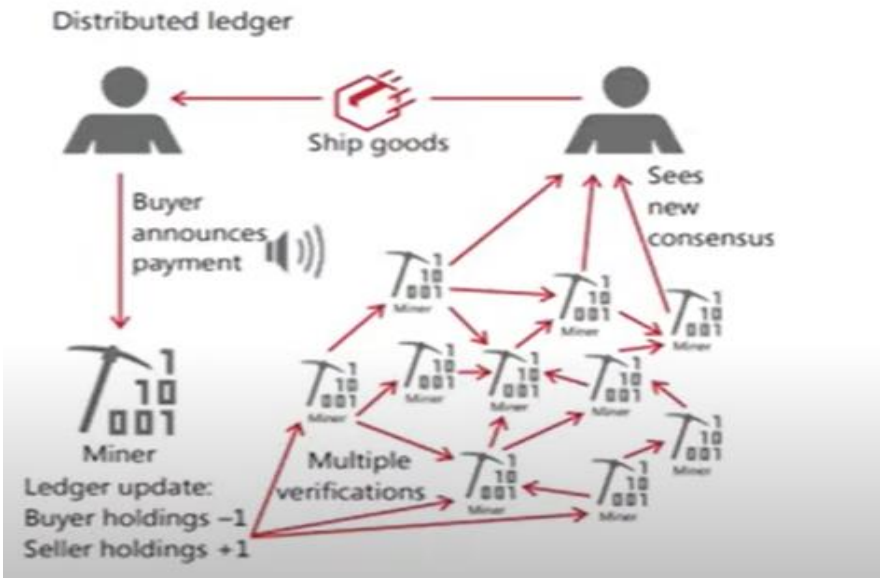
To maintain data integrity, availability and resiliency. Unlike the centralized system, there is no central administrator or single point of control. Here, all the participants within a network and network here is nothing but all the people who are connected to

each other with their computers, all such participants can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes or in fact, in few seconds. If a location abruptly fails or stops functioning, the remaining location, locations have the data and capacity to maintain the ledger or all transaction details in the absence of the failed location. This way distributed ledger provides real time information and reduced error of fail rates of transaction.

To summarize, in this video, we discussed distributed or decentralized ledgers. We noted that unlike a central ledger, here multiple nodes or multiple participants maintain the record and therefore, the possibility of failure is minimized for particularly the possibility of single party failure like a central party failure is minimized by sharing, maintaining and verification of records by multiple nodes and multiple locations thus reducing the risk of the system.

In this video, we will compare and contrast centralized and distributed or decentralized ledgers. Let us take an example where a buyer purchases goods from seller and the seller initiates the shipment upon perceived confirmation of the payment.





Now, this payment takes place via central authority which is bank. It is like a centralized ledger here. The buyer sends the payment instruction to their bank. The bank adjusts the account balances of the buyer by debiting the account of buyer, debit and crediting that amount to the seller's account and then bank confirms the payment to the seller. Now, think of the same transaction if it takes place through a decentralized ledger like a blockchain or Bitcoin.

Often this is called permissionless blockchain because here there is no central authority and no permission system is needed. So, these are like permissionless systems like cryptocurrency here. First, the buyer publicly announces the payment instruction stating that the cryptocurrency holdings of the buyer are reduced by 1 and those of the seller are increased by 1 unit depending upon the transaction volume. After a certain small delay, the miner includes this payment information in the ledger update. So a successful miner will update this information by solving the puzzle that this transaction has taken place.

So he will verify, he or she will verify the transaction and this information will be updated in the ledger. The updated ledger is subsequently shared with various other miners or nodes in the systems or users, each verifying that the newly added payment instruction is not a double spend or a, it is a genuine transaction, it is not a double spend or the same cryptocurrency has not been used earlier also. So it is a genuine transaction where cryptocurrency used for the first time, it is not a double spend attempt and it is authorized by the buyer. The seller then observes this transaction that the ledger and including the payment instruction, it emerges as the consensus. There is a consensus among all the nodes that the transaction has taken place.

So they are all verifying it through this consensus emerges and the proof of work of this miner is verified by all these nodes. So sort of they verify this transaction that is genuine

and the transaction concludes. This new information block as we will discuss later will be added to the blockchain and the chain will, this new transaction information will be augmented to the blockchain, the previous current blockchain, it will be augmented with this new transaction so that in future if new another transaction takes place, the next set of verification will use this additional information, the history of this particular cryptocurrency being transacted.

So to summarize in this video, we discussed centralized versus distributed or decentralized ledgers and how they operate.

Now, let us compare the characteristics of distributed and centralized ledgers. First and foremost, as the name suggests, the distributed ledgers are decentralized, so they are not centralized while centralized ledgers are decentralized, they are run by some kind of central party like a central bank or a government or some regulatory body and so on. The distributed ledgers are more suitable for large organizations with multiple ownership or shared across multiple nodes while centralized ledger is more suitable for small sized organizations where there is a central party controlling all the operations or transactions. In terms of speed and performance, distributed ledgers appear to be relatively slow because once a transaction is recorded on the distributed ledger, it cannot be changed or erased. So, erasing would be troublesome and therefore this ensures that the data integrity and accuracy is especially significant in sectors with centralized ledgers. These decentralized ledgers can be complex and difficult to understand making it difficult for them to deploy and manage and it necessitates specialized technical knowledge and expertise which might impede adoption and relatively slow.

In contrast, centralized ledgers are slightly faster, not as complex and the transaction is recorded with a central party which regulates and monitors the transaction data. In terms of cost, the cost of distributed ledgers can be slightly on the higher side because distributed ledgers struggle to scale to some large-scale applications or networks because they are serving large scale networks which limits their utility in some circumstances. As the number of nodes in the network increase, so does the complexity and time necessary to establish the consensus and potentially slowing down the network and increasing the cost as well. Because they rely on a large number of nodes to validate transactions because there is no central party, some of these DLT or decentralized ledger technology systems such as blockchain can be very energy intensive and costly. This can also be an environmental concern because the network requires a substantial amount of energy to sustain.

In contrast, the cost and energy requirements are lower for a centralized ledger because these centralized ledgers are more efficient and cost effective than decentralized ledgers especially for smaller organizations or those with limited resources. So, for there, these centralized ledgers are very useful. This is because the ledger can be maintained and

managed by a single counter party, single authority, eliminating the need for additional infrastructure or personnel. In terms of resilience, it is distributed in a distributed ledger because once a transaction is recorded on the distributed ledger, it cannot be changed or erased and thus ensuring the resilience and integrity and accuracy of the data. This is especially useful and significant when businesses where record keeping accuracy is critical such as health care, finance, banking, supply chain management and so on.

However, this may be an issue with the centralized ledger because there is a possibility of single point failure. For example, centralized ledgers are more vulnerable to cyber assaults than decentralized ledgers. A hacker who gains access to the centralized ledger may be able to compromise all of the data. So, there is no way to safeguard the original transaction or veracity of data as it was the case with distributed ledger. Coming to the control of information, here in distributed ledgers, it is decentralized because distributed ledgers are not controlled by a single body. No single party can modify the data or transactions recorded on the ledger. This increases transparency and accountability as well as security and resilience. Moreover, transparency is provided by distributed ledgers by making all transactions accessible to all network participants. There is especially vital industries that require transparency and accountability such as banking, health care and government.

In contrast, with centralized ledger, there is a single point of control. So, because a centralized ledger is administered and controlled by a single entity, data access can be tightly regulated and monitored. This makes it easier to maintain the data security and integrity while also lowering the chance of unauthorized access or modification. Here it is important to note that in the case of distributed or decentralized ledgers, they eliminate the need for intermediaries and allow for faster, more secure transactions. They can be more efficient than centralized ledger in some cases. This is especially significant areas that require speed and efficiency such as finance and logistics.

So, you do not need to wait for a central party to verify. In contrast, if you look at centralized ledgers with single point of control, this attribute is different because centralized ledgers provide organizations with greater data control. So, there is slightly control is more, which reduces the freedom and flexibility. Sometimes control can be beneficial in areas where data privacy and security are vital. This can also make it simpler to meet regulatory obligations.

Also, because centralized ledgers are maintained by a single institution, it might be difficult for outsiders to verify the data correctness and completeness. This can be a problem in industries that value transparency and accountability. So, there is a certain less flexibility and more control with centralized ledgers.

Lastly, coming to the aspect related to authorization and authentication, it is more direct with distributed ledgers. They use some kind of cryptographic verification. So, these distributed ledgers secure data using some cryptographic techniques, making them resistant to hacking and other forms of cyber assault. This is because the network verifies and approves each transaction on the ledger, making it incredibly difficult to alter or tamper the data. Because these distributed ledgers are frequently decentralized and distributed and not controlled by a single body, it can be difficult to regulate. And this can pose difficulties for authorities who must verify that the technologies use safely and securely. Now, while this DLT enables transparency, it can also bring privacy concerns.

In other circumstances, the ledger transparency makes it difficult to protect sensitive information. So, there is some sensitive information that is a concern. In other circumstances, the ledger transparency makes it difficult to protect sensitive information, which might be a risk in industries such as healthcare or finance. Now, let us contrast this with the centralized ledger. In the centralized ledger, the authentication and authorization is done by a central party.

Because central ledgers are frequently managed by a single party, large data access might be restricted. So there is a restriction to data access and outside parties may have restrictions from using the data or developing new applications that rely on it as a result. And because all data is stored in a single location that is managed by a single body, centralized ledgers can give data that is consistent and reliable, so slightly more reliable. This is especially crucial in the cities where precise data is required such as finance, healthcare or government. While centralized ledgers can provide strong control, consistency and efficiency, they can also be prone to cyber-attacks and assaults. They may be opaque and subject to political or economic pressure because of these some of these disadvantages, decentralized ledger solutions such as blockchain have gained a lot of popularity.

So to summarize in this video, we contrast and compared centralized and distributed ledgers across different attributes and also saw an example how they function.

In this video, we will introduce the concept of blockchain briefly to a non-technical audience. To begin with, technology is developing rapidly and since their invention calculators, computers and smartphones have proven as technological advances. However, today the internet and intellectual technologies have reached such a level that there is a need to rethink a traditional way of living including fundamental conceptions of law and state.

One of these technological advances is blockchain that has gained popularity along with the virtual currencies. In terms of technology such as public version of blockchain, it is an encrypted distributed database that everyone with enough technical resources can

access on the internet. So we are talking about public blockchain more specifically. Here each participant plays the role of member and a center what we call as node simultaneously. The distinguishing features of blockchain lie in its peer-to-peer communication structure, cryptography, distributed ledger and consensus mechanism.

Among them, the peer-to-peer network and distributed ledgers help blockchain participants eliminate the centrality of controlling authorities like central bank. While in the centralized systems, blockchains need trusted third parties such as banks or administrative agencies for their enforcement. Blockchain replaces such intermediary mechanisms with distributed public ledgers. As a result, in a trust-free blockchain network, the transactions can be enforced freely and untrustworthy across the peers. But the absence of central authorities does not self-make the network untrustworthy.

The cryptology behind blockchain ensures the trust sought by the parties to transactions. In this way, the parties can overcome almost all the possible security gaps on the blockchain. Now, meanwhile, the secret inventor of the Bitcoin virtual currencies Satoshi Nakamoto, whose mystery was contributed the worldwide fame of blockchain, he also introduced he or maybe a group of people introduced routine escrow mechanism. So these routine escrow mechanisms to replace the trusted third parties in centralized transaction systems. Now this routine escrow mechanism those of us are familiar with banking, they very well know what escrow mechanism is.

And they can be preferred to build a trusted relationship between vendors and recipients. For example, in banking, there's a escrow account maintained by the bank or a third party which one money is released or locked unless until the responsibility or duty is done by one of the party. So using this mechanism instead of directly releasing the payment to the vendor account, the recipients can send the routine escrow and block it until the performance of the contract similar to what we see in banking. And as soon as the vendor performs the contract following the previously agreed terms, this escrow kind of account escrow which locks the money before paying to the vendor. And as soon as the vendor performed the contract following the previously agreed terms, the routine escrow as a service provided instructs the payment to the vendor's account.

So then both vendors and recipients are expected to trust the routine escrows. And on the blockchain participants interact in the assigned nodes via private and public keys. They sign a transaction on the blockchain via private keys but send the transactions to another participant's address via their public keys. So these transactions are validated by other participants and are gathered in the candidate blocks that once validated by the blockchain network and are added to the chain and this process renews the network regularly.

So these are sort of block set of blocks. A new transaction is created which is verified and then added to this block and chain moves on. Further chain is augmented. So each recently validated block takes the address of the previous one and the chain is made from these encrypted blocks that is the blockchain and that is why any change in one block affects the entire chain. So if one block is affected, it will affect all the blocks and to modify the information in one block thus it requires some modification in the entire chain which is hardly possible. Now there are several advantages to this kind of structure of blockchain.

For example, there is testworthiness, transparency, traceability and decentralization. And here blockchain stores data in multiple nodes. Multiple nodes, there are multiple nodes that store data instead of a centralized intermediary. So instead of centralized intermediary earlier, not this. So now you have multiple nodes that are there and store data which makes it very difficult to hack because any security threat must be directed to at least 51% of these nodes because these nodes will ultimately verify and based on consensus mechanism at least 51% consensus would be needed.

So a threat must be directed to at least 51% of these nodes to alter the structure or alter the transaction data and become successful. Additionally, because the transactions on the blockchain are encrypted and blocks that are chained to each other. So the blocks that we were discussing are chained to each other. Any change on the block requires the consensus or consent of the majority. So majority consensus of these blocks would be required to alter this blockchain.

If that majority quota is not reached, neither transactions nor data can be interfered with or changed nor are registered transactions amended or removed from the distributed ledger. So to modify, alter or vitiate this chain, one needs to get the consensus of 51% of the node. And because of these, this is almost next to impossible given the cryptography involved. And therefore, these advantages trigger the application of blockchain to various sectors of life like agriculture, banking, law, economics and political elections and so on.

So to summarize in this video, we introduced various features of blockchain. And we noted that this blockchain structure seems to be very trustworthy and very safe and very difficult to modify the data and transaction or play or vitiate the data or structure encoded in this.

In this video, we will carry on with our discussion about blockchain properties. So blockchain is a type of ledger technology that stores and records the data. At the very basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operations of the blockchain network, no transaction can be changed once published. Next, blockchain also can be thought of as a list of records called blocks that store data publicly in a chronological order.

The information is encrypted using cryptography to ensure that the privacy of the user is not compromised and data cannot be altered. Blockchains are in a way distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Therefore, they are also considered as distributed ledgers or decentralized ledgers and there's only one ledger and all nodes have some level of access to that ledger. Now blockchains are tamper evident and tamper resistance digital ledgers implemented in a distributed fashion that is without a central repository and usually without a central authority like a bank, central bank, government or a company and each block is like a page of a ledger or record book. Also, information on blockchain network is not controlled by a centralized authority.

So this is unlike modern financial institutions like central banking. The participants of the network maintain the data and they hold the democratic authority to approve any transaction that can happen on the blockchain network and therefore a typical blockchain network is like a public blockchain. So as long as you have access to the network, you have access to the data within the blockchain. If you are a participant in the blockchain network, you will have the same copy of the ledger that all the participants have and each blockchain contains a set of transactions and other related data. Here each block is comprised of a block header containing metadata about the block. Such distributed ledger provides various advantages in terms of decentralization, security, transparency, immutability and efficiency.

Let us now understand the blockchain in its form as a block and chain. So if you look at the block in the blockchain, data is stored digitally in a record called a block. This block contains first block header, which has the information about the block such as the unique block reference number, the hash, the header also includes the hash of the previous block, the time when the block was created. There is also block content, which includes the record itself, for example, information about a transaction. The block acts like a ledger entry for this transaction.

Then we have the chain. So the blocks form a chronological order of database of transactions that is shared between multiple nodes, that is computers and servers in that network. Each block contains the reference of the block before it, meaning that they link together to form a chain, sort of linkage between across the blocks and altering the content of the block changes the hash of the block. So this impacts the previous blocks in the chain and alerts members. This ensures that the blockchain is secure.

To summarize, in this video, we discussed some of the key features of blockchain. We also discussed the composition of blockchain separately as a block and as a chain.

In this video, we'll continue with our discussion of blockchain properties. A blockchain is a tamper evident shared digital ledger that records transactions in a public or private peer

to peer network. In particular, the public blockchain is like a ledger distributed to all the member nodes in the network. The ledger permanently records the history of asset exchanges that take place between the peers in the network in a sequential chain of cryptographic hash link blocks.

All the confirmed and validated transaction blocks are linked and chained from the beginning of the chain to the most current block and hence the name blockchain. The blockchain thus acts as a single source of truth and members in a blockchain network can view only those transactions that are relevant to them. So in a way, blockchains are tamper evident and tamper instant digital ledgers implemented in a distributed fashion that is without a repository and usually without a central authority like bank, company or government. Now at the very basic level, they enable a community of users to record transactions in a shared ledger within that community such that under normal operation of the blockchain network, no transaction can be changed once published. For example, in 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies which is like electronic cash protected through cryptographic mechanisms instead of central repository or central authority.

Furthermore, blockchains are like distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. So each block is cryptographically linked to the previous one after validation and undergoing a consensus decision which makes it tamper evident and as the new blocks are added, older blocks become more difficult to modify, which makes it tamper resistant and the new blocks are replicated across copies of the ledger within the network and any conflicts are resolved automatically using established rules. Now this technology became widely known in 2009 with the launch of Bitcoin network, the first of many modern cryptocurrencies and in Bitcoin and similar systems that transfer digital information that represents electronic cash takes place in a distributed system. So Bitcoin users can digitally sign and transfer their rights to that information to another user and the Bitcoin blockchain records this transfer publicly allowing all the participants in that network to independently verify the validity of the transaction. So this Bitcoin blockchain is independently maintained and managed by a distributed group of participants and this along with cryptographic mechanisms makes the blockchain resilient to attempts to alter the ledger later on, that is modifying blocks or forging transactions in a duplicious manner.

So blockchain technology has thus enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum and because of this blockchain technology is often viewed as a bound to Bitcoin or possibly cryptocurrency solutions in general. However the technology is available for a wide variety of and broader variety of applications and is being investigated for various sectors applications. Also the numerous components of blockchain technology along with its reliance on cryptographic primitives and distributed

systems can make it challenging to understand. However each component can be described simply and used as a building block to understand the larger complex system. This can be informally defined as for example blockchains are like distributed digital ledgers of cryptographically signed transactions that are grouped into blocks.

Each block is cryptographically linked to the previous one making it tamper evident after validation and undergoing consensus decision. As new blocks are added older blocks become more difficult to modify which creates tamper resistance. So new blocks are replicated across copies of the ledger within network and any conflicts are resolved automatically using established rules. Lastly a blockchain is an ever-increasing chain of blocks of data and each block contains a record of a change or transaction that is logged in a chronological order and secured using cryptography.

Once added records are in effect permanent and immutable. So they cannot be lost or denied and if something is recorded on a blockchain it's deemed to be by users to be true. Group verification removes the requirement of intermediaries and anyone can access the record to verify that a transaction has taken place.

To summarize in this video we discussed some of the key properties of blockchain like tamper resistance and tamper evident which make it immutable, verifiable and secure from malicious attacks and attempts to, duplicious attempts to change or modify the transaction data or any such data.

In this video we will conclude our discussion about the blockchain properties. To begin with let us discuss the key differences in the blockchain and traditional ledgers. The three key differences in how blockchain differs from more familiar ledgers include propagation that is how new transactions originate with one user but propagate to a network of identical ledgers without a central controller. Then in permanence all transactions and records on blockchain are permanent and unable to tamper or remove. Programmability so many blockchains are programmable allowing for automation of new transactions and controls via smart contracts. Then let us discuss the formation of chains in blockchain.

So there are five components first is the transaction. Here two parties agree to make a transaction it could be of any asset that can be described in additional format for example transaction of money, contracts or deeds. Then we have smart contracts in some of the blockchains. A smart contract is a piece of software that sits within a blockchain and act as a digital contract for the transaction. At this stage data is entered relating to the contract such as the price, information about the product, order quantity and delivery date and so on. When the agreed terms are met the smart contract automatically triggers the action that requires verification. So next step is verification which is the record of the transaction that becomes a new block containing the transaction details a unique hash and reference to the previous blocks hash.

It is a sequence of linked hashes that creates a secure chain between blocks. Next we have the step called validation so for a new block to become part of the chain it must be validated by a group of nodes or the users in the blockchain by an agreed consensus mechanism which we will be discussing shortly and then distribution and wider network. So once a block has been validated it is added to the blockchain and distributed to all the members of the network. The transaction is recorded in near real time without the need for a third party and is held in a distributed ledger that cannot be altered. A very important key term here is consensus mechanism. Now consensus mechanisms make blockchain more secure by making it labor intensive to tamper with the blocks and different blockchains use different mechanisms.

One common mechanism is called proof of work where servers within the network or nodes solve a mathematical puzzle derived from the blocks header to validate the record. To change a block would mean solving mathematical puzzles for all the blocks in the chain and this would take a lot of time giving members of the network time to identify that the change is taking place. Lastly there is something called a distributed ledger. So rather than having a one single owner blockchain records are spread out among all their users the genius or the skill of this approach is in using a complex system of consensus and verification to ensure that even with no central owner and with the time lags between all the users there nevertheless remains a single agreed upon version of the truth. So here each participant in a blockchain which is also called node keeps a copy of all the historical transactions that have been added to the ledger and by comparing to the other node copies each record is kept synchronized and verified.

Unlike in a traditional ledger system there is no node with special rise to edit or delete the transactions in fact there is no central party at all and one of the situation in which blockchains can be useful is when tested central parties either unavailable or too expensive.

To summarize in this video we discussed some key attributes of the blockchain vis-a-vis traditional ledgers such as propagation, permanence and programmability. We also discussed the components of chain in the blockchain which included transaction, smart contracts, verification, validation and distribution via wider network. We also discussed consensus mechanisms and some of the properties of blockchain as distributed ledger.

In this video we will discuss the historical evolution of blockchain. Blockchain was officially introduced in 2009 with the release of its first application the bitcoin cryptocurrency. But its roots reached back several decades earlier many of the technologies that form the basis for blockchain today were in the works long before the emergence of bitcoin. Although blockchain as an entity has a relatively short history its influence today is widespread and its applications wide ranging and growing. Through the decades blockchain's development and evolution includes some of the very notable

developments. For example pioneers like Merkle and his Merkle tree, charm with digital cash, haber with time stamping, doff with proof of work, black and hash cash, fini with reusable proof of work dotted the early years of the pre-blockchain landscape.

Let us try to understand the evolution of blockchain over the years. In 1979 one of the early pre-blockchain technologies was the Merkle tree named after the computer scientist and mathematician Ralph Merkle. He described an approach to public key distribution and digital signatures called tree authentication in his PhD thesis. Merkle eventually patented this idea as a method for providing digital signatures. The Merkle tree provides a data structure for verifying individual records. Subsequently in 1982 David Chom described a vault system for establishing maintaining and testing computer systems among mutually suspicious groups.

The system emptied many of the elements that comprise a blockchain. Chom is also credited with inventing digital cash in 1989 and founded a company called DG Cash. Then in 1991 Stuart Haber and Scott Stornetta published an article on how to timestamp digital documents to prevent users from backdating and forward dating electronic documents. The goal was to maintain the documents complete privacy without requiring record keeping by a timestamping service. Haber and Stornetta updated the design to incorporate Merkle trees which enabled multiple document certificates to live on a single block.

Subsequently various other developments took place for example between 1993 to 1999. There was beginning of proof of work concept which was published in a paper by Cynthia Dok and Moni Naur to provide a computational technique for combating junk mail and in particular controlling access to a shared resource. Then in 1997 Adam Black introduced Hashcash and a proof of work algorithm that provided denial of service countermeasures. And in 1999 Marcus Jacobsen and Eriju has published the term proof of work and the peer-to-peer network was popularized by the now defunct peer to peer file sharing application Napster. Some argued that Napster was not a true peer to peer network because it used a centralized server but the services will help breathe life into the peer to peer networking making it possible to build a distributed system that could benefit from the computer power and storage capacity of thousands of computers. Then subsequently from 2000 to 2004 Stephen Const introduced the concept of cryptographically secured chains in his paper.

These secured chains are secured log files based on cryptographically concatenated entries. His model which showed that entries in the chain can be traced back from the genesis block to prove authenticity was the basis for today's blockchain models. And then in 2004, Halfen introduced reusable proof of work, a mechanism for receiving non-exchangeable or non-fungible hashcash tokens in return for an RSA signed token. The proof of work approach today plays a vital role in Bitcoin mining and crypto-conceives

like Bitcoin and Litecoin use this proof of work approach and Ethereum shifted to the proof of stake protocol to secure a network using a fraction of the energy that proof of work uses. Subsequently in 2008, a major development took place where Satoshi Nakamoto who thought to be a pseudonym used by a group of individuals published a white paper introducing the concept of cryptocurrency and blockchain and helped develop the first Bitcoin software. This blockchain infrastructure according to the white paper would support secure peer to peer transactions without the need for trusted third parties such as banks or governments.

This Bitcoin blockchain architecture was introduced and built on technologies and concepts from the previous few decades and Nakamoto's design also presented the concept of a chain of blocks making it possible to add blocks without requiring them to be signed by a trusted third party. Nakamoto defined an electronic coin as a chain of digital signatures in which each owner transfers the coin to the next owner by digitally signing a hash of the previous transaction in the public key of the next owner and adding these to the end of the coin. Thus, cryptocurrency was launched during the Great Recession when the government pumped large amounts of money into the economy and Bitcoin was worth less than a penny then. Nakamoto mined the first Bitcoin block validating the blockchain concept.

The block contained 50 Bitcoins and was known as the Genesis block aka Block 0. Nakamoto released Bitcoin B0.1 to the web service Sourcewatch as open-source software. Now it is on GitHub. In the spirit of cryptocurrency as money with fixed supply, Nakamoto set up a system to ensure that number of Bitcoin mined would not exceed 21 billion. Subsequently, a number of important developments took place. For example, in 2010, Bitcoin made history when programmer Laszlo Hans says pay 10,000 Bitcoins for two delivered pizzas.

A short time later that year, programmer Jed McCallop launched Mongox, a Tokyo-based Bitcoin exchange. Mongox was short of magic the gathering online exchange, a carrier from the FadC card game. At its peak, Mongox handled more than 70% of all Bitcoin transactions. Around 2011, almost 25% of the 21 million Bitcoin had been mined and by early February, the value of Bitcoin was equal to the US dollar. In 2012, the interest in cryptocurrency solidified and Bitcoin's price hoarded around $5 for most of the year with several fluctuations.

Then in 2013, Bitcoin again gained an upward trajectory that continued. In February, Coinbase reported selling $1 million worth of Bitcoin in a single month at more than $20 each. By end of March 2013, with 11 million Bitcoin in circulation, the currency's total value exceeded $1 billion. However, it was not all good for digital currency world as both Thailand and China banned cryptocurrencies. The US federal court seized Mongox funds in the US for transmitting money without license. In 2015 and 2014, despite setbacks,

one of the more important milestones in blockchain history occurred when Bitcoin magazine co-founder Bertrand published a white paper proposing a decentralized application platform leading to the creation of Ethereum and Ethereum Foundation.

Subsequently, financial institutions and other industries began to recognize and explore blockchain's potential, shifting their focus from digital currency to the development of blockchain technologies per se. But Bitcoin remained in the spotlight for better or worse. In 2015, the Ethereum Frontier network launched enabling developers to write smart contracts and decentralized apps that could be deployed to a live network. In 2016, the term blockchain gained acceptance as a single word rather than being treated as two concepts as they were in Nakamoto's original paper.

And in 2017, Bitcoin hit a record high of nearly $20,000. In fact, Japan recorded Bitcoin as a legal currency and several European banks formed the Digital Trade Chain Consortium to develop a trade finance platform based on blockchain. In 2018, which was the 10th year of Bitcoin, its value continued to drop, ending the year at about $3,800. The online payment firm Stripe stopped accepting Bitcoin payments. Google, Twitter and Facebook banned cryptocurrency advertising.

In 2019, Walmart launched a supply chain system based on Hyperledger platform. Amazon announced general availability of its Amazon managed blockchain service on AWS to help users build resilient web 3.0 applications on public and private blockchains. Ethereum network transactions exceeded 1 million per day and blockchain research and development took center stage as organizations embraced this blockchain technology. In 2020, a Deloitte survey revealed that nearly 40% of respondents incorporated blockchain into production and 55% viewed blockchain as a top strategic priority.

In 2021, Bitcoin reached an all-time high of $68,789. During its bull run, the Bitcoin market surpassed $3,000,000. Now interest in using blockchain for applications other than cryptocurrency continued as governments and enterprises considered blockchain for a variety of use cases including voting, real estate, fitness tracking, intellectual rights, IoT and vaccine distribution among others. The global blockchain technology market was valued at around $6 billion in 2021 and has been surpassing a trillion dollars by 2030. It is expected to surpass a trillion dollar by 2030, according to market researcher from Statista. In 2022, NFTs continued ascent on eco-friendly blockchain network emerged and blockchain applications increased among companies. In fact, Bitcoin mining crypt closed to Nakamoto’s 21-million-coin limit, reaching 19 million and leaving less than 10% of Bitcoin to be mined.

Blockchain's promise of secure and transparent transactions without the need for intermediaries will potentially change the way enterprises conduct practically every aspect of their daily business operations for decades to come. Technologies like AI, IoT

and NFTs and the metaverse will be significantly impacted by blockchain technology. For example, Gartner picks the business value of blockchain at more than $360 billion by 2026. It is modest when compared to the firm's estimate of $3.1 trillion by 2030.

To summarize this discussion, the core ideas behind blockchain technology emerged in the late 1980s and 90s. Starting from 1989 when Leslie Lamport developed the Paxos protocol and in 1990 submitted the paper, the part-time parliaments to ACM transactions on computer systems, the paper was finally published in a 1998 issue. In 1982, David Chom proposed the first ever blockchain-like protocol in his dissertation. In 1991, a signed claim of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed. These concepts were combined and applied to electronic cash in 2008 and described in the paper Bitcoin, a peer-to-peer cash system, which was published as a pseudonym by Satoshi Nakamoto and then later in 2009 with the establishment of Bitcoin cryptocurrency blockchain network.

One can essentially say that Bitcoin was just the first of many blockchain applications in that sense and electronic cash schemes in particular existed before Bitcoin like e-cash and net cash but none of them became as popular as Bitcoin. In fact, the use of blockchain enabled Bitcoin to be implemented in a distributed fashion with no intermediary such that no single user controlled the electronic cash and no single point of failure existed. This promoted the use of Bitcoin and this eliminated the need for a trusted third party. Many in fact cash schemes existed prior to Bitcoin but none of them achieved its widespread use. The use of blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed promoting the use of Bitcoin.

The primary benefit of Bitcoin was to enable direct transactions between user to users without the need for a trusted third party. So it also enabled the issuance of a new cryptocurrency in a defined manner to those users who could manage to publish new blocks and maintain copies of the ledger. Such users are called miners in Bitcoin. The automated payment of the miners enabled distributed administration of the system without the need to organize. By using a blockchain and consensus-based maintenance, a self-policing mechanism was created that ensured that only valid transactions and blocks were added to the blockchain.

In Bitcoin, the blockchain enabled users to be pseudonyms. This means that users are anonymous but their account identifiers are not. Additionally, all transactions are publicly visible. This has effectively enabled Bitcoin to offer pseudo-anonymity because accounts can be created without identification or authorization process and such processes are typically required for know your customer loss. Since Bitcoin was pseudo-anonymity and anonymity was there, it was essential to have mechanism to create trust in that

environment where users could not be easily identified. Prior to the use of blockchain technology, this trust was typically delivered through the intermediaries trusted by both parties around a transaction.

In this video, we will discuss some of the key characteristics and features that are inherent to blockchains. Since Bitcoin was pseudonymous, it was essential to have mechanism to create trust in an environment where users could not be easily identified. Prior to the use of blockchain technology, this trust was typically delivered through intermediaries trusted by all the parties in the transaction. Without these trusted intermediaries, the needed trust within a blockchain network is enabled by four key characteristics of the blockchain technology as we discuss here. First, the ledger. The ledger technology uses an append-only ledger which means that the data can only be added to the blockchain in time-ordered sequential order.

This property implies that once the data is added to the blockchain, it is almost impossible to change the data and can be considered practically immutable. And therefore, it provides full and correct transactional history. Unlike traditional databases, transactions and values in a blockchain are not overridden.

So this is like an append-only ledger. Here you can only add new information, you cannot modify the historical information. Next, it is a secure database with blockchains. So the blockchains are cryptographically secure, ensuring the data contained within the ledger has not been tampered and that the data within ledger is attestable. So this data within these ledger is auditable.

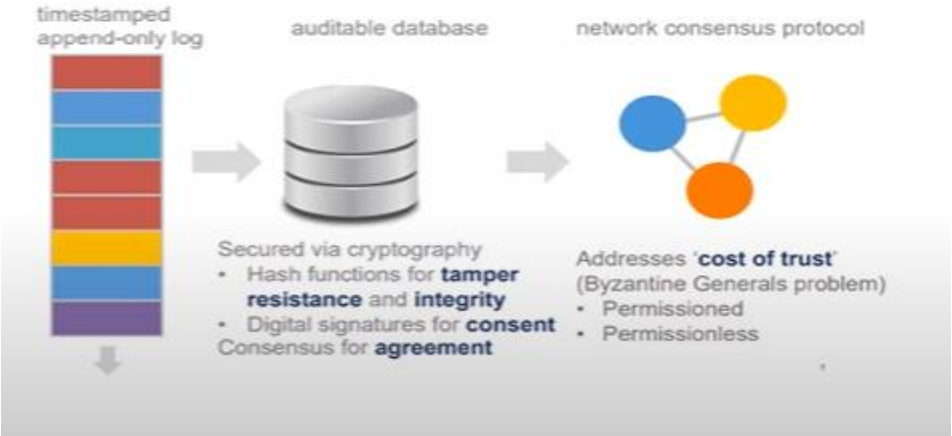
It is secured via cryptography. So it is tamper-resistance and its integrity is ensured through cryptography. Lastly, it is shared as well. So the ledger is shared among multiple participants or nodes on the blockchain. This provides transparency across the node, participant in the blockchain network and it is distributed. So this blockchain can be distributed. This allows scaling the number of nodes of a blockchain network to make it more and more resilient to attack by the bad actors like phishing attacks. By increasing the number of nodes, the ability of the bad actor to impact the consensus protocol, which we will discuss later, the consensus protocol used by blockchain is reduced.

So later whatever changes to the or transactions have been added, that is verified through a consensus mechanism. And as more and more nodes enter, the consensus mechanism becomes more and more robust. It becomes even more difficult to modify it. Later we will discuss there are two kind of blockchains. One is permissioned on private and permissionless or public. So most of the discussion focuses like instrument like Bitcoin with permissionless tokens, which address the issue of cost of trust or what we call as Byzantine journals problem.

Because of this consensus mechanism, it ensures that even if one or two nodes have gone bad, the entire mechanism is robust to any such phishing or malicious attacks. The data is verified by majority of the nodes and remains and maintains the integrity of the data. And therefore, by using this blockchain enabled instruments like Bitcoin, which is implemented in a distributed fashion such that no single user controls the instrument like electronic cache and no single point of failure exists. This promotes the use of blockchain based instruments and its primary benefit is to enable direct transaction between users without the need for a trusted third party. It also enables the issuance of instruments like new cryptocurrencies in a very defined manner to the users who manage to publish new blocks and maintain copies of the ledger and such users are called miners or nodes in this blockchain.

The automated payment of miners enable distributed administration of the system without the need to organize around the central counterparty. So thus by using a blockchain and consensus based maintenance, a self-policing mechanism is created that ensures that only valid transactions and blocks are added to the blockchain. So only valid transactions are added to the blockchain. Lastly, in an instrument like Bitcoin, the blockchain enabled users to be pseudonymous. This means that users are anonymous but their account identifiers are not anonymous. Additionally, all transactions are publicly visible. This has effectively enabled Bitcoin to offer pseudo anonymity because accounts can be created without any identification or authorization process. Such process are typically required as know your customer rules by banks in India and across the world.

Here let us quickly summarize this blockchain technology through this diagram that we can see here. So this is based on blockchain technology and generally here we deal with the peer to peer network where there are no client talk to a central server.



So there is no central counterparty but to many other nodes or clients and this peer to peer kind of network comes with a distributed database. Data is shared across all the nodes. So data is shared across all such nodes. The data forms a chain where each block points to its predecessor in some point in time. So there is a chain of blocks getting added.

Placing individual entities in the chain would be inefficient which is why multiple entries are bashed into blocks. This means that each block contains several data entries and thus the name of the technology blockchain and to establish the trust between all nodes or in other words make sure that no one simply changes the chain and sends a fake signal to the nodes. Block contains cryptographic reference. So there is a cryptographic reference which is called hash function. This reference often takes into account the content of the current and previous block so that correctedness of a block and the whole chain can be verified.

One calls it a smart contract. So each block is anchored to the previous block and this anchoring mechanism is done through cryptographic reference. The process of appending a new block to the chain is called mining. So through mining new blocks are added to the chain and it requires proof of work kind of mining algorithm. So one of the algorithm is proof of work. The chain itself is designed to be immutable. So one can it's only append only you cannot change it and entries can be changed and can't be deleted and there is always a new entry added like an event log that state what happened previously and this is publicly available through the use of public keys it can be verified by all the nodes or participants or members.

No one can easily take control of a blockchain and change everything to their advantage. Small scale manipulations can be spotted and negated by the network itself through this consensus mechanism that is in place across nodes. Users do not have to trust a central entity to manage something for them, the network itself is designed in a way to do that. The general idea of a blockchain here is to provide a publicly available decentralized database where everybody can participate in the work with the network and trust is established by the implementation itself because manipulation is difficult or next to impossible. So this kind of infrastructure results in the following key features of the blockchain that we discuss here. First it's decentralized the network is decentralized meaning a group of nodes maintains network and as a decentralized network and this is one of the key features of the blockchain technology.

So the blockchain puts the users in a straightforward position as the system does not require any governing authority they can directly access it from the web and store the assets or transaction details there. Second is immutability as we discussed here immutability something that can't be changed or altered so this is one of the top blockchain feature that ensures that the technology will remain as it is a permanent unaltered labeled network as it is a distributed system every node on the system has a

copy of the digital ledger so when a transaction is added every node needs to check its validity if the majority thinks through this consensus protocol if the majority thinks it is valid it is added to the ledger the new transaction detail is added this promotes transparency and makes it corruption proof without the majority consensus from the nodes no one can add any transaction block to the ledger and once the transaction block is added to the ledger here it is append only its immutable so no one can change it thus any user on the network won't be able to edit it or delete it or update it.

Next enhanced security so as it gets rid of the need of central authority no one can just simply change any characteristics of the network for their benefit so there is using encryption mechanism or cryptography ensures another layer of security for the system and every information of the blockchain is hash cryptography so every information is hash cryptography in the box so changing or trying to tampering with the data means changing all those hash so each block will have some hash cryptographic security mechanism and to change one block you need to change all those hashes that are there so if someone wants to corrupt the network they have to alter every data stored on the every node and that could be millions and millions of such information points where everyone has the same copy of the ledger so it is next to impossible to modify majority of the information points. Next you have distributed or ledger kind of phenomena this distributed ledger phenomena is like a public ledger which will provide every information about a transaction and the participant nodes many people can see what really goes on in the ledger the ledger on the network is maintained by all the users on the system and this distributed ledger responds really well to any suspicious activity or tampering and the nodes or members act as verifiers of this ledger so if a user want to add a new block or a transaction others would have to verify the transaction and give the green signal to make the blockchain features work every active node has to maintain the ledger and participate in this validation process.

Lastly the consensus mechanism so every blockchain succeeds because of this consensus algorithm or consensus mechanism every blockchain has a consensus to help the network make any transaction in simple terms the consensus is like a decision making process for the group of nodes that are active on the network these nodes can come to an agreement quickly and relatively in a faster manner so when millions of nodes are validating a transaction a consensus is very much necessary for a system to run smoothly nodes might not trust each other but they can trust the algorithm that run at the core of it.

To summarize in this video, we discussed the key characteristics of the blockchain these included the ledger technology the security sharing of the ledger across multiple participants and distributed property of blockchain where number of nodes the information is distributed across number of nodes or members in a blockchain. Next we discussed the key features these included immutability of the information that information cannot be or transaction related information cannot be altered

decentralization that it does not require any central counterparty enhanced security so security is enhanced through cryptographic measures and distributed ledger that means there are multiple nodes who carry a copy of ledger so it is very difficult to alter the original information and the consensus mechanism to safeguard and ensure immutability and unalterable property of this blockchain.

In this video we will discuss the categorization of blockchain into permissionless versus permissioned blockchains. To begin with blockchain networks can be categorized based on their permission model which determines who can maintain them or publish blocks if anyone can publish a new block then it is a permissionless blockchain if only particular users can publish blocks then it is a permissioned blockchain. So in simple terms a permissioned blockchain network is like a corporate intranet that is controlled while a permissionless blockchain is like a public intranet where anyone can participate.

So these permissioned blockchain networks are often deployed for a group of organizations and individuals typically referred to as consortium. In contrast cryptocurrencies such as bitcoin employ the permissionless model of the blockchain. Let us start our discussion with permissionless blockchains. Permissionless blockchain networks are decentralized ledger platforms open to anyone publishing blocks without needing permission from any central authority. So these permissionless blockchain platforms are often open source software freely available to anyone who wishes to download them. Since anyone has the right to publish blocks this results in the property that anyone can read the blockchain as well as issue transactions on the blockchain including those transactions within published blocks.

So any blockchain network user within a permissionless blockchain network can read and write to the ledger that is why it is a distributed or decentralized ledger and therefore true to its name this kind of permissionless blockchain allows anyone to take part in the network and access information. In short it is decentralized and open to public and that's why it's called permissionless because there are no gatekeepers and no censorship. Anyone who wants to access the blockchain does not need to pass through your conventional know your customer norms that are required to provide identification documents by banks in a conventional sense and now because it is accessible to the public the typical trade-off of permissionless blockchains is speed. They tend to be relatively slower than permission counterparts which only has a few numbers. Now typically these permissionless blockchains are open to anyone and transaction information stored on these blockchains is validated by the public because there is no regulatory body or central authority the network relies on the public or the nodes on the blockchain to reach a consensus concerning the validity of transactions and precisely because these permissionless blockchains networks are open to all to participate malicious users may attempt to publish blocks in a way that subverts or destroys the system.

So to prevent this permissionless blockchain networks often utilize a multi-party agreement or consensus system that requires users to expend or maintain resources when attempting to publish blocks. This prevents malicious users from easily subverting the system and examples of such consensus models include proof of work and proof of stake methods. The consensus systems in permissionless blockchain network usually promote non-malicious behavior through rewarding the publishers of protocol confirming blocks with a native currency maybe for example for Bitcoin blockchain the native currency is Bitcoin itself. The consensus mechanisms typically used in these types of networks are like proof of work and proof of stake and generally honesty is incentivized with these mechanisms in place and keeps the system working as expected.

Some examples of permissionless networks are like Bitcoin and Ethereum. Now coming to the permissioned blockchains. In permissioned blockchains these are closed or have access control layer. This additional layer of security only allows participants to perform the actions that are authorized to perform. In a permissioned blockchain a user would need permission from the network owner to become part of the SAD network. Typically, a user can only access read and write information on the blockchain if they are given access to it.

A private permissioned blockchain defines the role that dictate how each participant can contribute to the blockchain and what they can access. Also here only authorized users can publish blocks and therefore permissioned blockchain networks are ones where users publishing blocks must be authorized by some authority. It can be a centralized authority. Since only authorized users are maintaining the blockchain it is possible to restrict read access and to restrict who can issue transactions. Permissioned blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to only authorized individuals.

They also may allow someone to submit transactions to be included in the blockchain or again they may restrict this access only to authorized individuals. Such permissioned blockchain networks may be instantiated and maintained using open source or closed source software as well. Moreover, these permissioned blockchains offer the same level of traceability of digital assets as they pass through the blockchain as well as the same distributed resilient and redundant data storage system as a permissionless blockchain network. They also use consensus models for publishing blocks but these methods often do not require the expense or maintenance of resources as is the case with the permissionless blockchain networks. This is because the establishment of one s identity is required to participate as a member of the permissioned blockchain network and those maintaining the blockchain have a level of trust, certain level of trust with each other since they are all authorized to publish blocks and since their authorization can be revoked if they misbehave.

Here consensus models in permissioned blockchain networks are usually faster and computationally less expensive. Also these permissioned blockchains can be employed by organizations that need to be more tightly controlled and protect their blockchain. However if a single entity controls who can publish blocks, the users of the blockchain will need to have a certain trust in that entity and permissioned blockchain networks may also be used by organizations that wish to work together but may not fulfill or fully trust each other. So they can establish a permissioned blockchain network and invite business partners to record their transactions on a shared distributed ledger. These organizations can determine the consensus model to be used based on how much they trust each other.

Beyond trust permissioned blockchain networks provide transparency and insight that may help better inform business decisions and hold misbehaving parties accountable. This can explicitly include auditing and oversight entries making audits a constant occurrence versus a periodic event. Moreover some permissioned blockchain networks support the ability to selectively reveal transaction information based on a blockchain network user's identity or credentials. With this feature some degree of privacy in transactions may be obtained. For example it could be that the blockchain records that a transaction between two blockchain networks users took place but the actual contents of transaction is only accessible to the involved parties.

Lastly some permissioned blockchain networks require all users to be authorized to send and receive transactions. They are not anonymous or even pseudo anonymous. In such systems parties work together to achieve a shared business process with natural disincentives to commit fraud or otherwise behave as a bad actor since they can be identified easily. If bad behavior were to occur it is well known where the organizations are incorporated, what legal remedies are available and how to pursue those remedies in relevant judicial systems. A good permissioned blockchain example would be ripple which is a large cryptocurrency that supports permission-based rules for network participants. A lot of businesses prefer permissioned blockchain networks because they allow network administrators to configure settings and place restrictions as needed.

So now to summarize this video for blockchain networks that allow anyone to anonymously create accounts and participate they are called permissionless blockchain networks and these capabilities deliver a level of trust amongst parties with no prior knowledge of one another.

This trust can enable individuals and organizations to transact directly which may result in transactions being delivered faster and at lower cost. For a blockchain network that more tightly controls access these are called permissioned blockchain networks where some trust may be present among users and these capabilities help to bolster that test.

In this video we will compare permissionless and permissioned blockchains with the help of cryptocurrency example. To begin with the technological challenge in digital peer-to-peer exchanges so called the double spending problem. Any digital form of money is easily replicable and can thus be fraudulently spent more than once. Digital information can be reproduced more easily than physical banknotes. For digital money solving the double spending problem requires at a minimum that someone keeps a record of all transactions. Prior to cryptocurrencies the only solution was to have a centralized agent do this and verify all the transactions. Cryptocurrencies overcame this double spending problem via a decentralized record keeping through what is known as distributed ledger. The ledger can be recorded or considered as a file like a Microsoft Excel worksheet that starts with an initial distribution of cryptocurrency and records the history of all subsequent transactions. Next an up-to-date copy of the entire ledger is stored with each user which is what it makes it distributed and with the distributed ledger what we call as peer-to-peer exchange of digital money is feasible where each user can verify in their copy of ledger whether a transfer took place and that there was no attempt to double spend.

While all cryptocurrencies rely on a distributed ledger they differ in terms of how the ledger is updated one can distinguish predominantly with two classes with substantial differences in their operational setup as we will discuss now. First one class is based on permission DNT or distributed ledger technology. Such cryptocurrencies are very similar to conventional payment mechanisms in that to prevent any misuse or abuse the ledger can only be updated by the trusted participants in the cryptocurrency often termed as trusted nodes and these nodes are chosen by and they are subject to oversight by a central authority. For example the firm that developed the cryptocurrency and thus while cryptocurrencies based on permission system differ from conventional money in terms of how transaction records are stored decentralized versus centralized they share with it the reliance on specific institutions as the ultimate source of trust. Next in a much more radical departure from the prevailing institutional based setup a second class of cryptocurrency has emerged which promises to generate trust in a fully decentralized setting using permissionless DLT or distributed ledger technology.

The ledger recording transactions can only be changed by a consensus of participants in the currency while anybody can participate nobody has a specialty to change the ledger. The concept of permissionless cryptocurrencies thus was laid out for the case of bitcoin in a white paper by an anonymous programmer or group of programmers under the pseudonym Satoshi Nakamoto who proposed the currency based on a specific type of distributed ledger blockchain. This blockchain is a distributed ledger that is updated in groups of transactions called blocks and blocks are then chained sequentially as we have already discussed by the use of cryptography to form the blockchain and this concept has been adopted countlessly with other cryptocurrencies also. And working in this way

blockchain based permissionless cryptocurrencies have two key group of participants called miners. These miners who act as sort of bookkeepers or verifiers of the transactions and users of the blockchain who want to transact in this particular native cryptocurrency and therefore at face value the idea underlying these cryptocurrencies is simple instead of bank as a central authority recording transactions the ledger is updated by a set of miner who are the nodes here working to verify the transaction and update is subsequently stored by all the users and miners.

So, the update is recorded with all the users and miners who through consensus mechanism verify this transaction. So, let us understand this process through this diagram. So, in a conventional centralized kind of ledger you have one copy one central main copy with which all the parties reconcile their local database and the central party like a bank or a central bank it contains the main ledger and it is a central trusted third party. So, there is no such need for verification the central party is the owner of that ledger which for all the other members or those who are doing the transaction they have to reconcile their records with the central party. So, there is only one copy while in terms of this new blockchain distributed ledger technology you have two ways there are multiple copies of this ledger and for example first we have permissioned version of distributed ledger where a selected set of nodes can participate and these selected set of nodes are who have been given some kind of special access or permission by a central body. So, these nodes need some kind of permission from a central entity to access the network and once they are part of this network based on permission then they can make changes to the ledger and these access controls given to these nodes by the central body may include some kind of identity verification.

In another way the second which is more sort of now become the more norm rather than the exception is the permissionless blockchain. So, here the distributed ledger has permissionless access anybody can access and participate. So, here anybody can access there is no lock or identity verification needed. Each node in this peer-to-peer kind of network stores full and up to date copy of the entire ledger and every proposed local addition to the ledger by a network participant it is communicated across the network to nodes. In principle these nodes collectively attempt to validate so they collectively attempt through some kind of algorithmic consensus mechanism they collectively verify and validate the transaction if the transaction information is accepted it is added as a new block to the blockchain this if it is accepted it is added to the new block to the blockchain in the ledger and he showed in data consistency across the entire network.

So, this in transaction once verified and validated is communicated to the entire network and added as a new block to the blockchain. Next let us come to this tabular comparison between permission and permissionless chains. So, first point is storage of balances, holdings, maintenance of records. In both cases there is a decentralized DLT ledger

technology through which storage and transaction record maintenance is taking place. Second is verification to avoid double spending problem.

Now in both cases there is a peer-to-peer concept where distributed ledger is checked to see whether a specific unit of currency has been spent. However, in permissioned blockchain this verification is done by only those nodes which have authorized access while in permissionless there are all public nodes all everybody can do that. Now in terms of processing of transactions the ledger is updated through verification by a set of trusted nodes only which have access to the blockchain while in permissionless the updating of ledger is done through some kind. The proof of work kind of rule to follow the longest chain where maximum majority consensus has emerged. More than 51% of nodes have provided their consensus to verify the transaction and then it is communicated across the network.

In terms of supply, elasticity of supply or the volume that protocol there is a set of protocols and that can be changed or established by trusted nodes. So, the elasticity of supply of currency or the transaction happens through a set of protocol driven by a trusted node while permissionless is totally protocol determined no control, nobody can change that it is very specific protocol determined. Trust creating mechanism is based on the reputation of those the issuing firm and the trusted nodes who have this authorized access and these nodes are also subject to regulation by the issuing firm. While in case of permissionless chain it requires some kind of proof of work and consensus mechanism. So, these permissionless blockchains they incentivize honest verification and computing by a majority of the nodes.

To summarize in this video we discussed how permissioned and permissionless blockchains are segregated across the kind of participants. For example, we said that permission blockchains have nodes that have some kind of special access or permission by a central authority and these only these selected nodes who have the access they run verify and maintain operations in blockchain validate the transaction and so on. While in the permissionless blockchain there is a sort of peer-to-peer public network where anybody can be part of the network and it runs based on a set protocol according to which through some kind of consensus mechanism like proof of work all the nodes verify a transaction and communicated to the network once a transaction is verified communicated its information is added to the blockchain and this blockchain works. Both of these employ some kind of distributed ledger technology.

To summarize in this lesson, we noted that centralized ledgers are one way for keeping records where some central authority remains the owner such as central bank. In contrast, in the decentralized or distributed ledgers there is no such central authority and all the participants have access to the record of transactions. While centralized ledgers are efficient in controlling regulation and speed as compared to decentralized ledgers there is

a threat of single point failure due to malicious attacks. We noted that blockchain offers a unique way to maintain records in a secure tamper evident and tamper resistant manner. It is a sequence of blocks containing transaction records and each block is linked to each other in a cryptographic manner. Historical evolution of blockchain suggests three key components of blockchain including hash functions, Merkle tree and digital signatures.

These characteristics of blockchain include ledger that is decentralized, immutable, secured and distributed and works with some kind of consensus mechanism. Two types of blockchains are often employed including permission and permissionless blockchains. In the permissioned blockchain the members or nodes are authorized through some central authority and given access to record and modify transactions. In permissionless blockchains there is no such authority and members are incentivized in native currency for validating a transaction on the network in an honest manner through cryptographic principles.

Thank you.