Subject:
(410243)
Blockchain Technology
(BT)

Dr. S. R. Khonde

Unit II

Feature Engineering

Dr. S. R. Khonde

Content

- History, Centralized Vs. Decentralized Systems, Layers of Blockchain: Application Layer, Execution Layer, Semantic Layer, Propagation Layer, Consensus Layer, Why is Block chain important? Limitations of Centralized Systems, Blockchain Adoption So Far.

Case Study

- Study of a research paper based on Blockchain.

Course Outcome Mapped

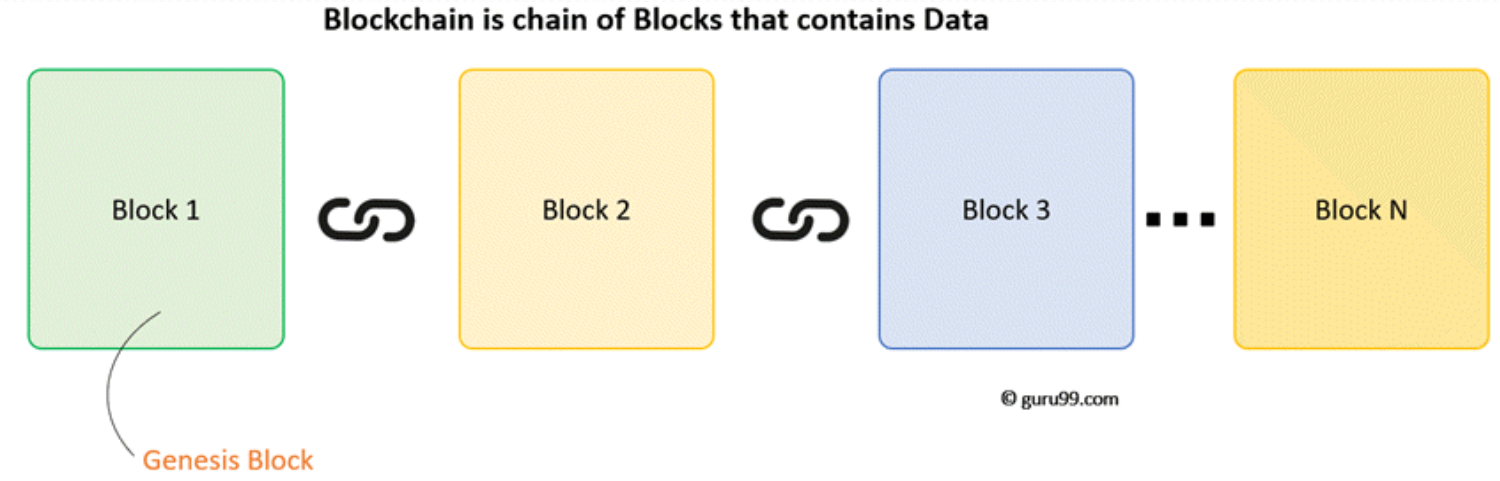
- CO1

Introduction to Blockchain

- Blockchain a buzz word used today is reshaping several sectors which was introduced to the world with Bitcoin. Bitcoin is nothing than a type of virtual money known as a crypto currency that can be exchanged.
- Blockchain is a backbone technology contributed in the development of crypto currencies.
- Bitcoin and blockchain are not similar. One of the uses for blockchain is creation of crypto currency such as Bitcoin.
- Now a days blockchain is used for many applications and has many uses that are currently being explored.

Introduction to Blockchain

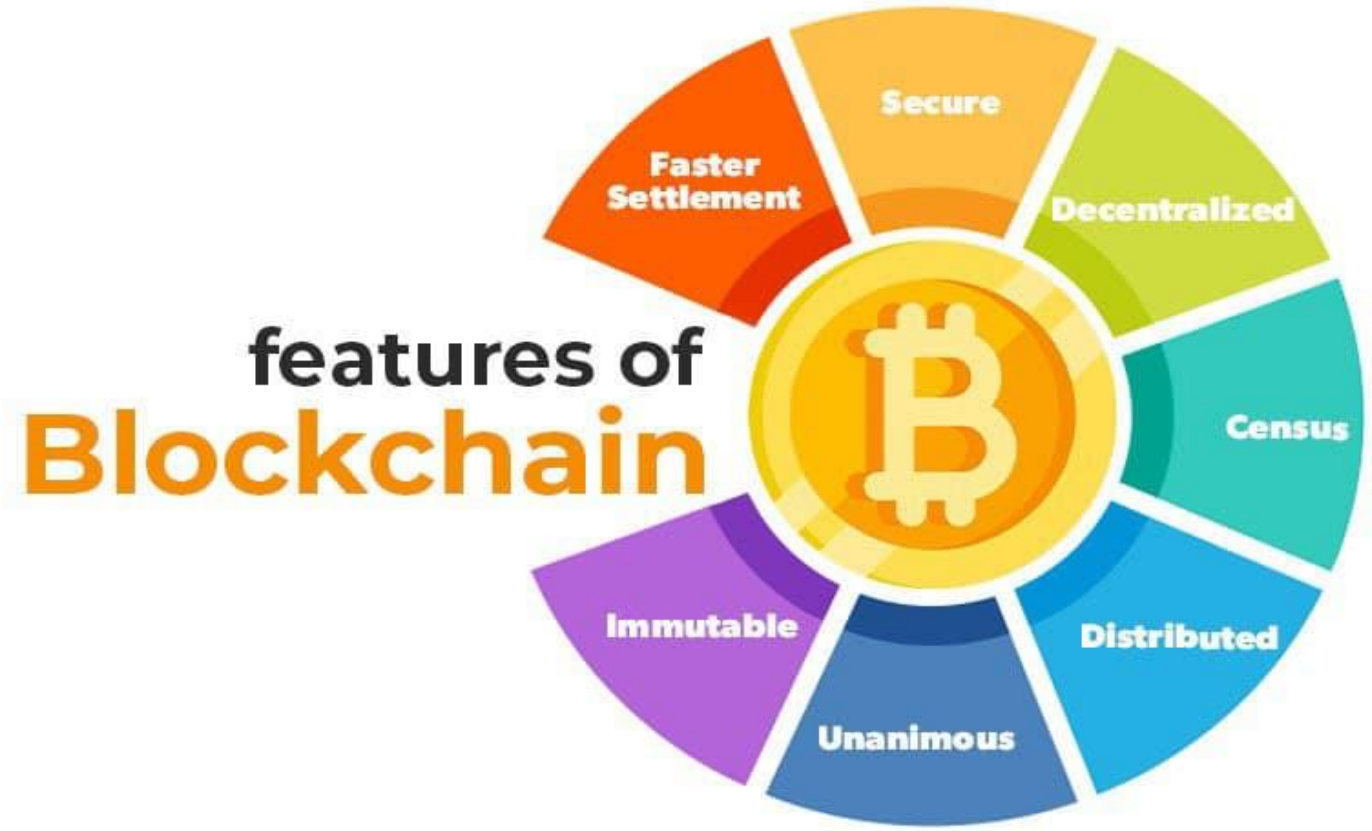
- Blockchain can be defined as a data structure that stores transactional records and ensures security, transparency, and decentralisation.
- It is a chain of records that are held in the form of blocks and are managed by many authorities.



Introduction to Blockchain

- Blockchain which is also known as distributed ledger is totally accessible to everyone on the network.
- Once the data is added in block of blockchain it is difficult to edit or modify it.
- Every transaction in blockchain is protected by a digital signature that ensures data legitimacy.
- Each transaction or data stored in blockchain is tamper-proof (cannot be tampered) and cannot be altered due to encryption and digital signatures.
- Blockchain follows an agreement to be followed by each participant known as Consensus.
- Every piece of information kept on blockchain is digitally recorded and has a shared history that is accessible to all for avoiding fraud and duplicate transaction.

Features of Blockchain



Features of Blockchain

Immutable

- Immutability means that the blockchain is a permanent and unalterable network. Blockchain technology functions through a collection of nodes.
- Every node in the network has a copy of the digital ledger. To add a transaction every node checks the validity of the transaction and if the majority of the nodes think that it is a valid transaction then it is added to the network. This means that without the approval of a majority of nodes no one can add any transaction blocks to the ledger.
- Any validated records are irreversible and cannot be changed. This means that any user on the network won't be able to edit, change or delete it.

Features of Blockchain

Distributed

- All network participants have a copy of the ledger for complete transparency. A public ledger will provide complete information about all the participants on the network and transactions.
- In distributed ledger tracking what's happening in the ledger is easy as changes propagate really fast in a distributed ledger.
- Every node on the blockchain network must maintain the ledger and participate in the validation.
- Any change in the ledger will be updated in seconds or minutes and due to no involvement of intermediaries in the blockchain, the validation for the change will be done quickly.
- If a user wants to add a new block then other participating nodes have to verify the transaction. For a new block to be added to the blockchain network it must be approved by a majority of the nodes on the network.

Features of Blockchain

Decentralized

- The blockchain network is decentralized which means that there is no central governing authority that will responsible for all the decisions.
- A group of nodes makes and maintain the blockchain network.
- Each and every node in the blockchain network has the same copy of the ledger.
- The decentralized nature of blockchain facilitates creating a transparent profile for every participant on the network. Thus, every change is traceable, and more concrete.
- Users now have control over their properties and they don’t have to rely on third-party to maintain and manage their assets

Features of Blockchain

Secure

- All the records in the blockchain are individually encrypted.
- Using encryption adds another layer of security to the entire process on the blockchain network.
- Since there is no central authority, it does not mean that one can simply add, update or delete data on the network.
- Every information on the blockchain is hashed cryptographically which means that every piece of data has a unique identity on the network.
- All the blocks contain a unique hash of their own and the hash of the previous block. Due to this property, the blocks are cryptographically linked with each other.
- Any attempt to modify the data means to change all the hash IDs which is quite impossible.

Features of Blockchain

Consensus

- Every blockchain has a consensus to help the network to make quick and unbiased decisions.
- Consensus is a decision-making algorithm for the group of nodes active on the network to reach an agreement quickly and faster and for the smooth functioning of the system.
- Nodes might not trust each other but they can trust the algorithm that runs at the core of the network to make decisions.
- There are many consensus algorithms available each with its pros and cons such as PoW, PoA, PoS, ...
- Every blockchain must have a consensus algorithm otherwise it will lose its value.

Features of Blockchain

Unanimous (agreed or supported by everyone)

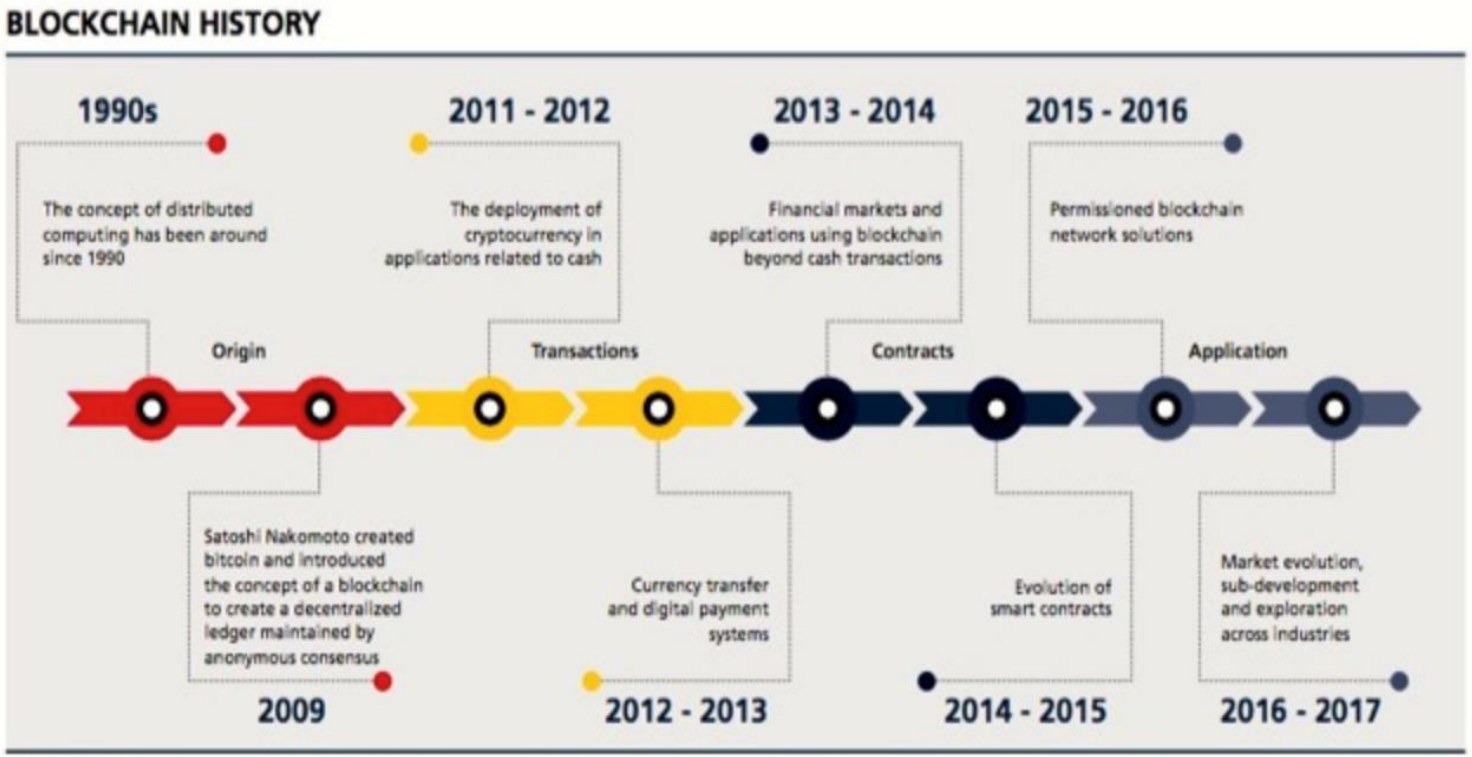
- All the network participants agree to the validity of the records before they can be added to the network.
- When a node wants to add a block to the network then it must get majority voting otherwise the block cannot be added to the network.
- A node cannot simply add, update, or delete information from the network.
- Every record is updated simultaneously and the updations propagate quickly in the network. So it is not possible to make any change without consent from the majority of nodes in the network.

Features of Blockchain

Faster Settlement

- Traditional banking systems are prone to many reasons for fallout like taking days to process a transaction after finalizing all settlements, which can be corrupted easily. On the other hand, blockchain offers a faster settlement compared to traditional banking systems. This blockchain feature helps make life easier.
- Blockchain technology is increasing and improving day by day and has a really bright future in the upcoming years. The transparency, trust, and temper proof characteristics have led to many applications of it like Bitcoin, Ethereum, etc. It is a pillar in making the business and governmental procedures more secure, efficient, and effective.

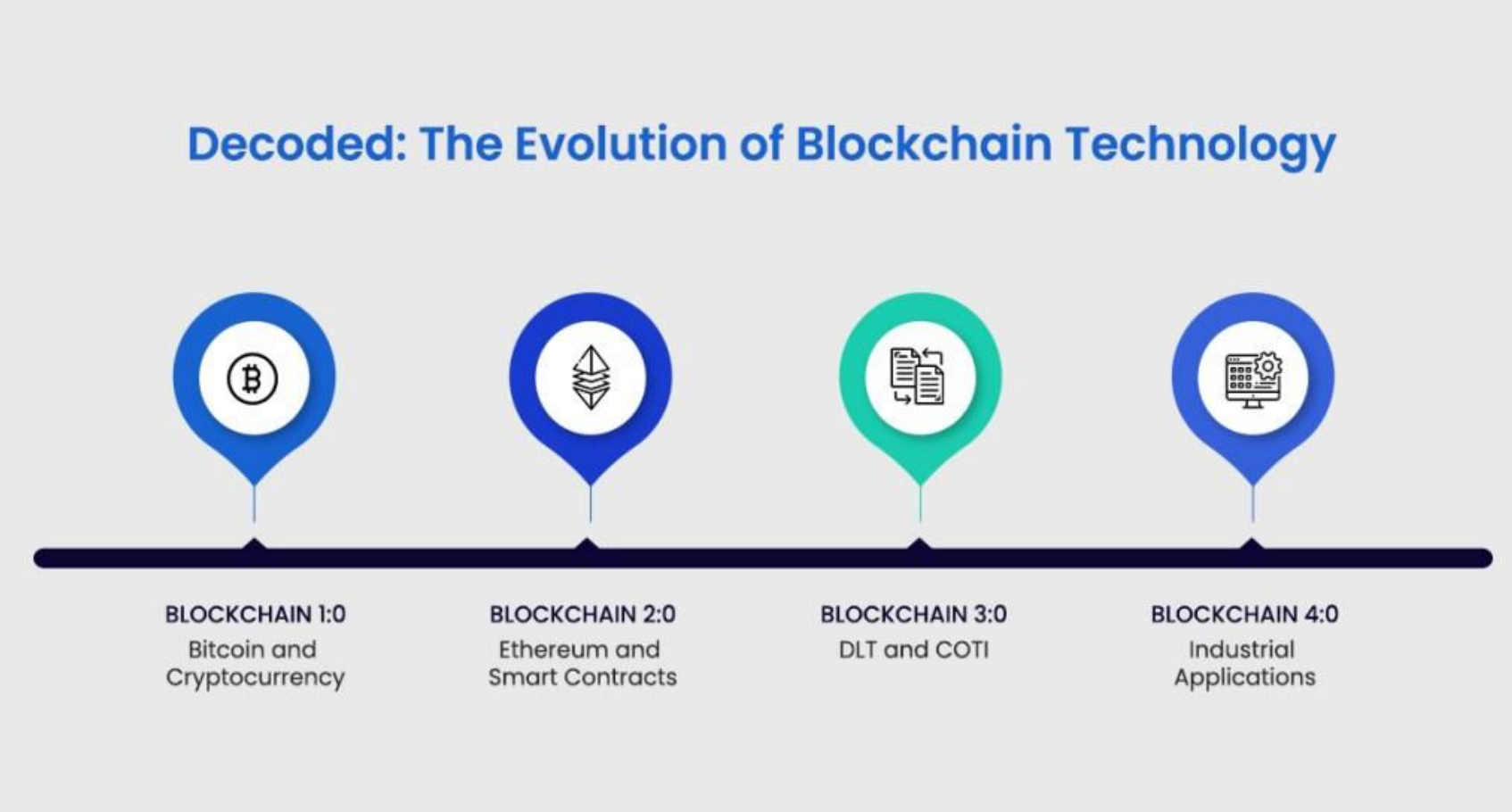
History of Blockchain



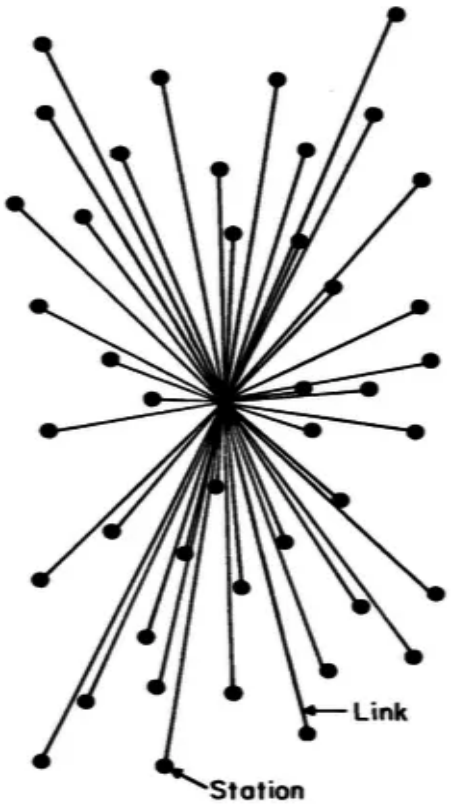
A history of blockchain technology; **Source:** Accenture

Dr. S. R. Khonde

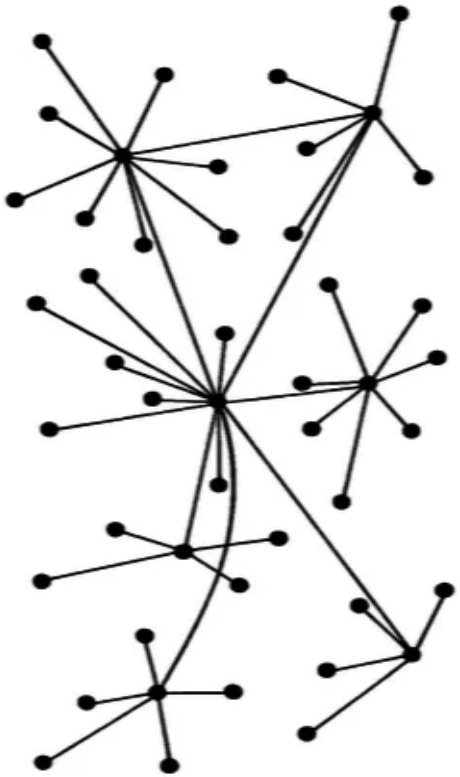
History of Blockchain



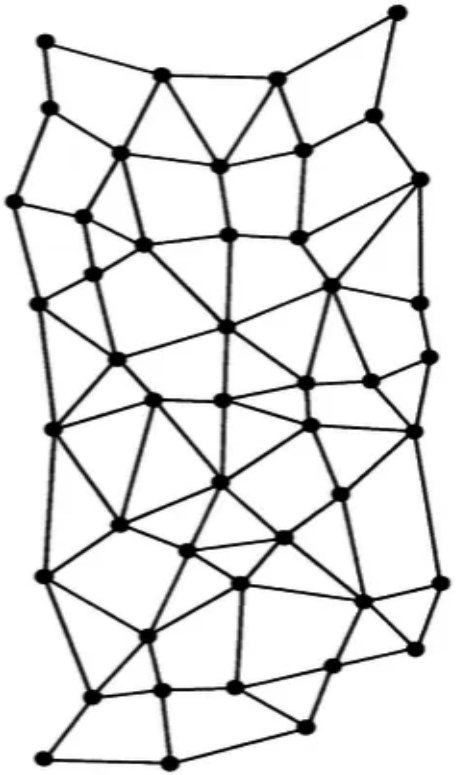
Systems



CENTRALIZED
(A)



DECENTRALIZED
(B)



DISTRIBUTED
(C)

Centralised Systems

- In a centralized system, all users are connected to a central network owner or “server”.
- The central owner stores data, which other users can access, and also user information. This user information may include user profiles, user-generated content, and more.
- A centralized system is easy to set up and can be developed quickly.

Limitations

- If the server crashes, the system no longer works properly and users cannot access the data.
- Because a centralized system needs a central owner to connect all the other users and devices, the availability of the network depends on this owner.
- Security concerns that arise when one owner stores (and can access) user data.

Centralised Systems

Pros

- Simple deployment
- Can be developed quickly
- Affordable to maintain
- Practical when data needs to be controlled centrally

Cons

- Prone to failures
- Higher security and privacy risks for users
- Longer access times to data for users who are far from the server

Decentralised Systems

- As its name implies, decentralized systems don’t have one central owner. Instead, they use multiple central owners, each of which usually stores a copy of the resources users can access.
- A decentralized system can be just as vulnerable to crashes as a centralized one. However, it is by design more tolerant to faults. That’s because when one or more central owners or servers fail, the others can continue to provide data access to users.
- Resources remain active if at least one of the central servers continue to operate.
- Server crashes in a decentralized system may affect the performance and limit access to some data.
- Access time to the data is often faster

Decentralised Systems

Pros

- Less likely to fail than a centralized system
- Better performance
- Allows for a more diverse and more flexible system

Cons

- Security and privacy risks to users
- Higher maintenance costs
- Inconsistent performance when not properly optimized

Distributed Systems

- A distributed system is similar to a decentralized one in that it doesn’t have a single central owner.
- But going a step further, it eliminates centralization. In a distributed system, users have equal access to data, though user privileges can be enabled when needed.
- The best example of a vast, distributed system is the internet itself.
- The distributed system enables users to share ownership of the data.
- Hardware and software resources are also allocated between users, which in some cases may improve the performance of the system.
- A distributed system is safe from the independent failure of components, which can improve its uptime considerably.

Distributed Systems

Pros

- Fault-tolerant
- Transparent and secure
- Promotes resource sharing
- Extremely scalable

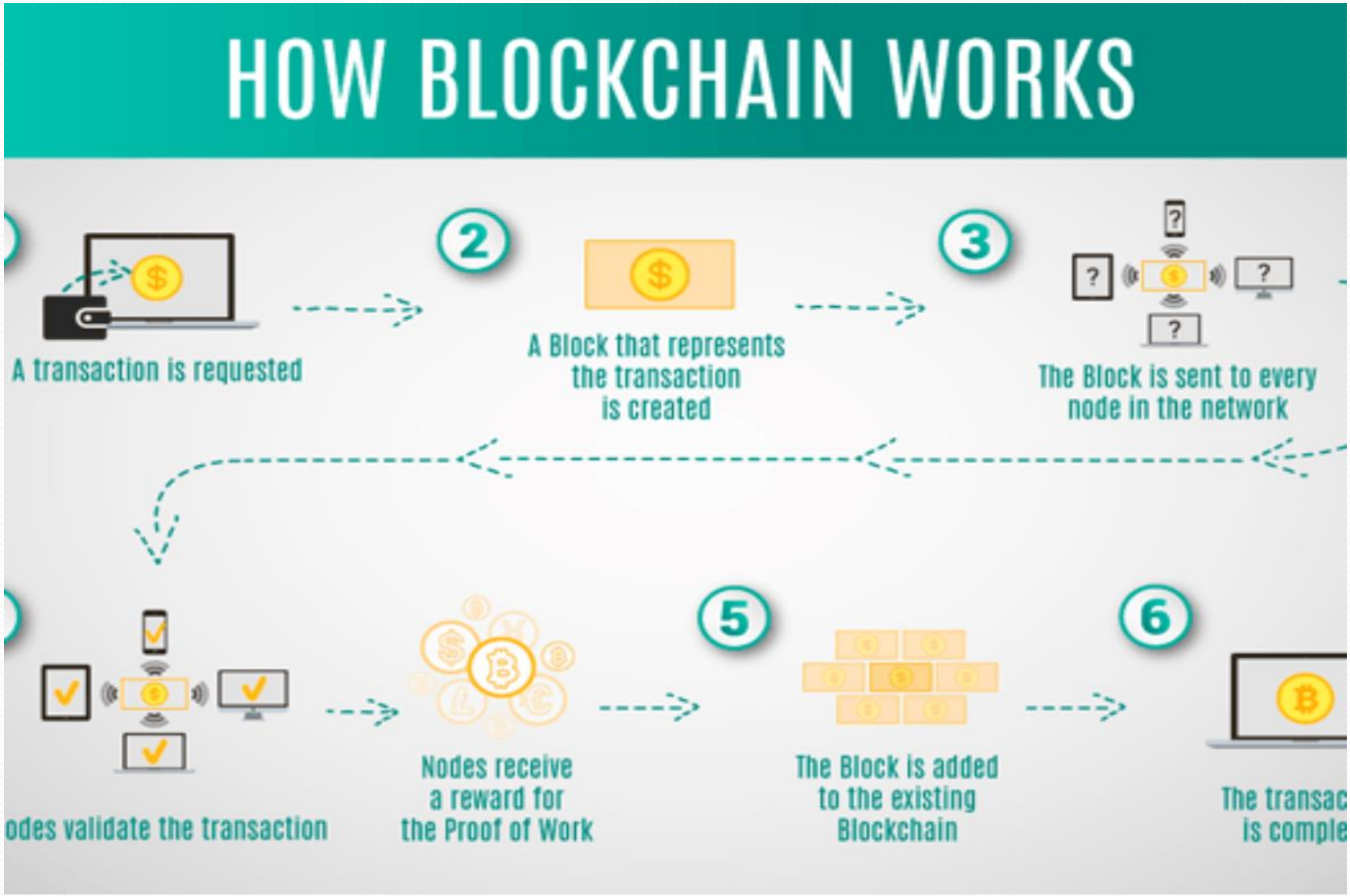
Cons

- More difficult to deploy
- Higher maintenance costs

Blockchain Mechanism

- Blockchain is a type of shared database that differs from a typical database in the way that it stores information; blockchains store data in blocks that are then linked together via cryptography.
- As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.
- Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.
- In Bitcoin's case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.
- Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.

Blockchain Mechanism



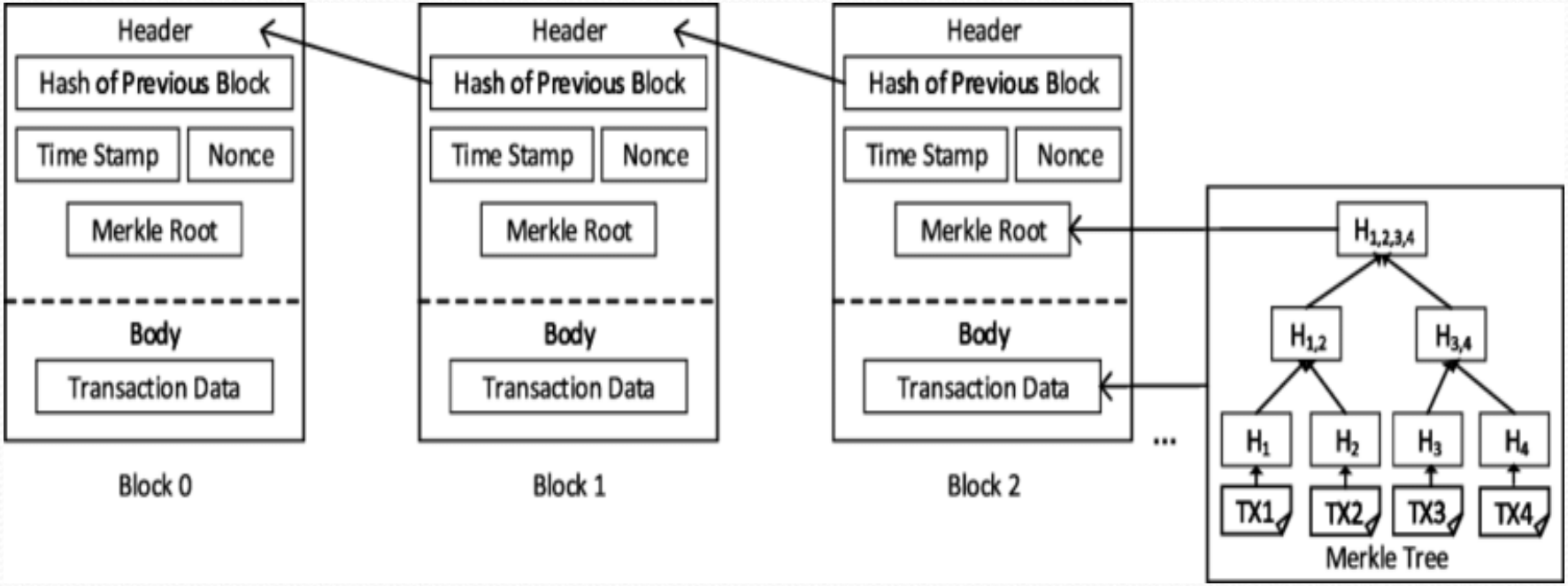
Block Structure

Block in a Blockchain–

- Blockchain is a linear chain of blocks.
- Each block contains a set of transactions and other essential details.
- Blocks are linearly connected and cryptographically secured.
- Each block consists of header and transactions.

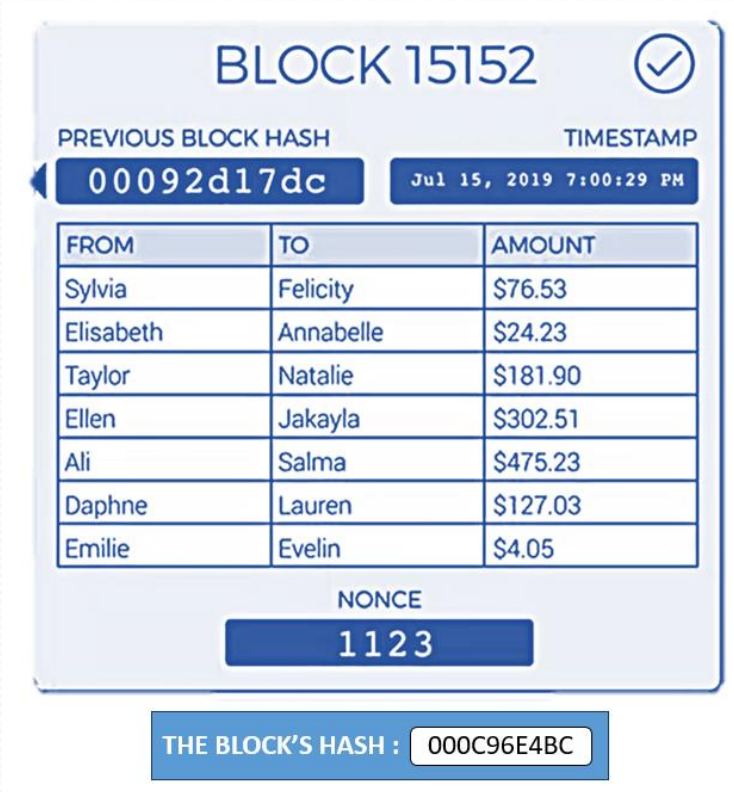
Block Header Structure

Each block header contains the previous block hash, current block hash, nonce, Merkle root, and other details.



Block Header Structure

- All blocks are connected linearly by carrying the hash of the previous block.
- The previous block hash is used to compute the current block hash.
- The first block with no previous block hash is called “Genesis Block.”
- For adding a new block to the network, the blockchain follows consensus mechanisms like proof of work (PoW), proof of stake (PoS), etc.



Dr. S. R. Khonde

Significant Elements Of A Block

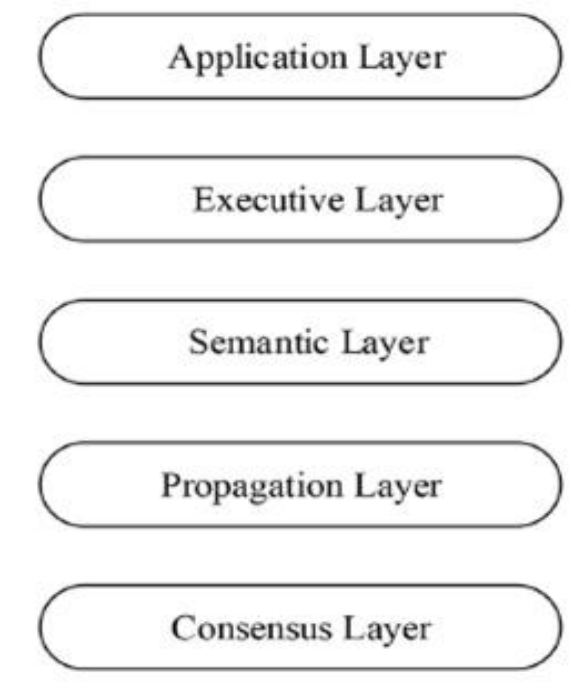
- ***Block Height :*** It's the sequence number of the block in the chain of blocks. Block Height: 1 is the genesis block (first block in the network).
- ***Block Size :*** It's a 4-bytes or 32-bit field that contains the size of the block. It adds size in Bytes. Ex – Block Size: 216 Bytes.
- ***Block Reward :*** This field contains the amount rewarded to the miner for adding a block of transactions.
- ***Tx Count :*** The transaction counter shows the number of transactions contained by the block. The field has a maximum size of 9 bytes.

Block Header

- The Block header is an 80-Byte field that contains the metadata – the data about the block.
- 6 components of the Block Header.
- ***Time:*** It's the digitally recorded moment of time when the block has been mined. It is used to validate the transactions.
- ***Version:*** It's a 4-bytes field representing the version number of the protocol used. Usually, for bitcoin, it's '0x1'.
- ***Previous Block Hash:*** It's a 32-bytes field that contains a 256-bits hash of the previous block. This helps to create a linear chain of blocks.
- ***Bits:*** It's a 4-bytes field that tells the complexity to add the block.
- ***Nonce:*** It's a 4-bytes field that contains a 32-bit number. These are the only changeable element in a block of transactions.
- ***Merkle Root:*** A 32-bytes field containing a 256-bit root hash. It's constructed hierarchically combining hashes of the individual transactions in a block.

Layers of Blockchain

- The blockchain technology is based on a layered approach.
- The blockchain technology is decomposed into several layers that will in turn help in better understanding of security and the design of the blockchain.
- Layers for the blockchain technology are:



Layers of Blockchain

Application Layer

- As we know a blockchain technology is a tamperproof, decentralized, and shared ledger technology, so there can be multiple applications that can build on the basis of these features of the blockchain. Some applications built in application layer can interface with the other layers; therefore, the application layer is on the top of this layer suit.
- The application layer is the one where a user can code the desired functionality and build the application for user of the application. Since the blockchain is a decentralized technology and there is no server involved, the application needs to be installed on each node. Although there are some instances where blockchain is in the backend and the applications need to be hosted on a web server and needs a server-side programming, but it would be good if there were no server involved in the blockchain network as it would defeat the purpose and benefit of blockchain technology.

Layers of Blockchain

Executive Layer

- This layer handles the executions of all the instruction that were performed at the application layer for all the nodes present on the blockchain network. The set of instruction could range from simple ones to multiple instructions. For example, smart contract is also small code that needs to be executed when some funds need to be transferred form one person to another person. Now if one application is present on all the nodes of the blockchain network the code has to be executed independently on all the nodes. In order to avoid the inconsistencies in the output, the execution of code on a set of input should always produce the same output for all the nodes present on the blockchain.

Layers of Blockchain

Semantic Layer

- This layer also called as logical layer of blockchain layer suit. This layer deals in validation of the transactions performed in the blockchain network and also validating the blocks being generated in the network. When a transaction comes up from a node, the set of instruction are executed on the execution layer and gets validated on the semantic layer. Semantic layer is also responsible for the linking of the blocks created in the network. As we already know each block in the blockchain contains the hash of the previous block except the Genesis block. This linking of block needs to be defined on this layer.

Layers of Blockchain

Propagation Layer

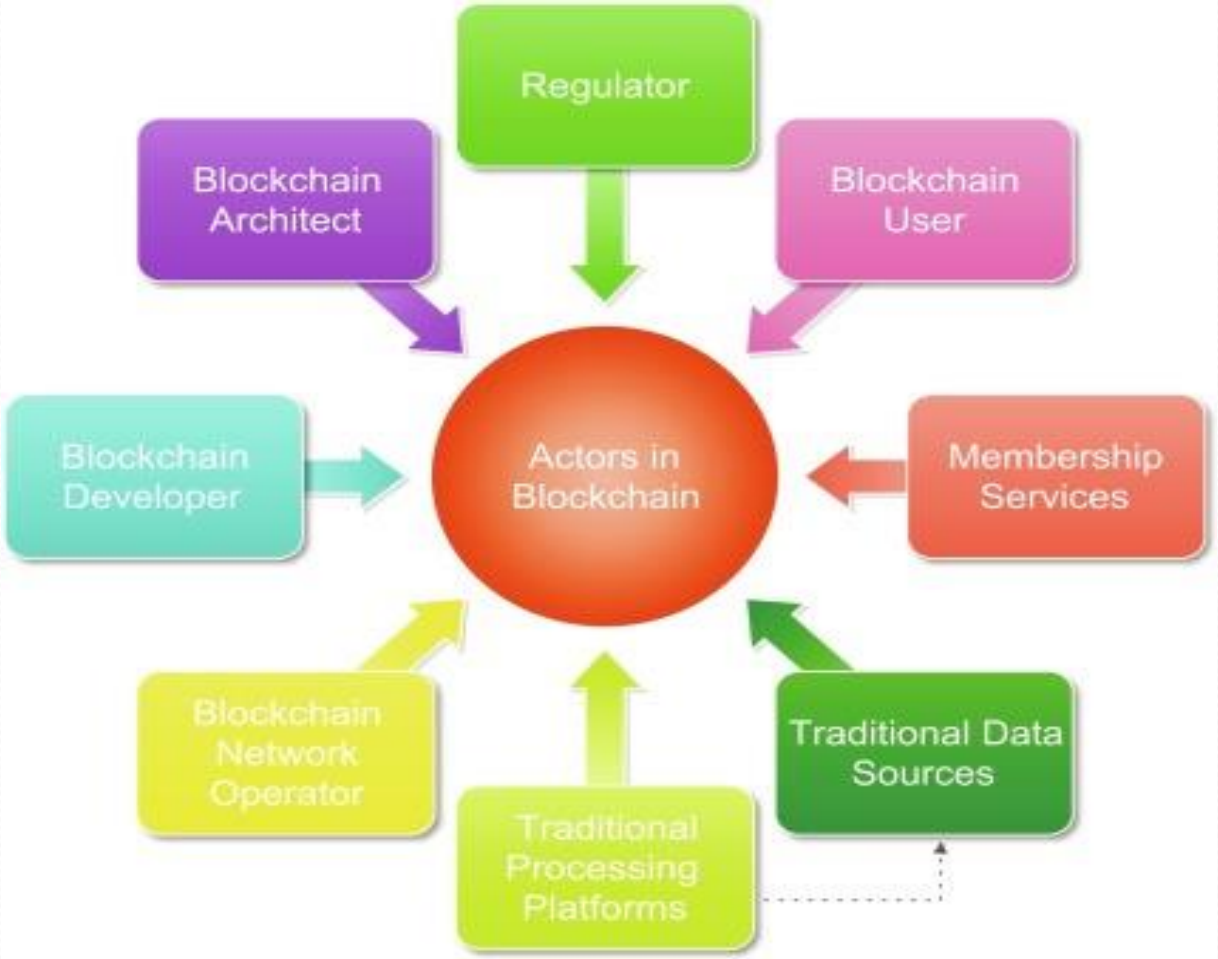
- A propagation layer deals with the peer-to-peer communications between the nodes that allow them to discover each other and get synced with another node in a network. When a transaction is carried out, it gets broadcasted to all other nodes in the network. Also, when a node proposes a block, it will immediately get broadcast in the entire network so that other nodes can use this newly created block and work upon it. Hence, the propagation of the block or a transaction in the network is defined in this layer and ensures the stability of the complete network. However, depending upon the network capacity or network bandwidth sometimes the propagation could occur instantly sometimes it may take a longer.

Layers of Blockchain

Consensus Layer

- This layer is the base layer for most of the blockchain systems. This main purpose of this layer is to make sure that all the nodes must get agree on a common state of the shared ledger. The layer also deals with the safety and security of the blockchain. There are many consensus algorithms which can be applied for generation of cryptocurrencies like Bitcoin and Ethereum, they uses proof-of-work mechanism to select a node randomly out of various nodes present on the network that can propose a new block. Once a new block is created, the block is propagated to all the other nodes to check if the new block is valid or not with the transactions in it and based on the consensus from all other nodes the new block gets added on to the blockchain.

Actors in Blockchain Technology



Actors in Blockchain Technology

Blockchain Architect

Responsible for architecture and design of the blockchain. Blockchain Architect is the one who is going to design, how the blockchain solution is going to be built. He will figure out what is some information that needs to get stored, what are the transactions and the business logic that needs to be embedded onto the network, and so on.

Blockchain Developer

The developer of applications and smart contracts that interact with the blockchain and are used by the blockchain users. The blockchain developer is the one who is going to take what has been an architect and then develop the actual code that will run on the blockchain network itself.

Actors in Blockchain Technology

Blockchain Network Operator

Manages and monitors the blockchain network. Each sub-work or the business in the network has a blockchain network operator. He also runs the blockchain network.

Traditional Processing Platforms

An existing computer system may be used by the blockchain to augment processing. The system may also need to initiate the request to the blockchain. Other systems send or get information that is required to build a blockchain solution.

Actors in Blockchain Technology

Traditional Data Sources

An existing computer system may provide data to influence the behavior of the smart contract. They are also part of the overall solution to store external data.

Membership Services

It manages different types of certificates, which are required to run a permission blockchain. Membership services provide the identity for users to come and transact on the blockchain. For example, if you open an account with the bank, they give you a username and password, a kind of login to access web services, Membership services is going to do more than that not only username and password but also give a digital certificate that will allow you to transact on the network.

Actors in Blockchain Technology

Blockchain User

The business user, operating in a business network. User experiences the application of that blockchain solution. They are not aware of blockchain. Blockchain user is the one who is going to perform the business transactions on the blockchain, So, these users could belong to multiple organizations that are participating in that blockchain.

Blockchain Regulator

The overall authority is a business network. Specifically, regulators are required to read the ledger's content broadly. The Blockchain regulator is an optional one, they might have only, read-only access onto the network where they see the transactions being performed are legitimate or not, following policies or not, etc.

Importance of Blockchain Technology

Due of various features provided by blockchain it becomes one of the important technology in todays modern era

- ***Immutability***
- ***Transparency***
- ***Digital Freedom***
- ***Truly Decentralized Services***
- ***Outstanding Use cases***
- ***Greater Safety***
- ***Inexpensive***
- ***Improved Efficiency***

Limitations of Blockchain Technology

Some of the limitations for blockchain are as follows

- ***Complexity of Blockchain***
- ***Network size***
- ***Lack of speed***
- ***Lack of standardization***
- ***Lack of interoperability***
- ***Unavoidable security flaw***
- ***Lack of privacy***
- ***High energy consumption***
- ***Scalability Issues***
- ***Politics***

Blockchain Adoption So Far

Industries adapting blockchain are as follows

- ***Automotive***
- ***Banking and finance services***
- ***Government***
- ***Healthcare and life sciences***
- ***Insurance***
- ***Media and entertainment***
- ***Retail and consumer goods***
- ***Telecommunications***
- ***Travel and transport***
- ***Supply chain***
- ***Oil and gas***
- ***Manufacturing***

End of Unit II