Unit 2

CHAPTER 2

Feature Engineering

University Prescribed Syllabus

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.

2.1 INTRODUCTION TO BLOCKCHAIN

GQ. Define Blockchain. What are important features of it?

- Blockchain, a ground-breaking technology that is reshaping several sectors, was mysteriously presented to the world with Bitcoin, its first contemporary application. Bitcoin is nothing more than a type of virtual money known as a cryptocurrency that can be exchanged for fiat money.
- Blockchain is the name of the underlying technology that has contributed to the development of cryptocurrencies.
- People frequently believe that Bitcoin and Blockchain are similar, however this is not the case. One of the uses for blockchain technology is the creation of cryptocurrencies, and in addition to Bitcoin, there are many more uses for the technology that are currently being explored.
- A data structure that stores transactional records and ensures security, transparency, and decentralisation is the simplest way to define Blockchain. It may also be viewed as a chain of records that are held in the form of blocks and are managed by many authorities.

- A distributed ledger known as a blockchain is totally accessibl to everyone on the network. Once data is placed on a blockchain, it is very difficult to edit or modify it.
- On a blockchain, every transaction is protected by a digita signature that attests to its legitimacy. The information save on the blockchain is tamper-proof and cannot be altere thanks to the use of encryption and digital signatures.
- Blockchain technology allows all the network participants t reach an agreement, commonly known as consensus. Every piece of information kept on a blockchain is digitally recorded and has a shared history that is accessible to everyone on the network.
- By doing this, any possibility of fraud or transaction repetition is avoided without the use of a third party.
- Consider the scenario where you are trying to find a way to transmit some money to a buddy who lives somewhere in order to better grasp blockchain. A bank or a payment transfer service like PayPal or Paytm are two options you can often employ.
- With this option, third parties are needed to complete the transaction, which results in a cost that is added to your money as a transfer fee.
- Additionally, in situations like these, it is impossible to guarantee the security of your money because it is very likely that a hacker may interrupt the network and take your money. The victim in both situations is the client. Blockchain is useful in this situation.
- In these situations, utilising a blockchain to transfer money instead of a bank makes the procedure considerably simpler and more secure. There is no additional cost since you process the cash directly, doing away with the need for a middleman.
- Moreover, the blockchain database is decentralised and is not limited to any single location meaning that all the information and records kept on the blockchain are public and decentralized.
- Since the information is not stored in a single place, there's no chance of corruption of the information by any hacker.

2.1.1 Features of Blockchain

The following features set the ground-breaking blockchain technology stand out :

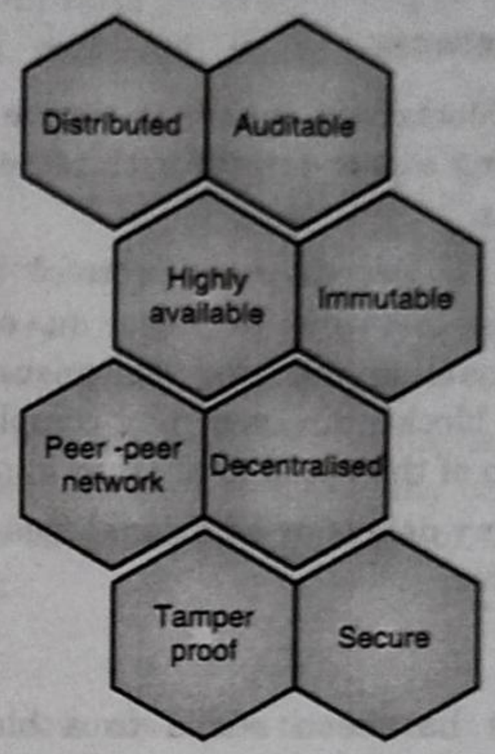


Fig. 2.1.1 : Features of Blockchain

☞ Distributed

- Collaboration is the only recurring concept in the blockchain. There must be several systems in place for collaboration to take place.
- Blockchain is a distributed system by nature since data is processed and stored by various parties. All network participants have access to the distributed ledger and its immutable record of transactions.
- With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

☞ Decentralised

- Blockchains are decentralized in nature meaning that no single person or group holds the authority of the overall network.

- While everybody in the network has the copy of the distribute ledger with them, no one can modify it on his or her own. Th unique feature of blockchain allows transparency and securi while giving power to the users.

☞ **Peer-to-Peer Network**

- The usage of Blockchain makes it simple to engage betwee two parties using a peer-to-peer architecture without the nee for a middleman.
- Blockchain is a peer-to-peer protocol that enables eac member of the network to have an exact copy of eac transaction, enabling machine consensus for approval. Fo instance, with blockchain, you may complete any transactio from one region of the world to another in a matter of seconds.
- Additionally, any delays or additional fees won't be subtracte from the transfer.

☞ **Immutable**

- Any data that has been added to a blockchain cannot b modified after it has been done so, which is known as th immutability feature of a blockchain.
- Consider sending an email as an illustration to better gras immutability. An email that has been sent to a large group o recipients cannot be cancelled.
- You'll have to ask each receiver of your email to erase it, whic is a laborious workaround. This is the operation o immutability.
- Data cannot be modified or altered once it has been processed Because each block in a blockchain retains the hash of the on before it, if you try to modify the data of one block, you'll hav to update the whole blockchain that follows it.
- Any changes to one hash will affect the remaining hashes a well. Since it takes a lot of processing power to modify all th hashes, it is quite difficult for someone to do so.
- As a result of immutability, data kept in a blockchain i immune to changes or hacker assaults.

☞ **Tamper-Proof**

- Because blockchains have the immutability characteristic built in, it is simpler to detect data manipulation.
- Because any alteration to even a single block can be easily discovered and corrected, blockchains are thought to be tamper-proof.
- Hashes and blocks are the two main methods for spotting tampering.
- Each block-related hash function is distinct.
- It may be compared to a block's fingerprint. Any modification to the data will result in a modification to the hash function.
- A hacker would have to modify the hashes of all the blocks following that one in order to make any changes because the hash function of one block is connected to the next, which is a challenging task.

☞ **Auditable**

- Blockchain does not only share the current state but the entire journey or log of how the state has been arrived. The log is available for each node to inquire.
- This makes activities happening on blockchain auditable.

☞ **Highly available**

Distributed and decentralized nature of blockchain network helps ensure consumers that the network always has a node available to serve the requests. This makes blockchain highly available

2.1.2 Origin of Blockchain

GQ. Explore the analogy of Rai stones with distributed ledger. **(4 Marks)**

☞ **Rai/Fei Stones**

- The capacity of blockchain to communicate information between untrusted parties has the potential to uplift everything from finance to politics, making it the most important advancement in knowledge storage and sharing since the creation of the internet.

- But Blockchain has a hidden past that dates back more than thousand years.

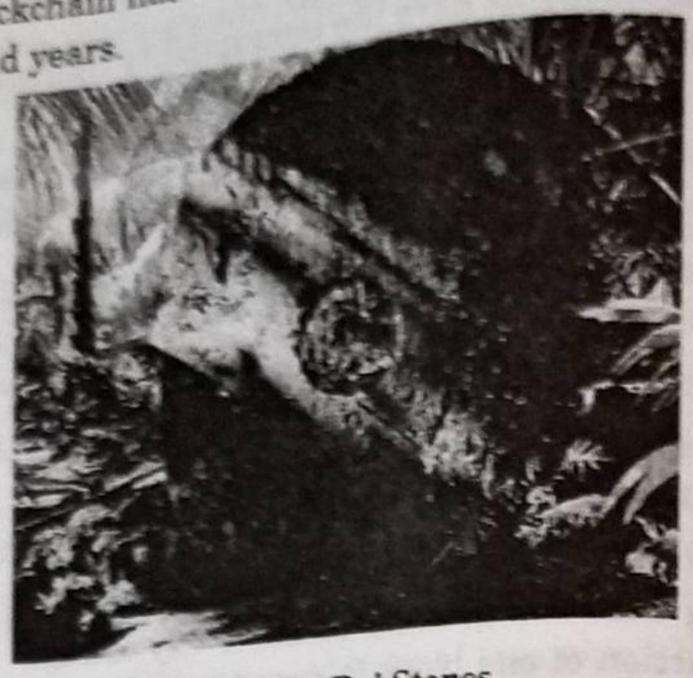


Fig. 2.1.2 : Rai Stones

- Although Bitcoin and the blockchain may appear to be comple new technical ideas, their foundation is actually far older tha you may think.
- As bizarre as it may seem, there is a historical counterpart f bitcoin in a system of ancient money that dates back hundred of years: huge stone discs known as rai, which were formerl employed as a symbolic kind of money on the Micronesia island of Yap.
- The biggest objects ever carried over the open Pacific Ocea before European contact were carved from limestone quarrie in the Palau islands, around 250 miles (400 km) from Yap.
- These enormous, huge stone structures (sometimes taller tha their owners) would not initially appear to have much i common with a digital value system that is encrypted intangible, and basically invisible to human senses.
- However, that physical mismatch conceals the astounding similarity between bitcoin and rai: both currencies rely on a public, community ledger system that offers security an transaction transparency without the need for a centralise banking institution.
- In bitcoin and other cryptocurrencies, that public ledger i called the blockchain: an open record of bitcoin ownership an transactions spread across multiple computers on the internet.

- In rai – and the ancient culture of the Yapese islanders who used the giant stone coins – there was an equally dependable antecedent to the blockchain ledger.
- Although they were very precious, Rai were usually left in one spot once they had been set up because of their size, weight, and relative fragility.
- The new owner(s) of a disc may not have resided nearby if a rai were gifted or traded as a consequence. An oral ledger was kept in communities to guarantee ownership was recognised and unquestionable and to preserve security.
- Every villager kept a mental record of who owned each stone, who they got it from, and when that transaction took place.
- When a Rai/Fei stone was spent, that new transaction was shared across the village people to update everyone's mental map – just like a very ancient, early take on Blockchain.
- If someone came along and tried to wrongly claim a stone was theirs, the village could consult its mental 'decentralized ledger'.
- According to the researchers, this oral ledger – told through stories shared by the Yapese and passed down over generations – helped the community to record and communicate changes in ownership of the rai, for things like wedding gifts, political enticements, or even paying ransoms.
- If this all sounds similar, that's because it's exactly how Bitcoin transactions take place today on the Blockchain, albeit now between computers rather than people.

2.1.3 History of Blockchain Technology

GQ.	Explain The birth of blockchain along with the history of blockchains?	(4 Marks)
GQ.	Explain the evolution of blockchain with timeline.	(4 Marks)
GQ.	Explain The emergence of bitcoin.	(2 Marks)
GQ.	Brief about Ethereum development.	(2 Marks)
GQ.	What are the different phases of blockchain evolution?	(6 Marks)
GQ.	Discuss about major blockchain platforms evolved during phase 3 of blockchain.	(6 Marks)

- Given the impact that blockchain technology is having on variety of industries, including manufacturing, education, an finance, it must rank among the most significant inventions the twenty-first century.
- Many people are unaware that Blockchain has a history tha extends back to the early 1990s.
- Numerous uses have emerged since its popularity began rise a few years ago, all but underscoring the type of influenc it is bound to have as the battle for digital economies heats up
- We'll learn about the development of the blockchain and it history in this conversation.
- For blockchain enthusiasts and aspirants, understanding th history of blockchain is crucial.

Blockchain History

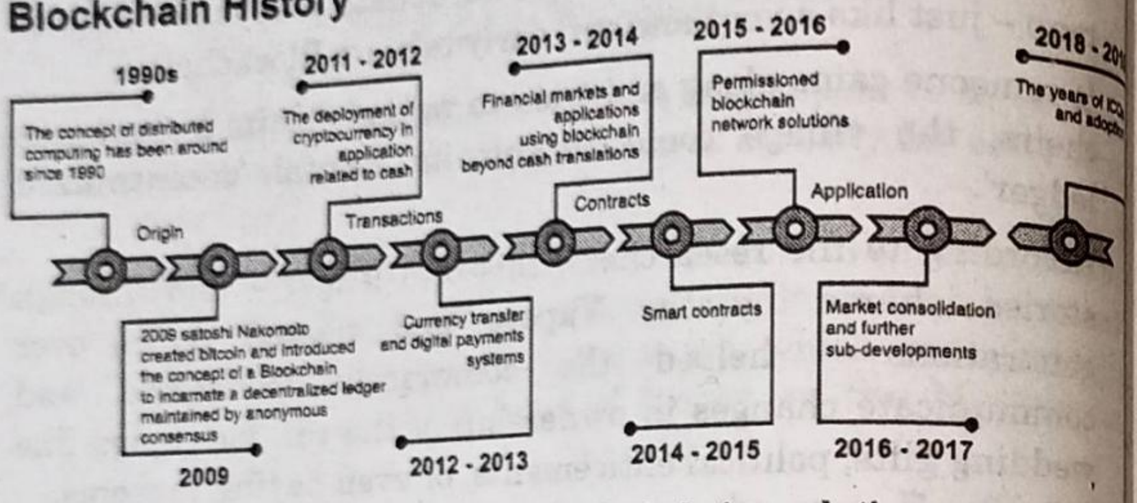


Fig. 2.1.3 : Timeline of blockchain evolution

☞ 1991–2008 : Early Years of Blockchain Technology

- Why did the blockchain develop? In 1991, Stuart Haber and W Scott Stornetta dreamed of what many today call to a blockchain. Their initial project was creating a chain of block that was cryptographically secure such that documen timestamps could not be altered.
- The system was modified in 1992 to include Merkle trees which increased performance and allowed for th accumulation of more documents on a single block.
- The work of one individual or group by the name of Satosh Nakamoto, however, is what gives Blockchain History its firs real importance in 2008, as opposed to earlier years.

- Blockchain technology is credited to Satoshi Nakamoto as its creator. There isn't much information available about Nakamoto, who is said to have worked on Bitcoin, the first use of the digital ledger technology.
- In 2008, Nakamoto created the first blockchain, from which the technology developed and found use in a variety of applications outside of cryptocurrencies. In 2009, Satoshi Nakamoto published the first whitepaper on the subject.
- He explained in the whitepaper how the decentralised feature of the technology meant that nobody would ever be in control of anything and that it was thus ideally suited to enhancing digital trust.
- Since Satoshi Nakamoto left the scene and gave control of the development of Bitcoin to other core developers, the technology of digital ledgers has developed, giving rise to new applications that make up the blockchain's history. As we can see, blockchain technology was created in 1991.

Blockchain Structure

- A peer-to-peer distributed ledger that is secure and used to record transactions among multiple computers is what Blockchain is, expressed simply. The only way to change the ledger's contents is to add a new block that is connected to an existing block. It may also be thought of as an internet-based peer-to-peer network.
- Blockchain, in layman's or commercial terms, is a platform that enables individuals to conduct transactions of any kind without the need for a central or reliable mediator.
- Everyone has access to the created database's contents because it is transparently shared across network users.
- Peer-to-peer networks and a time stamping server are used to manage the database on their own. Each block in a blockchain is set up so that it refers to the information in the block before it.
- Batches of transactions that have been approved by network participants are stored in the blocks that make up a blockchain. A cryptographic hash of a previous block in the chain is included with each block.

☞ Evolution of Blockchain : Phase 1- Transactions -2008-201 Blockchain 1.0: Bitcoin Emergence

- The majority of people think that Bitcoin and Blockchain a synonymous terms. That is untrue, as one is the fundamen technology that underlies most apps, among th cryptocurrency.
- At the height of the financial crisis in 2008, a mysterio individual, Satoshi Nakamoto sent a message to the enti world.
- This letter discussed Bitcoin, a brand-new peer-to-pe electronic payment system that did not include a middlemen.

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Fig. 2.1.4 : Original email message from Satoshi Nakamoto announcing Bitcoin

- He said that the double-spending issue that had trouble earlier digital currencies or cryptocurrencies had bee resolved. Nakamoto accomplished this by combining sever technologies and putting them together in creative way These technologies and ideas include, among other algorithms, game theory, economics, and cryptography.

- The word "blockchain" wasn't in use to characterise this new ledger technology at the time Bitcoin was introduced. Nakamoto created the first block, known as the "genesis block," from which subsequent blocks were mined and connected to create one of the longest chains of blocks holding various types of data and transactions.
- With the help of Satoshi's invention, a Bitcoin user may now deal digitally with another user without the need for a single, centralised middleman (like a bank) to approve the transaction. Previous digital transaction systems have failed to reach this achievement.
- Numerous applications have emerged since the advent of Bitcoin, a blockchain-based application, all of which aim to take use of the capabilities and guiding principles of the digital ledger technology. As a result, there is a vast number of uses for blockchain technology that have emerged over the course of history.

☞ Evolution of Blockchain : Phase 2- Contracts: 2013-2015: Blockchain 2.0 : Ethereum Development

- As one of the first contributors to the Bitcoin codebase and in a world where innovation is the norm, Vitalik Buterin is among a growing number of developers who believe that Bitcoin has not yet fully used the potential of blockchain technology.
- Because of the limits of Bitcoin, Buterin began developing what he thought would be a flexible blockchain that could serve a variety of purposes in addition to serving as a peer-to-peer network.
- A crucial turning point in the history of the blockchain came when Ethereum was introduced as a brand-new public blockchain in 2013 with more features than Bitcoin.
- By making it possible to store additional assets in addition to contracts, such as slogans, Buterin created Ethereum apart from the Bitcoin Blockchain.
- With the addition of the new functionality, Ethereum's capabilities were increased beyond those of a cryptocurrency to those of a platform for the creation of decentralised apps.
- Given its capacity to enable smart contracts that are used to carry out various functions, the Ethereum blockchain, which

was formally introduced in 2015, has developed into one of t
most significant implementations of blockchain technology.

- The blockchain technology for Ethereum has also be
successful in attracting a vibrant developer community, whi
has helped it build a real ecosystem.
- Ethereum blockchain processes the most number of dai
transactions thanks to its ability to support smart contrac
and decentralized applications. Its market cap has al
increased significantly in the cryptocurrency space.

☞ **Evolution of Blockchain : Phase 3- Applications-201**
Blockchain 3.0: the Future

- Ethereum and Bitcoin are just the beginning of th
blockchain's history and evolution. Several initiatives hav
emerged in recent years that all make use of the potential o
blockchain technology.
- In addition to developing new features utilising blockchai
technologies, additional initiatives have worked to fix some o
the shortcomings of Bitcoin and Ethereum.
- NEO, described as the first open-source, decentralised, an
blockchain platform developed in China, is one of the lates
blockchain applications.
- Even though the country has prohibited cryptocurrencies, i
remains active when it comes to blockchain technology. Wit
the support of Jack Ma, the CEO of Alibaba, NEO promote
itself as the Chinese Ethereum and aspires to challeng
Baidu's influence in the nation.
- IOTA was created as a result of certain developers usin
blockchain technology in the race to accelerate th
development of the Internet of Things.
- The cryptocurrency platform aims to offer no transaction cost
and unique verification procedures, and it is designed for th
Internet of Things environment. Additionally, it tackles som
of the scaling problems with Blockchain 1.0 Bitcoin.
- Other second-generation blockchain systems, in addition t
IOTA and NEO, are also making waves in the market. As a bi
to solve some of the security and scalability challenges relate

- to the early blockchain applications, the MoneroZcash and Dash blockchains were launched.
- The blockchain history previously covered includes open blockchain networks, in which anybody may view a network's contents. However, as technology has advanced, many businesses have begun integrating it within to improve operational effectiveness.
- In order to get a head start on the usage of technology, large businesses are making significant investments in employing professionals.
- When it comes to investigating blockchain technology applications, businesses like Microsoft and Microsoft appear to have taken the lead, leading to what are today known as private, hybrid, and federated blockchains.

☞ **2015 : Hyperledger**

- The Linux Foundation introduced the open-source blockchain Umbrella project in 2015. They continued by naming it Hyperledger, which is still being developed collaboratively as a distributed ledger.
- Under Brian Behlendorf's direction, Hyperledger aims to encourage cross-industry cooperation for the creation of blockchain technology and distributed ledgers.
- The primary goal of Hyperledger is to promote the use of blockchain technology in order to enhance the functionality and dependability of present systems that facilitate cross-border commercial transactions.

☞ **2017 : EOS.IO**

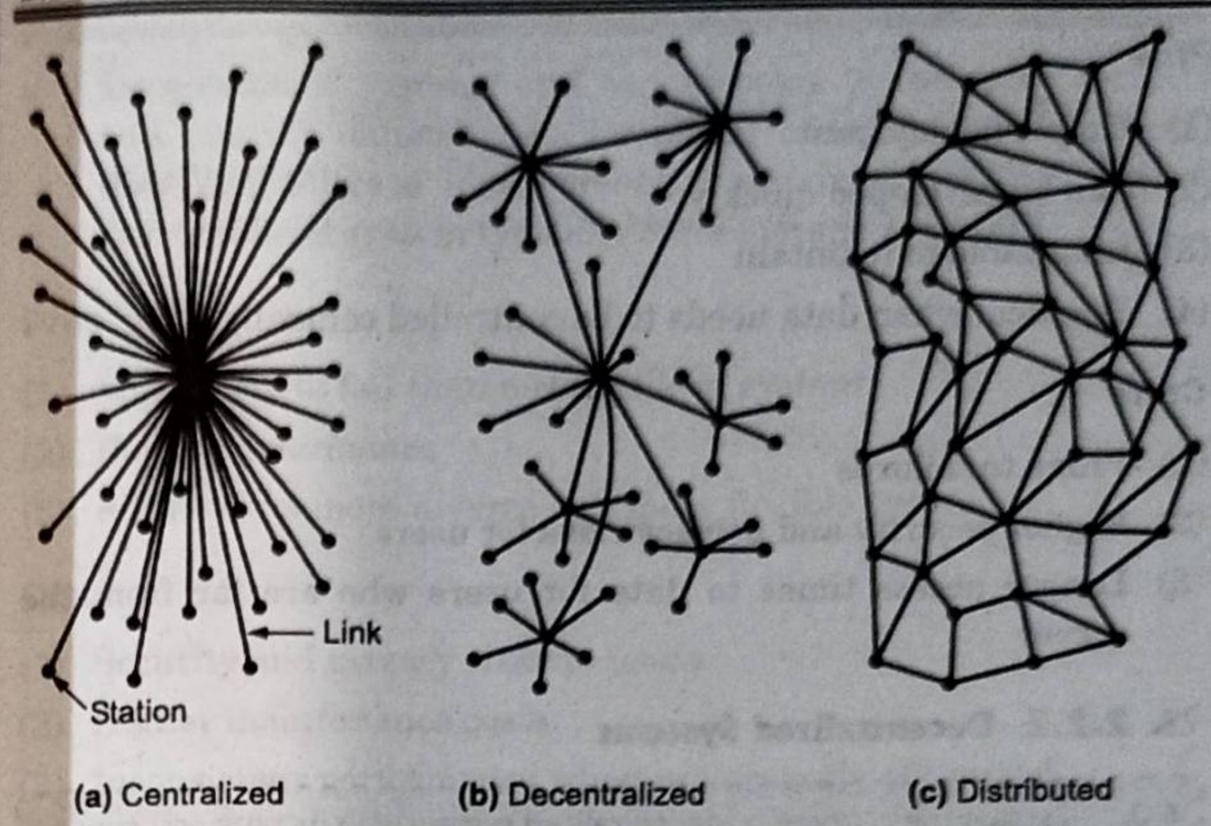
- The private firm block invented EOS. One was created in 2017 after a white paper describing a new blockchain system with EOS as the native coin was published.
- EOS, in contrast to other blockchain protocols, aims to mimic CPU and GPU functions found in real computers.

- Because of this, EOS.IO serves as both a platform for smar contracts and a decentralised operating system.
- Its primary goal is to promote the implementation o decentralised apps by means of an independent decentralise corporation.

2.2 CENTRALIZED VS. DECENTRALIZED VS. DISTRIBUTED SYSTEMS

GQ. Differentiate between centralised and decentralised system? **(4 Marks)**

- The distributed, centralised, and decentralised systems have an impact on practically everyone who uses the internet.
- It is fundamental to the growth and development of networks financial systems, businesses, applications, web services, and other systems.
- All of these systems are capable of functioning properly, although some are by design more reliable and secure than others.
- Systems can be quite compact, connecting just a few people and devices. Or they might be enormous and cover many continents.
- In any case, they deal with the same difficulties with scalability, fault tolerance, and maintenance expenses.
- The largest network in the world is the internet itself. In fact, it is so big that it integrates all these various systems into a sizable digital ecosystem. However, most businesses and people find it impossible to use all of these technologies. They have to choose. And you may have to choose, too.



(a) Centralized (b) Decentralized (c) Distributed

Fig. 2.2.1 : Centralized Vs. Decentralized Vs. Distributed Systems

2.2.1 Centralized Systems

GQ. Explain the concept of centralised system with its pros and cons. **(4 Marks)**

- All users in a centralised system are linked to a single "server" that controls the whole network. Both user information and data that may be accessed by other users are stored by the central owner.
- User profiles, user-generated content, and other details may be included in this user information. A centralised system may be quickly constructed and is simple to set up.
- However, this technique has a significant drawback. Users are unable to access the data if the server fails since the system is no longer functional.
- The availability of the network is dependent on this owner since a centralised system needs a central owner to link all the other users and devices.
- It is simple to understand why centralised systems are no longer the first option for many firms when you consider the obvious security issues that occur when one owner keeps (and has access to) user data.

Pros

(1) Simple deployment
(2) Can be developed quickly
(3) Affordable to maintain
(4) Practical when data needs to be controlled centrally

Cons

(1) Prone to failures
(2) Higher security and privacy risks for users
(3) Longer access times to data for users who are far from th server

2.2.2 Decentralized Systems

GQ. Explain the concept of decentralised system with its pros and cons. **(4 Marks)**

- Decentralized systems don't have a single central owner, a their name suggests. As an alternative, they use a number central owners, each of whom typically keeps a copy of th resources that users may access.
- Decentralized systems can experience crashes equally a frequently as centralised ones. It is, nevertheless, more fault tolerant by design. This is so that users may continue to acces data even if one or more central owners or servers fail.
- If at least one of the central servers is still running, resource are still available. This often implies that syste administrators may fix broken servers and take care of an other issues while the system itself continues to functio normally.
- In a decentralised system, server failures may degrad performance and restrict access to particular data. Howeve this approach provides a significant improvement over centralised system in terms of overall system uptime.
- This approach also has the benefit of often quicker data acces times. Owners can build nodes in various locations or place with a lot of user activity.

- Decentralized systems still expose users to the same security and privacy dangers as centralised ones, though. Although they can tolerate more errors, there is a cost for this. A decentralised system typically costs more to maintain.

Pros

(1) Less likely to fail than a centralized system
(2) Better performance
(3) Allows for a more diverse and more flexible system

Cons

(1) Security and privacy risks to users
(2) Higher maintenance costs
(3) Inconsistent performance when not properly optimized

2.2.3 Distributed System

GQ. Explain the concept of distributed system with its pros and cons. **(4 Marks)**

- In that it lacks a single central owner, distributed systems are comparable to decentralised ones. Further still, it does away with centralization.
- Users in a distributed system can enable user rights as required, but all users in the system have equal access to the data. The internet itself serves as the greatest example of a large, distributed system.
- Shared ownership of the data is made possible by the distributed system. Users are also given equal access to hardware and software resources, which might occasionally enhance system performance.
- A distributed system is protected from the simultaneous failure of many components, which can greatly increase uptime. The shortcomings of the previous systems led to the development of distributed systems.
- Distributed systems are the obvious choice for many businesses due to rising security, data storage, and privacy issues as well as the ongoing need to improve performance.

- The fact that distributed system technologies, most not the blockchain, are revolutionising several sectors is there not surprising.

Pros

(1) Fault-tolerant
(2) Transparent and secure
(3) Promotes resource sharing
(4) Extremely scalable

Cons

(1) More difficult to deploy
(2) Higher maintenance costs

2.2.4 Centralized vs Decentralized vs Distributed Systems Comparison

GQ. Compare between centralised Vs decentralised Vs distribute system? **(4 Mark**

- Now that you have a better understanding of every syste let's see how these systems compare with one another.
- The following head-to-head comparison focuses on key poin like fault tolerance, maintenance, scalability, developme and evolution. For each of these, we are using simple ratin like low, moderate, and high.

Table 2.7.1

Parameter	Centralized	Decentralized	Distributed
Fault tolerance	Low	Moderate	High
Maintenance	Low	Moderate	High
Scalability	Low	Moderate	High
Development	High	Moderate	Moderate
Evolution	Low	High	High

2.3 BLOCKCHAIN'S MECHANISM

GQ. Describe the blockchain mechanism in brief. **(4 Marks)**

- A distributed, peer-to-peer database called a blockchain stores an ever-increasing volume of transactions.
- Using consensus algorithms (i.e., a set of rules), each transaction, known to as a "block," is encrypted, timestamped, and verified by each authorised user of the database.
- A transaction cannot be added to the database if it has not been verified by all database users. A chain of transactions is formed when each transaction is sequentially connected to the one before it (or blocks).
- A transaction cannot be altered, resulting in an unchangeable audit trial. Only by including another transaction in the chain can a transaction be changed.
- Say, for example, that company X wishes to send money to company Y in order to settle an unpaid invoice for the purchase of software (Fig. 2.3.1).
- A block is made when Company X enters the transaction into the database.
- Every network user that has permission to receive broadcasts is informed of the block (or transaction).
- A block is subsequently added to the chain of transactions, providing an immutable and transparent record of the transaction, when all the participants have validated it (i.e., approved the payment).
- The transaction is then finished when the funds are transferred from company X to company Y.
- The blockchain's security prohibits hackers from impersonating legitimate network users.
- All transactions are replicated across the network of users and then stored in each member's computer system, enabling a distributed ledger-which may be shared across numerous locations, organizations, or countries.

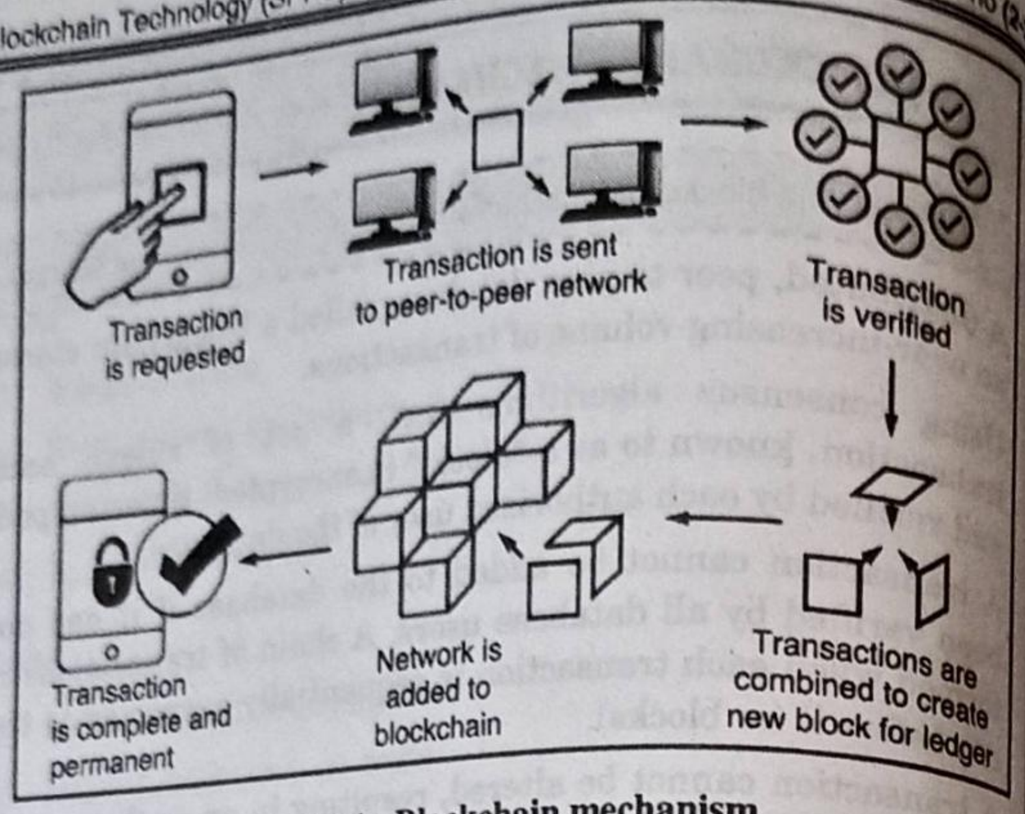


Fig. 2.3.1 : Blockchain mechanism

2.3.1 Structure of Block

GQ. Draw and explain the structure of block. (4 Marks)
GQ. State and explain the constituents of block header. (4 Marks)
GQ. Enlist the methods to identify the block uniquely? (4 Marks)
GQ. Write down the importance of genesis block? (2 Marks)

- Blocks are data structures within the blockchain database where transaction data in a cryptocurrency blockchain ar permanently recorded.
- A block records some or all of the most recent transactions no yet validated by the network. Once the data are validated, th block is closed. Then, a new block is created for ne transactions to be entered into and validated.
- A block is thus a permanent store of records that, once written cannot be altered or removed.
- A block is a container data structure that aggregate transactions for inclusion in the public ledger, the blockchain The block is made of a header, containing metadata, followe by a long list of transactions that make up the bulk of its size.
- The block header is 80 bytes, whereas the average transactio is at least 250 bytes and the average block contains more tha 500 transactions.

- A complete block, with all transactions, is therefore 1,000 times larger than the block header.

Table 2.3.1 : Structure of the Block

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

☞ Block Header

The block header consists of three sets of block metadata.

- First, there is a reference to a previous block hash, which connects this block to the previous block in the blockchain.
- The second set of metadata, namely the difficulty target, timestamp, and nonce, relate to the mining competition.
- The third piece of metadata is the merkle tree root, a data structure used to efficiently summarize all the transactions in the block.

Table 2.3.2 : The structure of a block header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The proof-of-work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the proof-of-work algorithm

Version

It states the version that the particular block is using, the are three types of Blockchain version.

(1) Blockchain Version 1.0 (cryptocurrency)-It used a public ledg to store the data, for example, Bitcoin.

(2) Blockchain Version 2.0 (smart Contract)- It is called smar contracts which is self-executing programs, for exampl Ethereum.

(3) Blockchain Version 3.0 (DAPPS)- It is used to create decentralized structure, for example, tor Browser.

(4) Blockchain Version 4.0 (Blockchain for Industry)- It is used create a scalable, affordable blockchain network such tha more people could use it.

Previous Hash

As Blockchain is a collection of several interconnected node also called a block, so previous hash stores the hashed value the previous node's address, First block in the blockchain called the Genesis Block and has no previous block hash valu

Merkle Root

A Merkle root uses mathematical formulas to check if the dat is not corrupted, hacked, or manipulated. For example Suppose one block has 10 transactions, then to identify tha block we need 10 transactions to combine and form one Has Value, so it uses the concept of the binary tree to create th hash of the block and that value is called the Merkle Root.

Timestamp

Timestamp in the blockchain is used as proof that th particular block is used at what instance of a time, also thi timestamp is used as a parameter to verify the authenticity o any block.

Difficulty Target

It specifies the complexity and the computation power require to mine the network, if we are having a high difficulty targe then it implies that we need more a computationally expensiv

machine to mine it. For example, in order to increase the difficulty target algorithms such as SHA-2, SHA-3. RIPEMD, MD5,BLAKE2 is used.

Nonce

It is abbreviated as 'number only used once' and it is a number which blockchain miners are finding and on average, it takes almost 10 times to find out the correct nonce. A nonce is a 32-bit number, having the maximum value as 2^(32) total possible value, so the job of the bitcoins miners is to find out the correct integer value which is a random integer between 0 and 2^(32), so it becomes computationally expensive.

Block Identifiers : Block Header Hash and Block Height

- A block's principal identifier is its cryptographic hash, or digital fingerprint, which is created by running the block header through the SHA256 algorithm twice.
- Since just the block header is utilised to compute it, the resultant 32-byte hash is more suitably known as the block header hash.
- The block hash of the very first bitcoin block ever produced, for instance, is 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.
- By simply hashing the block header, every node may independently extract the block hash, which uniquely and clearly identifies a block.
- Take note that when a block is transmitted across the network or kept on a node's persistent storage as part of the blockchain, the block hash is not really contained inside the block's data structure. Instead, as each node receives a block from the network, it computes the block's hash.
- To facilitate indexing and expedite block retrieval from storage, the block hash may be kept in a separate database table as part of the block's metadata.
- The block height, or position inside the blockchain, is a second identifier for a block.

- The first block that has ever been produced has a block heigh of 0 (zero), and it is the same block that was previously identified by the block hash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f b60a8ce26f.
- Thus, there are two methods to recognise a block: by using t block hash or by using the block height. Like boxes stacked o top of one another, each additional block that is placed "on to of the original block moves it up one position in the blockchain On January 1, 2014, there were roughly 278,000 blocks buil on top of the first block that was made in January 2009.
- The block height is not an unique identifier. The block heigh does not always identify a single block, even though a singl block will always have a unique and invariant block height.
- The same block height might be shared by two or more block that are competing for the same position on the blockchain Additionally, the block height is not stored inside the block; i is not a member of the block's data structure.
- When a block is received from the bitcoin network, each nod dynamically determines its position (height) on the blockchain For quicker retrieval, the block height might alternatively b saved as metadata in a database table that is indexed.

The Genesis Block

- The genesis block, which is the first block on the blockchain was made in 2009. Because it is the genesis block, you may start at any block in the blockchain and work your way backward in time to reach it. It is the common ancestor of all the blocks in the system.
- Because the genesis block is statically encoded inside the bitcoin client software, making it unchangeable, every node always starts with a blockchain of at least one block.
- Every node "knows" the hash and structure of the genesis block, the exact timestamp it was generated, and even the specific transaction included inside. As a result, every node has access to a safe "root" from which to construct a reliable blockchain.

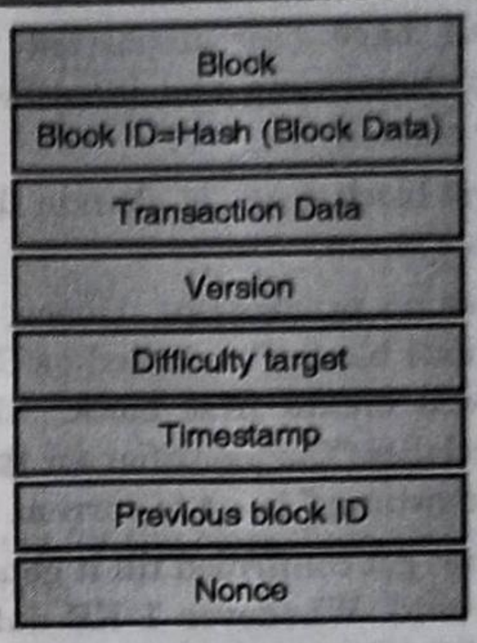


Fig. 2.3.2 : Sample block structure

2.3.2 Process of Chaining of Blocks

GQ. Elaborate the chaining process of blocks. **(4 Marks)**

GQ. If someone tries to hack Block no5 in a chain of 15 Blocks. What will happen and why? **(4 Marks)**

- Let us capture the data in fixed size sets (say 1 KB each), called as blocks. These blocks will get unique identifier based on the contents of data. These identifiers are created using hashing mechanism..

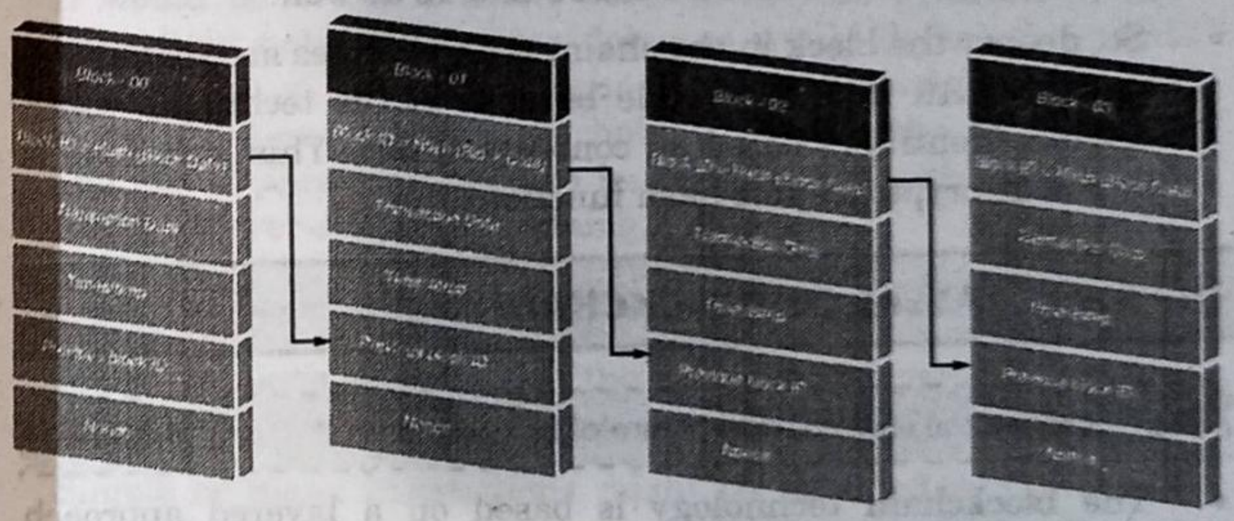


Fig. 2.3.3 : Chaining of blocks[For simplicity, few elements are not shown in block]

- Each block shall have four important sections: identifier, transaction data, timestamp and identifier of previous block along with other elements.
- Logically, the first block does not contain the pointer since the one is the first in a chain.
- The 1st block has no predecessor. Hence, it does not contain hash of the previous block. It is called as Genesis block. In the beginning, we will create first block: BLOCK-01. For the block, we will initialize "the identifier for the previous block" as zeros and the "timestamp" is set to current timestamp.
- This block does not get confirmed till it gets enough data i.e. (1 KB) that it can hold. Whenever 1 KB data is confirmed, we update "data" of BLOCK-01 to received data.
- The identifier of BLOCK-01 will be created using contents of block including "data", "timestamp" and "previous block identifier" of BLOCK-01.As BLOCK -01 is confirmed, the second block (BLOCK-02) is created with "previous block identifier: set to identifier of BLOCK-01.The process keeps repeating many times as required.
- There is potentially going to be a final block within the blockchain database that has a pointer with no value. Suppose there is chain of 10 blocks. Some malicious user try to update contents of BLOCK-07->it will impact on its identifier->it will require to change identifier of BLOCK-08->in turn ,it will need to change identifier of BLOCK 09 and 10 as well.
- So, deeper the block in the chain, more changes are required to update it.All this is possible because of the technique which creates identifiers based on contents of data.This technique is called as cryptographic hash functions.

2.4 LAYERS OF BLOCKCHAIN

GQ. Explain the layered architecture of Blockchain. **(6 Marks)**

- The blockchain technology is based on a layered approach Fig. 2.4.1. The block- chain technology is decomposed into several layers that will in turn help in better understanding of security and the design of the blockchain.

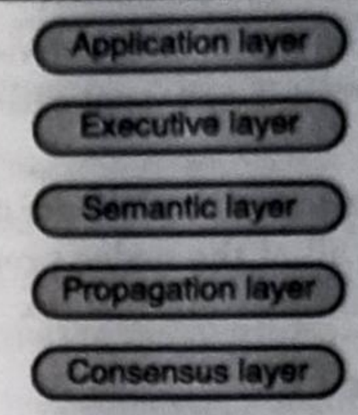


Fig. 2.4.1 : Blockchain layers

- There are few layers for the blockchain technology discussed in the following sections

(a) Application Layer

- As a shared ledger system that is tamper-proof, decentralised, and has many advantages, blockchain technology may be the foundation for a variety of applications.
- The application layer is on top of this layer suit because some apps with built-in application layers can communicate with the other levels.
- A user can programme the needed functionality and create the application for the application's user at the application layer. The programme has to be deployed on each node because the blockchain is a decentralised technology and there isn't a server involved.
- It would be better if there were no servers involved in the blockchain network because doing so would defeat the point and benefit of blockchain technology, even though there are some situations where blockchain is used in the background and the applications need to be hosted on a web server and require server-side programming.

(b) Execution Layer

- All instructions performed at the application layer are handled by this layer for all nodes connected to the blockchain network.
- Simple or many instructions might be included in the set of instructions. For instance, a smart contract is a little piece of code that must be run when payment has to be moved from one person to another.

- The code must now be performed individually on each nod the blockchain network if one application is present on a them.
- The execution of code on a set of inputs should always result the same output for all of the nodes present on the blockch in order to prevent inconsistent results.

(c) Semantic Layer

- This layer is also known as the logical layer in the blockch layer hierarchy. This layer is concerned with validating b the blocks that are created in the network and transactions that are carried out inside the blockchain.
- A set of instructions are carried out on the execution layer a validated on the semantic layer when a transaction is initiat from a node.
- The connection of the blocks created in the network is anoth function of the semantic layer. With the exception of t Genesis block, each block on the blockchain contains the ha of the one before it. On this layer, this block linkage must defined.

(d) Propagation Layer

- The peer-to-peer communications that enable nodes in network to find one another and synchronise with anoth node are handled by the propagation layer.
- Every node in the network receives a broadcast when transaction is completed. Additionally, when a node proposes block, it is immediately broadcast throughout the wh network so that other nodes can use it and contribute to it.
- As a result, this layer defines how a block or transacti distributes throughout the network and maintains the overa stability of the system.
- But depending on the network's capacity or bandwidt sometimes the propagation happens immediately and som other times it takes a while.

(e) Consensus Layer

- The majority of blockchain solutions start at this layer. This layer's primary goal is to ensure that all nodes must come to an agreement on a shared understanding of the shared ledger. The layer also addresses the blockchain's safety and security.
- There are a variety of consensus algorithms that may be used to create cryptocurrencies like Bitcoin and Ethereum. These algorithms employ the proof-of-work mechanism to choose a random node from among the network's nodes 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.

2.5 ACTORS IN BLOCKCHAIN TECHNOLOGY

GQ. List and explain various actors in a blockchain technology solutions. **(4 Marks)**

(1) Blockchain Architect

- Responsible for the architecture and design of the blockchain solution.
- A blockchain architect will design how a blockchain solution is going to be built.
- He/she will identify what information needs to be stored, what are some of the transactions and business logic that need to be embedded onto a network, how the network itself should to be created, etc.

(2) Blockchain developer

- A blockchain developer will take what has been architected and he/she will develop the actual code that will run on the blockchain network.

- The developer of applications and smart contracts
interact with the blockchain and are used by blockch
users.

(3) Blockchain network operator

- A blockchain network operator manages and monitors
blockchain network.
- Each business in the network has a blockchain netw
operator.

(4) Traditional processing platform

- There are traditional processing platforms or oth
systems of record that the blockchain connects to a
might send or get information.
- An existing computer system which may be used by
blockchain to augment processing. The system may a
need to initiate requests into the blockchain.

(5) Traditional data sources

- Traditional data sources and databases are also part
the blockchain solution.
- An existing data system which may provide data
influence the behavior of smart contracts.

(6) Membership services

- It is an important component. It defines or provides
identity for users to come and transact on the blockcha
For example, when you open an account in the bank,
bank gives you a username and password for login
access web services.
- The membership service will provide a digital certific
that will allow an individual to transact on the network
manages different types of certificates required to run
permissioned blockchain.

(7) Blockchain user

- A blockchain user will perform business transactions on the blockchain. These users could belong to multiple organizations that are participating in the blockchain network.
- He/she is a business user operating in a business network. Blockchain users interact with the blockchain using an application. However, they are unaware of the blockchain.

(8) Blockchain regulator

- The regulator could be an optional actor in a blockchain solution.
- The regulator might have read only access onto the network where he/she might have some oversight into whether the transactions performed are legitimate or not. Whether the transactions are compliant with the policies set by the blockchain regulator.
- A blockchain regulator is responsible for the overall authority in a business network. In particular, they may require broad access to the contents of a ledger.

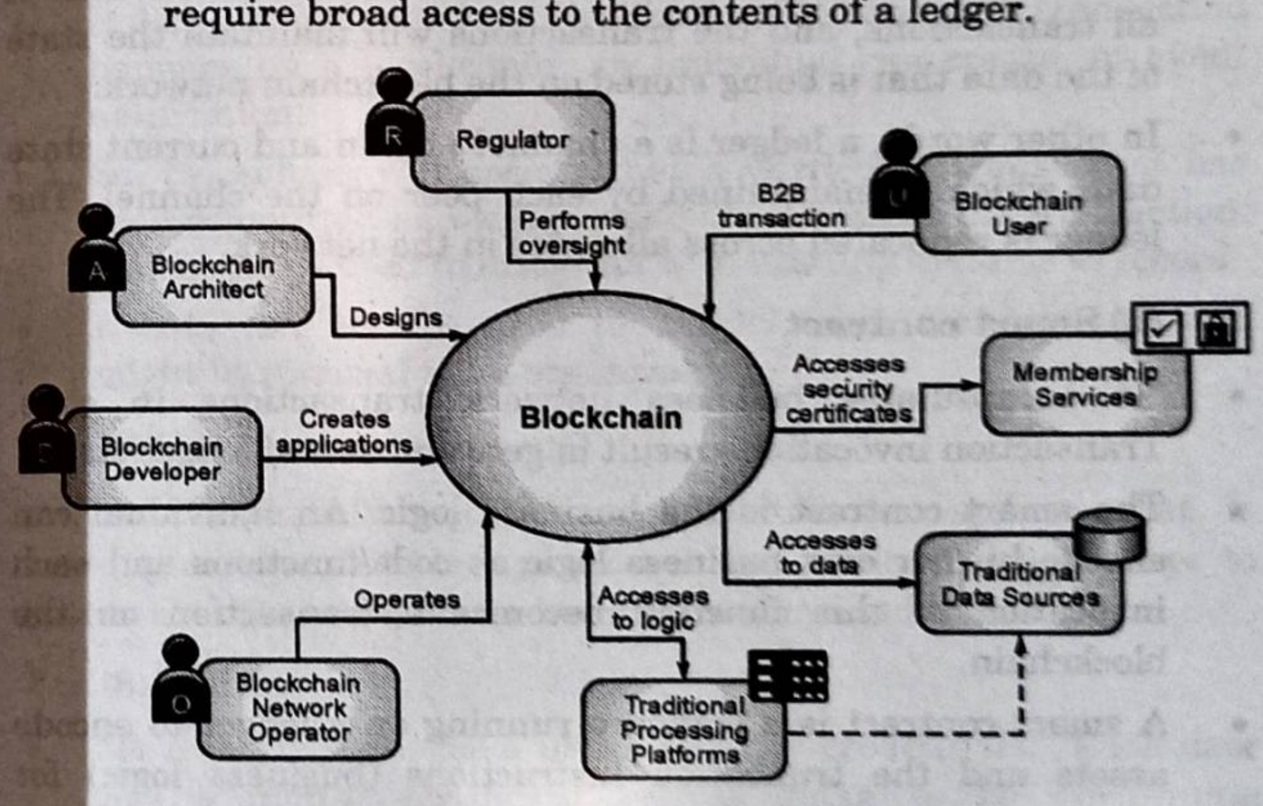


Fig. 2.5.1 : Actors in blockchain technology

2.6 IMPORTANT TERMS RELATED TO BLOCKCHAIN TECHNOLOGY

GQ. State and explain different terms related to blockchain. **(4 Marks)**

A variety of blockchain components are available in market. Some of the major components in a blockchain solution as follows :

(1) Ledger	(2) Smart contract
(3) Peer network	(4) Consensus network
(5) Membership	(6) Events
(7) System management	(8) Wallet
(9) System integration	

(1) Ledger

- It contains the current world state of the ledger and blockchain of transaction invocations."
- Every node in the blockchain network will maintain a ledger all transactions, and the transactions will maintain the sta of the data that is being stored on the blockchain network.
- In other words, a ledger is a channel's chain and current sta data which is maintained by each peer on the channel. T ledger is replicated across all nodes in the network.

(2) Smart contract

- "It encapsulates business network transactions in co Transaction invocations result in gets and sets of ledger stat
- The smart contract is the business logic. An individual c encode his/her own business logic as code/functions and ea invocation of this function becomes a transaction on t blockchain.
- A smart contract is a software running on a ledger to enco assets and the truncation instructions (business logic) f modifying the assets.

(3) Peer network

A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.

(4) Consensus network

- It is a collection of network data and processing peers forming a blockchain network.
- It is responsible for maintaining a consistently replicated ledger.

(5) Membership

- "It manages identity and transaction certificates as well as other aspects of permissioned access."
- A membership service provides identities for the users to transact on the blockchain.

(6) Events

- "It creates notifications of significant operations on the blockchain (e.g., a new block) as well as notifications related to smart contracts.
- It does not include event distribution." Whenever a transaction happens on a blockchain, an individual can create an event notification.
- So, blockchain will specify that a particular transaction has been committed and will provide the details of the transaction, which can be used to integrate with existing systems of record.
- Events can also be used to trigger other transactions that might be internal to an organization.

(7) System management

The blockchain network is a distributed system that is running across multiple organizations so it requires new ways to create, change, and monitor blockchain components.

(8) Wallet

- "It securely manages a user's security credentials." Each user has a digital certificate and is going to be performing transactions using the digital certificate.

- There needs to be a place where a user can securely store t private information. So, a digital certificate contains private identity of an individual.
- He/she should not be sharing the information with anyb else, which is securely managed in a wallet.

(9) System integration

- It is responsible for integrating blockchain bi-direction with external systems.
- It is not a part of the blockchain, but used with it.

2.7 WHY IS BLOCKCHAIN IMPORTANT ?

GQ. Elaborate the importance of blockchain w.r.t to safety. (4 Marks)

GQ. How decentralization is achieved through blockchain technology? (4 Marks)

GQ. How digital freedom can be achieved through blockchain? (4 Marks)

GQ. Which features makes blockchain important over traditional system? (4 Marks)

- By examining its fundamental characteristics, you m understand the blockchain's significance at its core.
- Blockchain stands out as the finest option because to thes properties that make it tempting in a variety of situations.

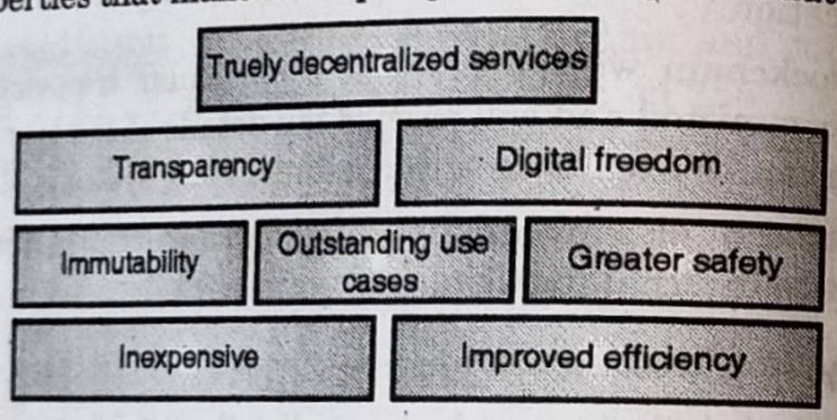


Fig. 2.7.1 : Importance of blockchain

☞ Immutability

- Blockchain cannot be changed. This creates several chances fo platforms that require immutable characteristics to improv the functionality of their system in a highly competitiv industry.
- Take the supply chain as an example. Immutability enable

businesses to guarantee that the packages are not harmed while in transit.

- The package information cannot be changed in any manner since blockchain is immutable. The system will alert you to any changes.

☞ Transparency

- Transparency is another crucial factor that contributes to blockchain's significance. There are several blockchain variants.
- Due to its nature, public blockchain offers transparency. It serves many purposes in our society, including voting.
- Companies can use it to make sure that procedures are fully or partially transparent to the end user.

☞ Digital Freedom

- Freedom is one of your rights as a person. There are centralised organisations that provide connectedness in terms of the economics but also limit our independence.
- Consider your bank as an example. If considered appropriate, it has the power to halt your transactions or seize your account.
- Some banks take this action, even though the account holders haven't broken any laws. So, if you are taking blockchain into account, you will find there is no centralized authority.
- You can achieve true digital independence with blockchain. You are your own bank. You have sole authority over when and how much money you withdraw.
- You are the only owner and liable party for your assets because there is no centralised authority. It grants you the independence in the digital world that is mainly dependent on blockchain technology.

☞ Truly Decentralized Services

- Our advanced civilization is built on decentralised services. There will be decentralised services for every industry out there, whether it is asset management or energy management.

- People will have easy accessibility to products that
already on the market because to this. Decentralized
will be present in almost every sector.
- The music industry, for example, can benefit from
decentralized services where both creator and consume
participate without the need for any approval from a
centralized corporation.

Outstanding Use-Cases

- Blockchain is not restricted to a single use-case. Blockchain
therefore a great technology for our society's future.
- Nearly every industry, including banking, governme
education, healthcare, the oil industry, and others, may uti
it. They also have a great influence.

Greater Safety

- In order to increase the security of the data kept on
network, blockchain employs cryptography. In addition to
encryption, the decentralised element of blockchain make
more secure than previous systems.
- To safeguard the data and systems on the blockchain netwo
cryptography makes use of sophisticated mathemat
methods.
- Additionally, every block on the network has a distinct ha
making it impossible for hackers or malevolent actors to al
or fake any data.

Inexpensive

- Comparatively speaking to other technologies, blockchain
less costly. The buffer necessary to run the network effectiv
is removed when centralised authority is removed.
- Cost effectiveness is increased since there is no need to pay
middleman when there is no centralization. Using blockch
in the supply chain drastic decrease paperwork.
- The expense of the documentation is significant. There a
other expenses, such as paying staff to handle the paperwo
and keep the middlemen up to date.

Improved Efficiency

- Another justification for the significance of blockchain is increased productivity. The root of the problem is improved procedures, intermediate elimination, and security.
- Additionally, transactions, particularly international ones, now take seconds to complete rather than a week.

2.8 LIMITATIONS OF BLOCKCHAIN TECHNOLOGY

GQ. What are the limitations of blockchain technology? **(6 Marks)**
GQ. Blockchain needs high energy consumption. How? **(4 Marks)**
GQ. What are the interoperability and scalability issues of blockchain? **(4 Marks)**

- Although we are talking about the future, there are now just a few blockchain use cases that can be found and accepted, despite the fact that there are several protocols and consortiums supporting it.
- Mostly because to a lack of knowledge, resources, ability to handle the complexity that already exists, and countless other problems. What are the primary limitations limiting blockchain's potential then?

Complexity of Blockchain

- The network's intricacy is what gives blockchain its charm. The greater the number of participants involved in a transaction, the more widely applicable the blockchain will be.
- Due to the fact that there were initially so few nodes running the blockchain, many PoCs were completely impractical in terms of cost-effectiveness and operationality.
- Additionally, the majority of companies and banks are now utilising blockchain in limited ways. Entities have used a mixed strategy rather than adopting a totally centralised or decentralised strategy.
- This significantly increases complexity. Even though their current applications are minor, additional businesses must deploy specialised blockchain expertise.

- Secondly, it is difficult to easily replicate a block... application across different activities and use-cases. ... application requires a better comprehension of the operati... requirements, and blockchain might be very differen... applications like land records and insurance contracts.

Network size

- Blockchains (like other distributed systems) are "antifr... in the sense that they respond to attacks by becoming m... robust, rather than being particularly resistant to malic... actors.
- But to do that, you need a lot of users. To fully benefit fro... blockchain, a network must be stable and have a grid of n... that is broadly spread.

Lack of speed

- The requirement to accelerate processing rates is anot... significant issue that has to be addressed. The netw... typically slows down as the number of users rises, mak... transactions take longer to process.
- Large transaction costs might come from this, which wo... make the technology less and less appealing. Additionally, t... system's encryption may slow it down even more. ... transaction may take several hours, or even days, to comple...
- Therefore, it works well for conducting significant transactio... where timing is not a key consideration. This difficulty wi... blockchain adoption might soon present a barrier.

Lack of standardization

- The absence of standards is a fourth problem preventing ... more widespread use of blockchain technology.
- To achieve a scalable acceptance of any technology over th... world, standards are necessary. For the blockchain technolo... to function across all networks, they must all speak the sam... language in order for the transaction to be understood as ... completed.
- However, this is a problem with all new technology at th... beginning until standards eventually improve with time as ... practise.

Lack of interoperability

- As more companies began adopting blockchain, there is a tendency for many of them to create their own systems with unique features (governance rules, blockchain technology versions, consensus models, etc.).
- Most of these distinct blockchains do not interact with one another, and there is presently no global standard to let various networks to communicate to one another.
- Interoperability between blockchain networks refers to the capacity to share, see, and access data without the intervention of a middleman or centralised authority.
- Due to this lack of compatibility, broad adoption may be all but impossible.

Unavoidable security flaw

- Bitcoin and other blockchains have one significant security flaw: if more than 50% of the computers acting as nodes to serve the network report a fraud, the lie will be accepted as the truth.
- When Satoshi Nakamoto created bitcoin, he highlighted this so-called "51 percent attack."
- Because of this, the community actively monitors bitcoin mining pools to make sure no one unintentionally gets such network dominance.

Lack of privacy

- An added challenge with the blockchain is privacy.
- The transparency that results from having a record of a network's transaction history that is accessible to the public and simple to verify is one of the biggest advantages of blockchain technology, and public blockchain networks in particular.
- This is not always seen positively, though, as it also puts users' or organisations' privacy at risk. Many businesses that deal with privacy need to have clear guidelines.
- Businesses are hesitant to use some of the most well-known blockchain protocols because they want to preserve their trade secrets and other sensitive information.

☞ High Energy Consumption

- One of the most well-known and original uses of blockchain is bitcoin. Every node that is a member of blockchain network has to have 200 GB of storage sp available for the Bitcoin Core.
- A daily 5 GB upload and 500 MB download is one of criteria. Certainly, many nations need to modernise th infrastructure significantly before using blockchain.
- Energy use continues to be a major problem for miners in context of the Bitcoin blockchain. According to studi conducted by the University of Cambridge, Bitcoin uses m energy than the whole country of Switzerland.
- The energy is mostly used to maintain the continuo operation of the whole network. Imagine the situation if th were many more similar networks because there is only blockchain at now.

☞ Scalability Issues

- Another potential problem and limitation for many blockcha applications is scalability. Compare Visa, the large centralised payment system, with Bitcoin, the large cryptocurrency payment system.
- The maximum speed of Bitcoin is 7 transactions per secon but Visa can perform 65,000 transactions per second.
- In a centrally controlled architecture, the controlling authori determines the flow and doesn't needlessly inform other pee about a transaction. This expedites and saves time.
- Because a majority of nodes must approve the transaction in blockchain architecture, validation might take severa minutes.

☞ Politics

- There have been many possibilities for public argument between various community sectors since blockchain protocol provide a chance to digitise governance models and becaus miners are effectively building another sort of incentive governance model.

- The issue or event of "forking" a blockchain, which entails altering the blockchain protocol after a majority of a blockchain's users have approved it, is where these differences, which are a significant aspect of the blockchain sector, are most visibly expressed.
- These discussions, albeit occasionally controversial and extremely technical, are instructive for anybody curious in the mix of democracy, consensus, and novel options for governance experimentation that blockchain technology is enabling.

⏭ 2.9 BLOCKCHAIN ADOPTION SO FAR

GQ. Comment on various hurdle in adoption of blockchain technology by industry.

GQ. What can be the problems of blockchain technology adoption by finance sector?

GQ. What do you think, which limitations of blockchain are major hurdles in its adoption?

GQ. Are Interoperability and standardization are major roadblocks in blockchain adoption? Comment.

- Blockchain ecosystems require widespread acceptance in order to function well. The efficiency and scalability of blockchains will be constrained without widespread adoption.
- Governments and other public organisations must actively assist the adoption of blockchain and DLTs by addressing the different hurdles.
- Organizations are increasingly joining together to create collaborative blockchain working groups in order to address shared problems and create universally beneficial solutions without disclosing confidential information.
- Numerous operational apps and projects that are in great working order already exist. The evolution of the blockchain will continue, as with any technical advancement.
- There could be difficulties, but they shouldn't be viewed as roadblocks.

- **Industries adapting Blockchain are :**
  - (1) Automotive
  - (2) Banking and financial services.
  - (3) Government.
  - (4) Healthcare and life sciences.
  - (5) Insurance.
  - (6) Media and entertainment.
  - (7) Retail and consumer goods.
  - (8) Telecommunications.
  - (9) Travel and transport
  - (10) Supply chain
  - (11) Oil and gas
  - (12) Manufacturing