2.1 HISTORY OF BLOCKCHAIN

- The Blockchain Technology was described in **1991** by the research scientist **Stuart Haber** and **W. Scott Stornetta**. They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be backdated or tampered. They develop a system using the concept of **cryptographically** secured chain of blocks to store the time-stamped documents.
- In **1992**, Merkle Trees were incorporated into the design, which makes Blockchain more efficient by allowing several documents to be collected into one block. **Merkle Trees** are used to create a 'secured chain of blocks.' It stored a series of data records and each data records connected to the one before it. The newest record in this chain contains the history of the entire chain. However, this technology went unused and the patent lapsed in 2004.

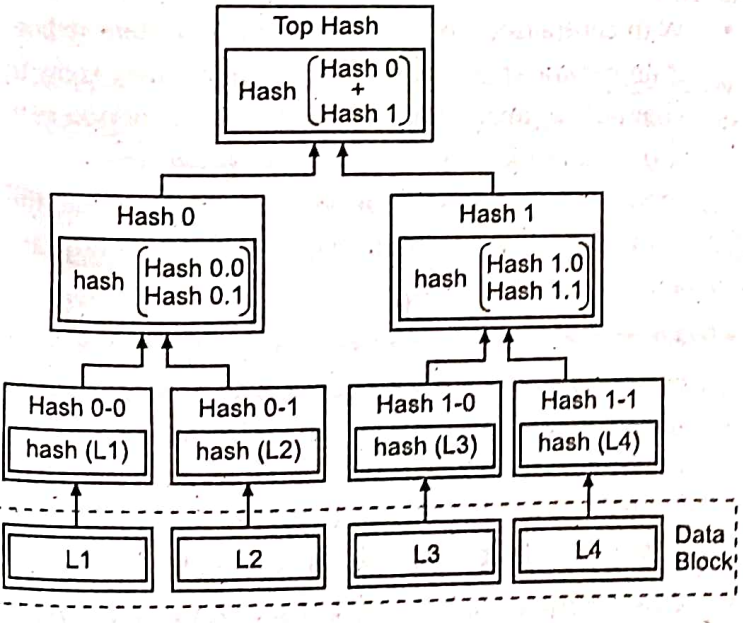

Fig. 2.1

Hal Finney

- In **2004**, computer scientist and cryptographic activist **Hal Finney** introduced a system called **Reusable Proof of Work (RPoW)** as a prototype for digital cash. It was a significant early step in the history of cryptocurrencies. The RPoW system worked by receiving a non-exchangeable or a non-fungible Hashcash based proof of work token in return, created an **RSA-signed** token that further could be transferred from person to person.
- RPoW solved the double-spending problem by keeping the ownership of tokens registered on a trusted server. This server was designed to allow users throughout the world to verify its correctness and integrity in real-time.

Satoshi Nakamoto

- Further, in **2008**, **Satoshi Nakamoto** conceptualized the theory of **distributed Blockchains**. He improves the design in a unique way to add blocks to the initial chain without requiring them to be signed by trusted parties. The modified trees would contain a secure

history of data exchanges. It utilizes a peer-to-peer network for time stamping and verifying each exchange. It could be managed autonomously without requiring a central authority. These improvements were so beneficial that makes Blockchains as the backbone of cryptocurrencies. Today, the design serves as the public ledger for all transactions in the Cryptocurrency space.

- The evolution of Blockchains has been steady and promising. The words block and chain were used separately in Satoshi Nakamoto's original paper but were eventually popularized as a single word, the Blockchain, by **2016**. In recent time, the file size of Cryptocurrency Blockchain containing records of all transactions occurred on the network has grown from **20 GB** to **100 GB**.

2.2 CENTRALIZED VS. DECENTRALIZED SYSTEMS

- In the world of Blockchain, you will find the decentralized vs. centralized debate a lot. After all, Blockchain technology can make centralized systems a thing of the past.

	Centralized	Decentralized
Third-Party Involvement	Yes	No
Control	Full control stays with the central authority	Control stays with the user itself
Hackable	More prone to hacks and data leaks	Less prone to hacks and data leaks as no single point of failure
Single Point of failure	Yes	No
Ease of use	Intuitive and easy to use	Not easy to use
Exchange fees	Higher fees	Less fees
Anonymous	Users are not anonymous	Offers anonymity

- Centralization revolves around us more than you can expect. If you are using social media platforms such as Facebook, then you are using a centralized system. Other popular online platforms such as YouTube are also centralized.

So, What Does It Mean?

- It means that a central authority is in control of the data and functions of the said platform. So, if you are using the Facebook platform, then the company Facebook has complete control over the different aspects of their features including the ability to decide who and who cannot join the platform.
- If you want a technical perspective, then the centralized system requires third-party intermediaries to verify data. This means if you are sending a message to your friend using the Facebook platform, then the data will be verified and then transferred by the said platform.
- Another great example would be sending an email. The moment you send an email to another person, the email service provider has the knowledge of what you sent and when you sent it. This information is stored privately without any identifier, but the email service, in any case, has a copy of that information.
- In short, the centralized services have your information stored with your consent. If you remember the first time you create an account on any centralized platform such as Facebook, Yahoo, Gmail, etc., then you had to give them your full name, nationality, date of birth and any other information to register on the platform.

Advantages of Centralization

- There are undoubtedly multiple benefits or advantages of centralization. They are listed below:

1. Command Chain

- With centralized, the command chain is clearly defined. If an organization utilizes centralization, they know the chain of command. This means that every person in the organization knows their role and whom they need to report too. They also know which person is under their control and are responsible for their subordinates' actions as well.
- All of these also mean that delegation is easy in the chain. Senior executives can easily delegate work to their subordinates and finalize and finish the work in the best possible way. If work is successfully completed, it creates a level of trust among the workers and chain, improving the confidence required to make it work.
- When it comes to a network that utilizes centralization, one central node or a collection of nodes are responsible for transactional verification.

2. **Reduced Costs**

- One of the biggest advantage of centralization is the cost associated with it. Any centralized network or infrastructure requires less support and cost. As centralized organizations or networks are pre-planned, the costs associated with it do not cross budgets until and unless it is absolutely required to expand the network.

3. **Quick Decision Implementation**

- There is no doubt that centralization organizations or networks enable quick decision implementation. As centralized networks have fewer nodes or people, it requires less communication among the different levels of authorization.
- Also, if a centralized network decides to implement a change, it can be done in a matter of minutes. For instance, a centralized network can put more stress on the KYC procedure and decided to add more requirements for it. As the network is centralized, they can push the new guidelines or change the KYC procedure which can go live almost instantly after proper testing.

Disadvantages of Centralization

- There are also various disadvantages of centralization. Some of them are as below:

1. **Trust**

- Even though centralized organizations are secure and trustable, they are not 100% secure or trustable. The trust is an agreement that is set by the service provider and the user.
- However, that's an agreement and it can break easily. Big corporations suffer from trust issues from their users, from time to time.
- It happens when there is a lapse of security in the system; people tend to ignore the service for some time before the service provider mends the trust by offering solutions and remuneration to those affected.
- All of this happens because of centralization and the reason that all the data are stored in a centralized database.

2. **Single Point of Failure**

- Centralization also means that the whole network is dependent on a single point of failure. Organizations know about the disadvantage and hence have deployed measures to contain it. However, the fact that there is a chance for failure is a big disadvantage for mission-critical services.

3. **Scalability Limitation**

- As a single server is used in most cases, it leads to scalability limitations.

What's the Current State of Centralization?

- Centralization is undoubtedly an effective way to manage organizations or networks. It has been effectively used by big organizations such as Microsoft, Facebook, Yahoo and so on. In fact, our governments are also reliant on a centralized approach.
- In the case of a centralized government, the political executives coordinate the power. You can also exert the power in multiple cases.
- For a big corporation, centralization ensures that its data remains safe. This is needed so that their trade secrets do not get leaked. However, there is a modified way of handling the data with the option to use decentralized networks such as Blockchain.
- We can easily say that centralization is still very prevalent in the current market. And, not all businesses don't need to adopt decentralization just for the sake of it. Different business models thrive in a centralized network and it will take a while before more and more business move towards decentralized models.

What is Decentralization? And How Does it Work?

- Now that we have a complete understanding of centralization, it would be easy for us to understand and learn about decentralization.
- The idea of decentralization is new. It came to light with the release of Bitcoin in 2009. It also introduced one new cool concept that makes decentralization possible, i.e., Blockchain Technology. Here, if one user sends Bitcoin to another user, it doesn't have to go through a centralized authority.
- However, this doesn't mean that the transaction is not verified. The transactions are verified with the use of consensus algorithms.
- The network used by Bitcoin is connectable by anyone.
- That means it is open. It also exhibited other key features such as transparency, where anyone can verify the transactions if needed. In such a network, a person or machine that connects to the network is termed as "node." In the end, there will be a network with thousands of nodes that are capable of sending and receiving funds from each other.

- Let's take a real-world example to understand the concept.
- A decentralized energy network is where people can connect and buy energy from other independent entries. This way, they do not have to pay the intermediaries for accessing energy in the first place.
- The distributed energy network relies on Blockchain technology with no need for a centralized authority. The nodes that are generating the energy can share it with the network and get paid for it.

Advantages of Decentralization

There are multiple advantages of decentralization.

1. Full Control

- One of the most significant advantages of decentralization is that the users are in full control of their transactions.
- This means that they can start a transaction when they want without the need to authorize it from a centralized authority. In simple terms that the verification process is not dependent on third-parties and a decentralized network utilizes consensus methods to verify the information.

2. Data Cannot be Altered or Deleted

- Blockchain technology's data structure is append-only. This means that there is no chance for anyone to modify or alter the data once it is stored. There is another Blockchain Technology that utilizes different data models such as Corda, but they also follow the immutability property.

3. Secure

- Decentralized networks are secure because of how they handle data and transactions. They use cryptography to ensure that the data ledgers are secure. Also, the data in the current block require data from the adjacent block so that it can use cryptography to validate the data.

4. Censorship

- Decentralization also means less censorship. In a centralized system, there are more chances that information can be censored. However, the decentralized network is less prone to censorship, as there is no central authority that controls the data. Let's take an example to understand the scenario.
- Twitter, for example, is known to censor accounts as finds some offensive posts or does it when t government tries to censor accounts if it goes again their agenda.
- In the case of decentralization, peers can intera directly and hence there is no or less censorship.

5. Open Development

- Decentralized networks mostly support op development. This is because of its nature and how operates. By having an open developme environment, the network gets amazing services, too and products built on top of it.
- Linux, for example, is open-source and has ecosystem that enables anyone to improve on it. Th same is true for decentralized networks. In compariso a centralized network or closed solutions do not g the chance to have open development. This limi development to a great extent.

Disadvantages of Decentralization

- There are of course many disadvantages decentralization. Some of the disadvantages includ the following:
  - **(i) Conflict:** Decentralization can lead to conflict if it not well maintained in an organizational structure.
  - **(ii) Cost:** In an organizational setting, decentralizatio can cost more than centralization as it require setting up of systems that can mak communication more automatic.
  - **(iii) Crime:** When it comes to decentralized Blockchain then the crime can be one big disadvantage. As everything is done on the network is anonymous and can lead to misuse.
  - **(iv) Volatility:** Decentralized cryptocurrency shows volatile behavior where the prices fluctuate a lot!

What is the Current State of Decentralization?

- Decentralization is here to stay. You'll see that many of the major companies, organizations and even governments are adopting it as it offers more efficiency to the network in the long run.
- Dubai is one of the first waves of governments that are currently adopting Blockchain to its whole governance structure. It is now termed as the Blockchain development world capital, as decentralization or Blockchain Technology is influencing it.

- At the time of writing, Dubai has been able to integrate Blockchain into eight industry sectors, including real estate, tourism, security, transportation, finance, health and education. The end result is to become the world's first Blockchain City.
- IBM is also at the forefront of embracing Blockchain technology and using it to improve the food supply chain.
- They created IBM Food Trust, which is all about bringing efficiency and transparency to food supply chains. They are working in conjunction with Walmart and benefit all the participants in the network with actionable and traceable information.
- There are also various decentralized ledger projects out there including the likes of Hyperledger, Corda and others.

Use-Cases: Centralized vs. Decentralized

- In this article, we will go through some of the use-cases that are related to centralized and decentralized. All these use-cases will help you better understand how each of these concepts differentiates and how decentralization can really help to solve some of the key core problems of centralized systems.

1. Payments System

- One of the most obvious use-cases of decentralization is the payment system. After all, the concept itself arose with the introduction of Bitcoin, the first event decentralized currency.
- All the currencies in the world that are operated by banks work on top of centralized servers. By doing so, they have full control over all the operations and also know about all your entire financial activities.
- This means that they know about your spending habits. However, one of the worst things about using a centralized currency is that if someone gets hold of your bank credentials, they can easily access all your money and use it for their own benefit.
- Another disadvantage of centralized payment systems is that there can be a disruption or failure and you will not be able to access your funds when you need it.
- So, how does a decentralized system solve all of these? Well, by being decentralized. As there is no central authority or point of failure, your funds are always available.
- It also removes the chance of your funds getting hacked or accessed by a malicious actor. So, if you use Cryptocurrency as a way to receive and send payments, you take out the role of the centralized entity from the process improving it in all the way. You can term these cryptocurrencies as peer-to-peer digital currencies.
- Another benefit of the payment system is the removal of intermediate fees. The only fees that are associated with the process are either small or non-existent. They are also borderless and secure.
- So, what are the pros of using a global payment system? They are as below:
  - ➢ Quick transactions
  - ➢ Cheap transactions
  - ➢ No information is shared among the third party
  - ➢ Secure
  - ➢ No single point of failure
  - ➢ Transparent

2. Government Voting

- Voting has always been a controversial topic among the government and the people who choose the government. The opposing parties are also keen to use the topic to find a way to defend themselves. So, what actually happens?
- The whole voting scenario is dealing with one most important issue, transparency. The current way of carrying out the vote doesn't take transparency into account. This results in a lot of conspiracy theories on how the votes are manipulated internally. As these theories exist, there is no way to validate them as the system is not transparent.
- That's where a decentralized voting platform can come into rescue. Governments can use it to run the votes and provide transparent voting. This way, they can rest all the theories that come out when general election results are declared.
- By using a transparent voting system or a voting system running on a decentralized network, the voters can easily verify the votes. This also means that no party can do frauds when it comes to counting of votes. Another benefit of using this approach is that results can be declared as soon as voting is finished.

- So, what are the benefits of a decentralized voting system?
  - ➢ There won't be any manipulation or fraud
  - ➢ No conspiracy theories
  - ➢ No threats

3. **Energy**

- Another useful use-case that we are going to discuss in our Decentralized vs Centralized comparison concept.
- Right now, centralized entities mainly control and distribute the energy who decide where they want to provide their services and at what price.
- To solve this, decentralization can come up with a unique solution. It can use a decentralized power grid which you can use to cut the middleman.
- It also provides equal opportunity to everyone who wants to get energy or generate energy and then sell it to others.
- The pros are of course there including
  - ➢ Fair market
  - ➢ No third party involvement
  - ➢ The decentralized payment system can work with decentralized energy platforms.

2.3 LAYERS OF BLOCKCHAIN

Understanding the Layers of the Blockchain

- If you have looked into cryptocurrencies or Blockchain in any way, you have probably come across terms like layer one and layer two protocols. Are you curious about what these layers are and why they exist? Let's discuss Blockchain layer architecture in this article.
- Blockchain technology is a one-of-a-kind mix of several current technologies: Cryptography, game theory and so on, with a wide range of possible applications such as cryptocurrencies. Encoding and decoding data is a mathematical and computational discipline known as cryptography. The study of the mathematical models of strategic interaction among rational decision-makers is known as game theory. Blockchain eliminates intermediaries, lowers costs and improves efficiency by bringing transparency and security.
- Without the oversight of a central authority, Distributed Ledger Technology (DLT) keeps information verified by cryptography among a group of users who agreed through a predetermined network protocol. Combining these technologies fosters trust between people or parties who would otherwise have no motive to do so. They make it possible for Blockchain networks to exchange value and data between users securely.
- Due to the lack of a centralized authority, Blockchains must be very safe. They must also be extremely scalable to handle increasing users, transactions and other data. Layers were born out of the requirement for scalability concurrent to the preservation of top-notch security.

What is Blockchain Scalability?

- The phrase "scaling" in Blockchain Technology refers to an increase in the system throughput rate, which is measured in transactions per second. With the widespread adoption of cryptocurrencies in everyday life, Blockchain layers are now required to improve network security, recordkeeping and other functions.
- The number of transactions handled by a system per second is referred to as "throughput." While Visa's VisaNet electronic payment network can process over 20,000 transactions per second, Bitcoin's (BTC) mainchain cannot handle more than seven transactions per second.
- The Blockchain is the first layer in a decentralized ecosystem. Layer two is a third-party integration used in conjunction with layer one to enhance the number of nodes and as a result, system throughput. Many layer two Blockchain technologies are currently being implemented. Smart contracts are used in these solutions to automate transactions.
- Blockchain developers are attempting to broaden the scope of Blockchain management as Bitcoin becomes a more significant force in the commercial world. They hope to reduce processing times and increase TPS by developing Blockchain layers and optimizing layer two scalability.

The Blockchain Trilemma

- The Blockchain trilemma refers to the commonly held notion that, in terms of decentralization, security and scalability, decentralized networks can only provide two of the three benefits at any given time.
- Computer scientists devised the consistency, availability and partition tolerance (CAP) theorem in the 1980s to express possibly the most significant of these difficulties. The CAP theorem states that decentralized data storage, such as Blockchain, can only satisfy two of the three guarantees mentioned above simultaneously.

- This theorem has evolved into the Blockchain trilemma in the context of the current distributed networks. The widely held notion is that public Blockchain infrastructure must sacrifice security, decentralization or scalability.
- As a result, the holy grail of Blockchain Technology is to create a network with impenetrable security over a broadly decentralized network while also handling internet-scale transactional throughput.
- Before delving into the trilemma's dynamics, let's define scalability, security and decentralization in general terms:
  - ➢ The Blockchain's scalability refers to its ability to handle a higher volume of transactions.
  - ➢ Security refers to the ability to secure data on the Blockchain from various types of assaults and the Blockchain's defense against double-spending.
  - ➢ Decentralization is a type of network redundancy that ensures that the network is not controlled by fewer entities.

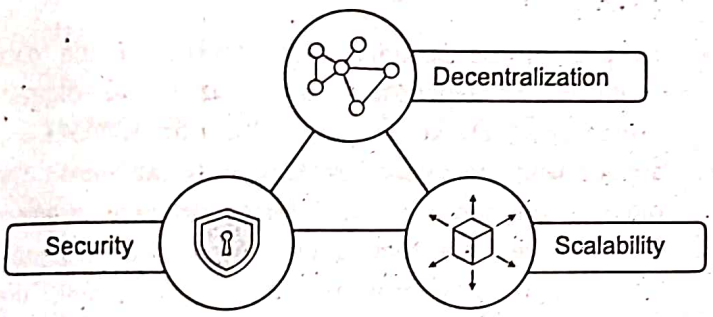

Fig. 2.2: The Blockchain trilemma

The Interplay Among Scalability, Security and Decentralization

- To settle a transaction, the network must first agree on its validity. The agreement may take some time if the system has a large number of members. As a result, we can show that scalability is inversely proportional to decentralization when security parameters are identical.

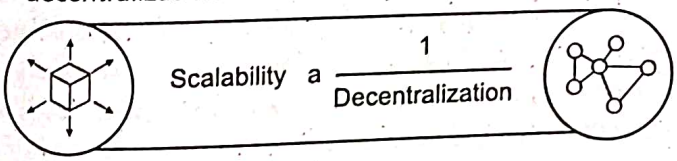

Fig. 2.3: Scalability vs. decentralization

- Now, assuming that two proof-of-work Blockchains have the same degree of decentralization and consider security to be the Blockchain's hash rate. The confirmation time decreases as the hash rate rises and scalability rises as security improves. As a result, scalability and security are proportionate with constant decentralization.

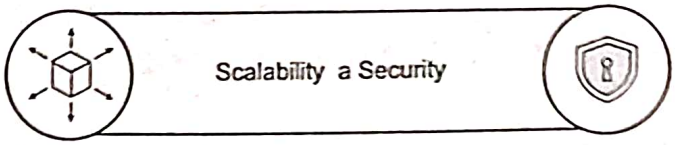

Fig. 2.4: Scalability vs. security

- As a result, a Blockchain cannot optimize for all three desired features simultaneously, forcing it to make trade-offs. Ethereum is the most recent example of the trilemma in action. The Ethereum platform has seen a boom in usage due to the growth of Decentralized Finance (DeFi) applications this summer. Ethereum can only grow to a certain point.
- Due to the increased demand, transaction fees have risen to the point where some people cannot engage with the Blockchain. Increased Ethereum fees are an example of the trilemma, as we can see that Ethereum did not scale without sacrificing security or decentralization.
- The focus of Ethereum was on decentralization and security, with the number of transactions per second being limited (scalability). To encourage miners to prioritize their transactions, users paid higher fees. Similarly, decentralization and security have taken precedence over scalability in Bitcoin.
- It's no secret that the scalability of Blockchains like Bitcoin and Ethereum is currently limited. Therefore, a global community of start-ups, corporations and technologists is working frantically on layer one and layer two solutions to solve the Blockchain trilemma.
- Layer one Blockchain networks are designed for speed, security and expansion. Layer two refers to technology enhancements and products that can be utilized to expand the scalability of existing Blockchain networks. Getting the perfect balance between the two layers might be a game-changer for Blockchain adoption and the expansion of decentralized networks.
- Developers are approaching the issue from a variety of perspectives. The increased block size in Bitcoin Cash (BCH) was an attempt to improve Bitcoin's scalability. However, there is no evidence that it is becoming more popular.
- Bitcoin is seeking to tackle the problem by adding a layer to the existing Blockchain layer. The layer two solutions will bundle numerous transactions together and only query the base layer Blockchain once in a

while, according to the idea behind scaling solutions. Ethereum is taking a hybrid approach, with sharding scaling the base layer Blockchain and the community anticipating several layer two solutions to boost throughput even further.

The Layered Structure of the Blockchain Architecture

- In the case of Blockchain architecture's distributed network, each network participant maintains, authorizes and updates new entries. A collection of blocks with transactions in a specific order represents the structure of Blockchain Technology. These lists can be saved as a flat file (in .txt format) or a simple database. Blockchain architecture can take public, private or consortium forms.
- The layered architecture of Blockchain is categorized into six layers.

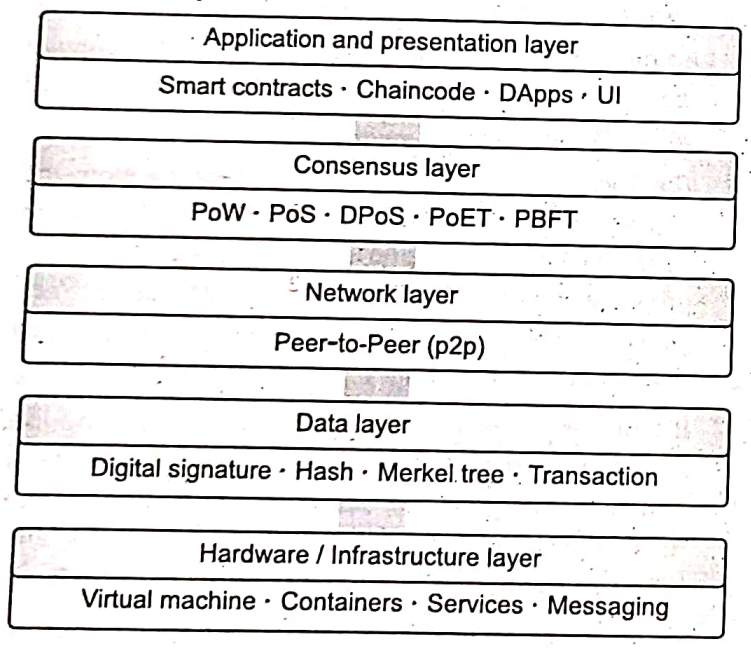

Fig. 2.5: Layered structure of the Blockchain architecture

Hardware or Infrastructure Layer

- The Blockchain's content is stored on a server in a data center somewhere on this lovely globe. Clients request content or data from application servers while browsing the web or utilizing any apps, which is known as the client-server architecture.
- Clients can now connect with peer clients and share data. A peer-to-peer (P2P) network is a large group of computers that share data. Blockchain is a peer-to-peer network of computers that computes, validates and records transactions in an orderly manner in a shared ledger. As a result, a distributed database is created, storing all data, transactions and other pertinent data. A node is a computer in a P2P network.

Data Layer

- A Blockchain's data structure is expressed as a linked list of blocks in which transactions are ordered. The data structure of the Blockchain consists of two fundamental elements: pointers and a linked list. A linked list is a list of chained blocks with data and pointers to the previous block.
- Pointers are variables that refer to the position of another variable and a linked list is a list of chained blocks with data and pointers to the previous block. The Merkle tree is a binary tree of hashes. Each block contains the root hash of the Merkle tree and information like the preceding block's hash, timestamp, nonce, block version number and current difficulty goal.
- For Blockchain systems, a Merkle tree provides security, integrity and irrefutability. The Blockchain system is built on Merkle trees, cryptography and consensus algorithms. Because it is the first in the chain, the genesis block, i.e., the first block, does not contain the pointer.
- To protect the security and integrity of the data contained in Blockchain, transactions are digitally signed. A private key is used to sign transactions and anyone with the public key may verify the signer. The digital signature detects information manipulation. Because the data that is encrypted is also signed, digital signatures ensure unity. As a result, any manipulation will render the signature invalid.
- The data cannot be discovered because it is encrypted. It cannot be tampered with again, even if it is caught. The sender's or owner's identity is also protected by a digital signature. As a result, a signature is legally linked to its owner and cannot be disregarded.

Network Layer or Propagation Layer

- The network layer, commonly referred to as the P2P layer, is responsible for inter-node communication. Discovery, transactions and block propagation are all handled by the network layer. Propagation layer is another name for this layer.
- This P2P layer ensures that nodes can find one other and interact, disseminate and synchronize to keep the Blockchain network in a legitimate state. A P2P network is a computer network in which nodes are distributed and share the workload of the network to achieve a common purpose. The Blockchain's transactions are carried out by nodes.

Consensus Layer

- The consensus layer is essential for Blockchain platforms to exist. The consensus layer is the most necessary and critical layer in any Blockchain, whether it is Ethereum, Hyperledger or another. The consensus layer is in charge of validating the blocks, ordering them and guaranteeing that everyone agrees.

Essential Elements of the Consensus Layer

- The consensus layer establishes **a clear set of agreements** among nodes in a distributed **P2P** network.
- The consensus layer ensures that **power stays decentralized and diffused.** As a result, no single party has complete control over the Blockchain network.
- The consensus layer ensures that **only one chain is followed** and that it contains the truth.
- The consensus layer consists of the **rules to which nodes adhere** so that transitions are validated and blocks are established in a manner consistent with those rules.
- The consensus layer achieves **unanimity of truth acceptance** among the participating nodes.
- In a **P2P** network, the consensus protocol aids in achieving **reliability.**

Application Layer

- Smart contracts, chaincode and decentralized applications (DApps) make up the application layer. The application layer protocols are further subdivided into the application and the execution layers. The application layer comprises the programs that end-users utilize to communicate with the Blockchain network. Scripts, application programming interfaces (APIs), user interfaces and frameworks are all part of it.
- The Blockchain network serves as the back-end technology for these applications and they communicate with it via APIs. Smart contracts, underlying rules and chaincode are all part of the execution layer.
- Although a transaction moves from the application layer to the execution layer, it is validated and executed at the semantic layer. Applications give instructions to the execution layer, which executes transactions and ensures the Blockchain's deterministic nature.

Blockchain Layers Explained

Layer Zero

- Blockchain layer zero is made up of components that help to make Blockchain a reality. It's the technology that allows Bitcoin, Ethereum and other Blockchain networks to function. Layer zero components include the internet, hardware and connections that will enable layer one to run smoothly.

Layer One

- This is the foundation layer and its security is based on its immutability. The Ethereum network or layer one, is what people allude to when they say Ethereum. This layer is in charge of consensus processes, programming languages, block time, dispute resolution and the rules and parameters that maintain a Blockchain network's basic functionality. It is also known as the implementation layer. Bitcoin is an example of a layer one Blockchain.

Problems with Layer One

- These scaling solutions boost the network's throughput when used together. However, with the growing number of Blockchain users, layer one appears to be falling short. The archaic and clumsy proof-of-work consensus process is still in use on the layer one Blockchain.
- While this approach is more secure than others, it is limited by its speed. Miners are required to solve cryptographic algorithms using computational power. As a result, more computational power and time are required in the long run. Also, the workload on layer one Blockchain has increased as the number of users has grown. Processing speeds and capacities have slowed as a result.

Possible Solutions

- Proof-of-stake is an alternate consensus that Ethereum 2.0 will adopt. This consensus approach certifies new transaction data blocks based on the staking collateral of network participants, resulting in a more efficient procedure.
- Sharding is a scaling solution for the burden on the layer one Blockchain problem. Simply said, sharding divides the task of validating and authenticating transactions into smaller, easier-to-manage chunks. As a result, the workload can be distributed over the network to use more nodes' computing capability. Because the network processes these shards in parallel, several transactions can be processed both sequentially and simultaneously.

Layer Two

- The overlapping networks that sit on top of the base layer are known as L2 solutions. Protocols make use of layer two to increase scalability by removing some interactions from the base layer. As a result, smart contracts on the primary Blockchain protocol only deal with deposits and withdrawals and ensure that off-chain transactions follow the regulations. Bitcoin's Lightning Network is an example of a layer two Blockchain.
- So, what is the difference between layer one and layer two Blockchain? The Blockchain is the first layer in a decentralized ecosystem. Layer two is a third-party integration used in conjunction with layer one to enhance the number of nodes and as a result, system throughput. Many layer two Blockchain Technologies are being implemented at present.

Layer Two Scaling Solutions

- Layer two protocols have exploded in popularity in recent years and they're proving to be the most effective approach to solving scaling issues in PoW networks, in particular. Various layer two scaling solutions are explained in the sections below.

Nested Blockchain

- A nested layer two Blockchain runs on top of another. In essence, layer one establishes the settings, whereas layer two conducts the procedures. On a single mainchain, there might be several Blockchain tiers. Consider it a typical business structure.
- Rather than having one person (e.g., the manager) conduct all of the work, the manager delegated tasks to subordinates, who then reported back to the management when they were finished. As a result, the manager's workload is reduced while scalability is improved. The OMG Plasma Project, for example, works as a level two Blockchain for Ethereum's level one protocol, allowing for cheaper and faster transactions.

State Channels

- A state channel improves total transaction capacity and speed by facilitating two-way communication between a Blockchain and off-chain transactional channels via various approaches. To validate a transaction over a state channel, the miner does not need to be involved right away.
- Instead, it's a network-adjacent resource that's protected via a multi-signature or smart contract mechanism. The ultimate "state" of the "channel" and all its inherent transitions are posted to the underlying Blockchain when a transaction or batch of transactions is completed on a state channel.
- State channels examples include Bitcoin Lightning and Ethereum's Raiden Network. In the trilemmatradeoff, state channels give up some decentralization in exchange for increased scalability.

Sidechains

- A sidechain is a transactional chain that runs alongside the Blockchain and is used for massive bulk transactions. Sidechains have their consensus method, which can be adjusted for speed and scalability and a utility token is frequently utilized as a part of the data transfer mechanism between side and mainchains. The mainchain's principal function is to provide general security and dispute resolution.
- In several important ways, sidechains differ from state channels. To begin with, sidechain transactions are not private between participants; instead, they are published openly on the ledger. Furthermore, security breaches on sidechains do not affect the mainchain or other sidechains. Building a sidechain from the ground up necessitates a significant amount of time and work.

Rollups

- Rollups are layer two Blockchain scaling solutions that perform transactions outside of the layer one network and then upload the data from the transactions to the layer two Blockchain. Layer one can keep rollups secure because the data is on the base layer.

Table 2.1: Two Alternative Security Models for Rollups

Optimistic Rollups	Rollups with Zero-Knowledge
These are based on the assumption that transactions are legitimate by default. As a result, they only computer to detect fraud when there is a difficulty.	These rollups perform computations off-chain. The validity proof is then submitted to the base layer or mainchain.

- Users benefit from rollups since they help to boost transaction throughput, open participation and lower gas costs.

Layer Three

- The application layer is often referred to as layer three or L3. The L3 projects act as a user interface while masking the technical aspects of the communication channel. L3 applications are what give Blockchains their real-world applicability, as explained in the layered structure of the Blockchain architecture.

2.4 IMPORTANCE OF BLOCKCHAIN

- The rapid progress of Blockchain technology is showing no signs of slowing down. In the past few decades, many things that seemed impossible have turned out to be false, such as high transaction fees, double spending, net fraud, retrieving lost data, etc. But, now all this can be avoided with the help of Blockchain Technology.
- Blockchain started in 1991 as a way to store and secure digital data. Blockchain is an open ledger that several parties can access at once. One of its primary benefits is that the recorded information is hard to change without an agreement from all parties involved. IBM explained that each new record becomes a block with a unique, identifying hash. Linking the blocks into a chain of records forms a Blockchain. Bitcoin Cryptocurrency uses Blockchain Technology.
- Blockchain helps in the verification and traceability of multistep transactions needing verification and traceability. It can provide secure transactions, reduce compliance costs and speed up data transfer processing. Blockchain technology can help contract management and audit the origin of a product. It also can be used in voting platforms and managing titles and deeds.

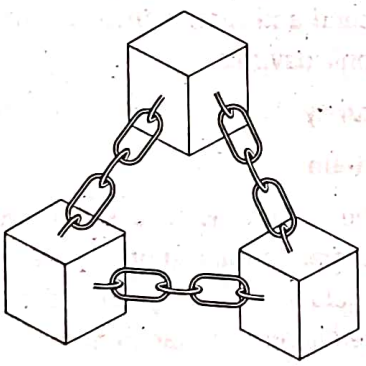

Fig. 2.6

Note: The data is recorded in chronological order. Also, once the data is recorded, it cannot be changed.

What Are the Benefits of Blockchain Technology?

- Here's a list of key benefits you can expect to achieve when adopting Blockchain technology into your business:
  - ➢ It is an immutable public digital ledger, which means when a transaction is recorded, it cannot be modified.
  - ➢ Due to the encryption feature, Blockchain is always secure.
  - ➢ The transactions are done instantly and transparently, as the ledger is updated automatically.
  - ➢ As it is a decentralized system, no intermediary fee is required.
  - ➢ The authenticity of a transaction is verified and confirmed by participants.

Building Trust in Government

- In specific applications, Blockchain could reduce government redundancy, streamline processes, decrease audit burden, increase security and ensure data integrity. One process ripe for streamlining is GSA's FASTLane process, which manages incoming proposals from vendors. Booz Allen Hamilton wrote it currently takes 40 days to process incoming submissions. However, GSA hopes that a Blockchain solution will help process them in 10 days.

Reducing Government Corruption

- While Blockchain won't prevent crime, the World Economic Forum (WEF) wrote there are five use cases to address weaknesses in government systems.

1. Public Procurement / Government Contracting

- WEF wrote that government contracting is the largest area of government spending with the greatest potential for corruption worldwide. A Blockchain-based process can facilitate third-party oversight of transactions and provide greater objectivity and uniformity through automated contracts. There also would be more transparency and accountability of transactions and participants. However, its implementation could be hindered by how it's deployed. WEF wrote that the easier it is to access and use the Blockchain platform, the more vulnerable it is to abuse. Further, if offline transactions continue outside of the Blockchain platform, its anti-corruption potential will be limited.

2. Land Title Registries

- As mentioned earlier, Blockchain is a way for some countries to increase efficiency in land title registries. WEF wrote that Honduras and India are working on using Blockchain to expand property rights and enhance transparency in a process known to have corrupt practices. Blockchain-based land registries could provide a secure, decentralized, publicly verifiable and immutable record system where people could prove their land rights. A limitation would be that countries without land registries would have to

build and digitize the information before Blockchain could be used.

3. Electronic Voting

- Governments are considering Blockchain-based voting platforms due to concerns about election security, voter registration integrity, poll accessibility and voter turnout. Blockchain's information security qualities could help address election tampering and increase poll accessibility. WEF said a limitation would be Blockchain's vulnerability to cyber attacks and other security issues.

4. Beneficial Corporate Ownership Registries

- According to WEF, secretly operated companies present avenues for money laundering, influence peddling and steering government investments. Blockchain can develop central registries to help track conflicts of interest and criminal activity. It also could provide transparency and disclosure. However, there are several limitations as most countries don't require companies to maintain beneficial ownership information themselves. Also, a Blockchain-based registry would require buy-in from politicians, lawyers, banks and big business, which may be a heavy lift in some locations.

5. Grant Disbursements

- Because of the millions of dollars granted to various institutions, the opaque donation process is ripe for inefficiency and corruption. Blockchain could reduce the number of actors and managers, could streamline the process and improve verification. WEF said a limitation would be among the less technologically savvy who might be excluded from grant disbursement processes. In addition, it would not address how recipients spend grant money.

How will Blockchain Disrupt Industries?

- Several industries like Unilever, Walmart, Visa, etc. use Blockchain Technology and have gained benefits in transparency, security and traceability. Considering the benefits Blockchain offers, it will revolutionize and redefine many sectors.
- Here, are the top five prominent industries that will be disrupted by Blockchain Technology in the near future:

1. Banking
2. Cyber Security
3. Supply Chain Management
4. Healthcare
5. Government

1. Banking

Before Blockchain

- Banking has transfer fees, which can be both expensiv and time-consuming for people. Also, sending mone overseas becomes even more difficult due to th exchange rate and other hidden costs.

After Blockchain

- Blockchain eliminates the need for a middleman Blockchain is disrupting the banking system b providing a peer-to-peer payment system with th highest security and low fees.
  - ➢ Blockchain technology provides instant and borderless payments across the globe
  - ➢ Cryptocurrencies (like Ethereum, Bitcoin) remove the requirement for a third party to perform transactions.
  - ➢ Blockchain records all the transactions in a public ledger which is globally accessible by Bitcoin users.

Let's consider an example of Abra

- ➢ Abra is a financial Cryptocurrency application which helps in performing peer-to-peer money transfers.
- ➢ With this application, Cryptocurrency users can save, send and receive their digital money on their electronic devices.

2. Cyber Security

Before Blockchain

- Earlier, cyber attacks were a significant threat to the public. Several organizations were developing an effective solution to secure the data against unauthorized access and tampering.

After Blockchain

- Blockchain quickly identifies malicious attack due to the peer-to-peer connections where data cannot be tampered with.
- Every single piece of data stored on the Blockchain network is verified and encrypted using a cryptographic algorithm.
- By eliminating the centralized system, Blockchain provides a transparent and secure way of recording transactions (without disclosing your private information to anyone).

For example, a software security company called Guardtime offers Blockchain-based products and services.

- Rather than following the centralized system, the company utilizes Blockchain Technology and distributes data to its nodes.

3. Supply Chain Management

Before Blockchain

- Due to the lack of transparency, supply chain management often had its challenges like service redundancy, lack of coordination between various departments and lack of reliability.

After Blockchain

- Tracking of a product can be done with Blockchain Technology, by facilitating traceability across the entire Supply chain.
- Blockchain gives the facility to verify and audit transactions by multiple supply chain partners involved in the supply chain management system.
  - ➢ Blockchain records transaction (history, timestamp, date, etc.) of a product in a decentralized distributed ledger.
  - ➢ Each transaction is recorded into a block.
  - ➢ With Blockchain, anyone can verify the authenticity or status of a product being delivered.
- Let's consider an example of the Pacific Tuna project.
- Here, Blockchain supply chain management provides a step-by-step verification process to track tuna fish. The process results in preventing illegal fishing.

4. Healthcare

Before Blockchain

- In the healthcare system, patients can connect to other hospitals and collect their medical data immediately. Apart from the delay, there are high data corruption chances since the information is stored in a physical memory system.

After Blockchain

- Blockchain removes a central authority, which results in instant access to data.
- Here, each block is linked to another block and distributed across the computer node. This becomes difficult for a hacker to corrupt the data.

For example: United Healthcare is an American healthcare company that has enhanced its privacy, security and medical records' interoperability using Blockchain.

5. Government

Before Blockchain

- Rigged votes is an illegal activity that occurs during most traditional voting systems. Also, citizens who want to vote to wait a little longer in a queue and cast their votes to a local authority, which is a very time-consuming process.

After Blockchain

- Voters are allowed to vote without the need of disclosing their identity in public.
- The votes are counted with high accuracy by the officials knowing that each ID can be attributed to just one vote.
- As soon, the vote is added to the public ledger, the information can never be erased.

Consider an example of MiVote

- MiVote is a token-based Blockchain platform that is similar to a digital ballot box.
- Using MiVote, through a smartphone, voters can cast their votes, where the records are stored in the Blockchain securely.
- Moving forward, let's understand the fundamentals of Blockchain.

Fundamentals of Blockchain

1. Public Distributed Ledgers

- A Blockchain is a decentralized public distributed ledger that is used to record transactions across many computers.
- A distributed ledger is a database that is shared among the users of the Blockchain network.
- The transactions are accessed and verified by users associated with the Bitcoin network, thereby making it less prone to cyberattack.

2. Encryption

- Blockchain eliminates unauthorized access by using the cryptographic algorithm (SHA256) to ensure the blocks are kept secure.
- Each user in the Blockchain has their key.

3. Proof of Work

- Proof of Work (PoW) is a method to validate transactions in a Blockchain network by solving a complex mathematical puzzle called mining.

Note: Users trying to solve the puzzle are called miners.

4. Mining

- In Blockchain, when miners use their resources (time, money, electricity, etc.) to validate a new transaction and record them on the public ledger, they are given a reward.

2.5 LIMITATIONS OF CENTRALIZED SYSTEMS

- Centralization refers to the process in which activities involving planning and decision-making within an organization are concentrated to a specific leader or location. In a centralized organization, the decision-making powers are retained in the head office and all other offices receive commands from the main office. The executives and specialists who make critical decisions are based in the head office.

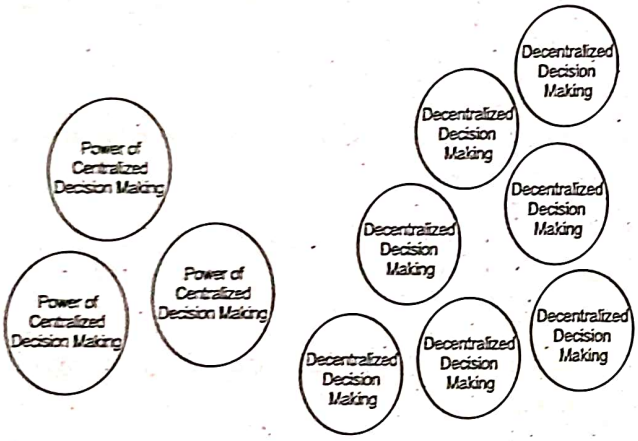

Fig. 2.7

- Similarly, in a centralized government structure, the decision-making authority is concentrated at the top and all other lower levels follow the directions coming from the top of the organization structure.

Limitations

1. Bureaucratic Leadership

- Centralized management resembles a dictatorial form of leadership where employees are only expected to deliver results according to what the top executives assign them. Employees are unable to contribute to the decision-making process of the organization and they are merely implementers of decisions made at a higher level.
- When the employees face difficulties in implementing some of the decisions, the executives will not understand because they are only decision-makers and not implementers of the decisions. The result of such actions is a decline in performance because the employees lack the motivation to implement decisions taken by top-level managers without the input of lower-level employees.

2. Remote Control

- The organization's executives are under tremendous pressure to formulate decisions for the organization and they lack control over the implementation process. The failure of executives to decentralize the decision-making process adds a lot of work to their desks.
- The executives suffer from a lack of time to supervise the implementation of the decisions. This leads to reluctance on the part of employees. Therefore, the executives may end up making too many decisions that are either poorly implemented or ignored by the employees.

3. Delays in Work

- Centralization results delays in work as records are sent to and from the head office. Employees rely on the information communicated to them from the top and there will be a loss in man-hours if there are delays in relaying the records. This means that the employees will be less productive if they need to wait long periods to get guidance on their next projects.

4. Lack of Employee Loyalty

- Employees become loyal to an organization when they are allowed personal initiatives in the work they do. They can introduce their creativity and suggest ways of performing certain tasks. However, in centralization, there is no initiative in work because employees perform tasks conceptualized by top executives. This limits their creativity and loyalty to the organization due to the rigidity of the work.

2.6 BLOCKCHAIN ADOPTION

- The adoption of Blockchain is rapidly increasing in various sectors across India and the world at large. India is touted to become a $5 trillion economy by 2024-25 and Blockchain has the potential to play an integral role towards its growth. It is estimated that government-related Blockchain projects could add $5.1 billion to India's GDP in 2032. Blockchain provides business efficiencies when deployed in daily business processes as the nature of technology is such that it removes intermediaries and creates a decentralized database that can be accessed by the relevant stakeholders for decision-making.
- Large enterprises are exploring the adoption of Blockchain in India in their daily processes and many start-ups are experimenting with the technology to provide different use-cases, especially in banking,

insurance and financial services. The government of India is also actively adopting and channelising resources to leverage the technology for use-cases in farm insurance, education, land title registry and electronic health management, etc.

- Increased Blockchain adoption will help accelerate digitization in India. Over the past few years, the government has successfully created the foundation for digital infrastructure for recording and sharing data through the applications such as Aadhar, UPI, Digilocker and e-Sign along with digitally enabled tax governance networks such as the GSTN. With an already well-established groundwork for collecting data, ramping up efforts to merge Blockchain with these applications will help in the digitization process.
- Governance in India faces several challenges as we are the world's largest democracy and the world's second-largest populated country. Given the diversity and the complexity involved in managing the Public Distribution Services (PDS), Blockchain offers unique advantages and possibilities to help improve governance. Blockchain provides a way of tracking and managing the goods sent to the beneficiaries as every stage of the supply chain can be tracked on the Blockchain. The information is readily available to track in real-time on the Blockchain and ensures that there are no leakages within the PDS and that the final recipient receives the goods and services as allocated. Increased Blockchain adoption will directly provide benefits to the economy through better contract management and procurement, greater quality control and reduced leakages and wastage across the supply chains.
- Further adoption of Blockchain will support SMEs and allow the private sector to conduct business more efficiently. With the deployment of Blockchain, if the government allows 'self-regulation', the governance will drastically improve as entities can interact directly with each other on the distributed ledger through a trusted medium with reduced dependency on cumbersome regulatory oversight and compliance. Improved transparency and accountability will highly increase business efficiencies as the time and the costs to approve permissions and provide clearances will drastically reduce through embedded smart contracts, helping improve the 'Ease of Doing Business".

Blockchain is also beneficial in the agricultural sector of India by deploying the tech in National Agriculture Market (eNAM), which is an online trading platform for agricultural commodities in India. By recording the flow of information on the Blockchain, audit trails of all the farmer's produce are created and the data cannot be hampered as every record on the Blockchain is cryptographically hashed. This reduces the mistrust between farmers and arhatiyas (mandi intermediaries) and also reduces the transaction costs, increasing the trade of commodities across India. Moreover, Blockchain encourages farmers to produce high-quality goods as the incentive to earn a larger amount for their produce can be attached by providing certification of the provenance of organic produce that fetches a higher price in the export market.

- During a time of natural calamity, Blockchain can help in disaster management and insurance claims by automatically releasing claims in real-time by fetching the required data for claim management through smart contracts, saving the cost and money involved in the process. The education sector benefits through Blockchain as it allows easier verification of education certificates and record-keeping.
- Blockchain has the potential to impact social structures and economies and its invention can be compared to other revolutionary innovations such as electricity, steam engine, the computer and the internet. The benefits of increased adoption of Blockchain are unprecedented, however, several factors will play a major role in accelerating its growth and awareness and education about the technology should become a part of the education system.
- To reap complete benefits of the tech, it is integral that there is cross-collaboration between institutions, industry and academia with support from the government. Also, it is highly recommended that since the tech is decentralised, the government must work alongside other countries to achieve interoperability of data and processes on the Blockchain to ensure smooth application in payments systems, healthcare records, supply chain, etc.
- Blockchain provides immense employment opportunities for India especially as the tech requires software developers, business acumen and legal expertise. The application of Blockchain will also act as a catalyst to revamp the existing governance processes and achieve higher efficiency and transparency in the system.

CASE STUDY: STUDY OF RESEARCH PAPER BASED ON BLOCKCHAIN

- We are moving towards digitalization and the most common term which comes to everyone's mind while talking about the same is, "currency". To support this, we have 'Bitcoins'. Bitcoin is a type of digital currency that can be exchanged on the Blockchain, the shared ledger technology. Bitcoins are in essence, electricity converted into long strings of code that have money value. Bitcoin is a form of digital currency, created and held electronically. Blockchain is a shared ledger technology which is used to transfer Bitcoins. It is also finding its application in various other domains such as e-voting system, government, health care, etc. The security of transactions has become such a major concern these days. The Blockchain network comes with full-fledged security features and hence are being welcomed everywhere. With security other special characteristics of Blockchain have also been briefed in our work. It is known to us very well that any invention has to go through a lot of challenges; same is the case with Blockchains. The idea of Bitcoin was conceptualized by Satoshi Nakamoto, an anonymous figure. In May 2008, he shared a white paper about Bitcoin. He did not disclose who he was. He outlined how the currency would work.
- The first major Blockchain innovation was Bitcoin, a digital currency experiment.
- The second innovation was called Blockchain, which was made keeping in mind that the technology that operated the Bitcoin should be separated from the currency and used for all kinds of other inter organizational cooperation. Almost every major financial institution in the world is doing Blockchain research at the moment and 15% of banks are expected to be using Blockchain in 2017.
- The third innovation was called the "smart contract," embodied in a second-generation Blockchain system called Ethereum, which built little computer programs directly into Blockchain that allowed financial instruments, like loans or bonds, to be represented rather than only the cash-like tokens of the Bitcoin.
- The fourth major innovation, the current cutting edge of Blockchain thinking, is called "proof of stake." Current generation Blockchains are secured by "proof of work," in which the group with the largest total computing power makes the decisions. These groups are called "miners" and operate vast data centers to provide this security, in exchange for Cryptocurrency payments. The new systems do away with these data centers, replacing them with complex financial instruments, for a similar or even higher degree of security.
- The fifth major innovation on the horizon is called Blockchain scaling. A scaled Blockchain accelerates the process, without sacrificing security, by finding out how many computers are necessary to validate each transaction and dividing up the work efficiently. To manage this without compromising the legendary security and robustness of Blockchain is a difficult problem, but not an intractable one. A scaled Blockchain is expected to be fast enough to power the internet of things and go head-to-head with the major payment middlemen (VISA and SWIFT) of the banking world.
- Bitcoin is a type of digital currency that can be exchanged on the Blockchain, the shared ledger technology. Bitcoins are, in essence, electricity converted into long strings of code that have money value. Bitcoin is a form of digital currency, created and held electronically. No one controls it. Bitcoins aren't printed, like the normal currency in fact they're produced by people and increasingly businesses, running computers, using software that solves mathematical problems. Without having any physical existence Bitcoins are of very high value in terms of money and each the day value in physical currency of Bitcoin changes. It's most important characteristic and the thing that makes it different to conventional money, is that it is decentralized. No single institution controls the Bitcoin network. This gives many people relief because it means that a large bank can't control

their money. Bitcoins in many parts of the world have become a mode of payment for example in countries like Argentina it is used to pay for Uber. It is created as a reward for the process known as mining. Blockchains shift some control over daily interactions with technology away from central elites, redistributing it among users. In doing so, they make systems more transparent and more democratic. The governments and industry giants are investing heavily in Blockchain research and development to enhance their services.

- After understanding about Bitcoin the question comes in our mind, "how this digital currency is shared?" The answer to same is Blockchain. A shared ledger allows any participant in the business network to see the system of records. In layman language it is a technology that transfers Bitcoin. Blockchain technology was used by the global network of computers which used it to collectively manage the database that records Bitcoin transactions. That is why the Bitcoin is managed by its network and not any one by central authority.

Blockchain is also a shared ledger technology but the sharing is between all the people on network. Without the consent of all the people on the network changes cannot be made on the document. And the most critical area where we use the Blockchain is transactions as here the records of transactions is not stored between with one or two people but with the network as a whole.

The step to step explanation to the working of Blockchain is explained below :

- Let's start with the person who requests a transaction say it is A. Let A has to send some digital currency to B.
- The requested transaction is represented online as a block.
- A verified transaction can involve Cryptocurrency, contacts, records, or other information. Cryptocurrency: It is the currency that which has no physical form, it only has the network existence and it cannot be exchanged for any other item such as platinum. No central bank has control over this currency and also the network is completely decentralized.
- This block is now broadcast to every party in the network.
- Those in the party look for the validity of the transaction.
- Once verified, the block is then added to the chain which provides an incredible and transparent record of transaction. And which is also permanent and unalterable.
- The digital currency moves from A to B. Transaction is complete.

Applications of Blockchain

- **Network Operations:** The IBM Blockchain Platform enables founders to initiate, invite and configure a network with a simple user interface. Initiating a network creates three ordering peers and two certificate authorities. This provides a founder with a ready to use foundation for creating their business network. Founders can then invite additional participants to the network using any number of peers. Participants will receive email notifications of their invite so that they can easily join the network. The Network Operations user interface also enables a founder to configure core network components such as identity verification and channel creation. This helps to ensure that only permissioned users access the network and confidential transactions are enabled via channels.
- **Operational Monitoring:** Users require the ability to monitor the activity on a network as it grows in terms of transactions and participants. The IBM Blockchain Platform provides both a Network Traffic Dashboard and Network Health Monitor. These dashboards enable proactive adjustment to network operations and clearly define resource consumption within the network.
- **Blockchain States:** Rethinking about the public services in the context of opening up data, services and decisions in the public sector through digital media

and technologies, a new generation of open, transparent, collaborative and accountable eGovernment services are under development. Recently, a report has been published which outlines how Blockchain-based technologies could provide new tools to reduce fraud, avoid errors, boost productivity, cut operational costs, support compliance and force accountability in many public services. Potential applications of the same include tax collection, identity management, distribution of benefits, local (or national) digital currencies, property and land registry and any kind of government record. The same technology also opens the doors for the non-state actors to provide state-like services, from notary services to global citizenship and identity. Data used by public institutions is often internally fragmented and opaque to other actors, notably citizens, businesses and watchdogs. Blockchain technology could allow records to be created and verified with a greater level of speed, security and transparency. Record keeping is the most immediate application of the Blockchain Technology in public administrations. The combination of time-stamping with digital signatures on an accessible ledger is expected to deliver benefits for all users, enabling them to conduct transactions and create the records and store them.

- **Smart Contracts:** As compared to the traditional ledger the Blockchain ledgers surely present several interesting and novel features. It not just records the time and a detail of transactions but beyond that it also plays a more active and potentially autonomous role in the implementation and management of transactions. Blockchains also have the feature of automatic execution of transaction with response to certain conditions being met, providing a 'guarantee of execution'. Based upon this self-executing smart contract are being developed rapidly. Smart contracts can be defined as a 'computerized transaction protocol that executes the terms of a contract'. In simple terms it means that, the terms of an agreement between two or more parties are programmed into set of instructions or say code that are stored on Blockchain that are stored on the Blockchain. When certain conditions described in the code made are met, the required actions that are defined in the code are automatically executed.
- **E-voting System:** Even after this advancement in technology elections are conducted offline. This technology has given very promising results in the voting system as no one can alter the votes as well as it is cheap than conducting polls offline. It has been seen as a many means of increasing engagement and turnout and even reconnecting links between citizens and political institutions, claims that should be read with some skepticism, e-voting could be done in many ways: using the internet or a dedicated, isolated network; requiring voters to attend a polling station or allowing unsupervised voting; it can also be done using any gadgets that we use on everyday purpose like mobile phones, laptops etc. Now we still are in dilemma whether to continue trusting central authorities to manage elections or to use Blockchain Technology to distribute an open voting record amongst the citizens. The Blockchain is transparent and distributed among users which I can be used to logging and verifying. Usually, votes are recorded, managed, counted and checked manually. Blockchain-enabled e-voting (BEV) would empower voters to do these tasks themselves by allowing them to hold a copy of the voting record. The historic record cannot be changed, because other voters would see that the record differs from theirs. An illegitimate vote cannot be added, because other voters would be able to see that it is not compatible with the rules (perhaps because it was already counted or is not associated with a valid voter record). BEV would shift power and trust away from central actors, such as electoral authorities.

Challenges to Blockchain

- **Regulations:** We all are aware of the fact that when it comes about technology innovation the regulatory authority often lags. Day by day new products and services are coming up based on the Blockchain transactions but sadly we have no regulations on how transactions should be written. Transparency is the

most important feature of Blockchain but the highly regulated industries may need to develop new regs for Blockchain. Similarly, there are many special characteristics which may need to be altered based on various situations.

So for this we need properly regulations governing the Blockchain.

- **Standards:** As with regulations, we currently lack one common set of standards for writing transactions on a Blockchain. In fact, there are three open source consortium organizations, each with its own standards and code. Part of this evolution is complicated by the wide variety of usages for Blockchain and the most appropriate form standards will need to take in addressing these use cases. The regulations that evolve to regulate this environment will help drive the adoption of standards and may well drive these consortiums together.
- **Need More Validation:** Another obstacle to adoption is executives fear that the technology has not been tested enough in pilots and POCs. Ultimately, what are Blockchain's limitations? Early POCs validate its scalability, but what are its limitations for handling a large volume of enterprise transactions and data? Different applications will face different scalability issues as adoption increases. And how much time and computing power will be necessary to process a huge number of transactions?
- **Culture:** From ages we have a certain way or say tradition of doing transactions. The Blockchain Technology takes us away from the traditional way of doing things. It is a major shift from centralized network to the decentralized one and not all the institutions can accept the concept of decentralization. Blockchain is more of the business process change and less of the technology implementation.

Challenges to Implementation of Blockchain

- **Cost and Efficiency:** We have various types of Blockchain and each of them comes with different speeds and effectiveness with which the transactions can be done. Out of many types, those which give high amount of speed and effectiveness are quite costly. So in order to give the best of service to the people and also aid maximum benefits from the Blockchain Technology one has to go for the best Blockchain which is quite costly.
- **Security and Privacy:** The Bitcoin transactions are tied to the "wallets" instead of the individuals. Applications of the Blockchain require that the transactions and contracts should be linked to known identities. This raises a serious question about the privacy and security of the data that is stored and accessible on the Blockchain. Till now no one has every managed to break the architecture of a Blockchain. But still, it is not easy to get over the taught, "technology has its own advantages and disadvantages". This is the reason why some of the institutions are finding it difficult to shift to this technology.
- **Organization:** The Blockchain creates most value for organizations when they work together on areas of shared pain or shared opportunity, especially problems particular to each industry sector. The problem with many current approaches, though, is that they remain stove-piped: organizations are developing their own Blockchains and applications to run on top of them. In any one industry sector, many different chains are therefore being developed by many different organizations to many different standards. This defeats the purpose of distributed ledgers, fails to harness network effects and can be less efficient than current approaches.

EXERCISE

1. Describe the history and evolution of Blockchain Technology.
2. Differentiate between centralized and decentralized systems.
3. What are the advantages and disadvantages of centralized systems?
4. What are the advantages and disadvantages of decentralized systems?

5. Draw and explain the layered structure of the Blockchain architecture.
6. What are the essentials elements of the consensus layer?
7. Describe the importance of Blockchain Technology.
8. Explain the benefits of Blockchain adoption. Giv suitable use cases.

✠ ✠ ✠