Decentralization

UNIT-2

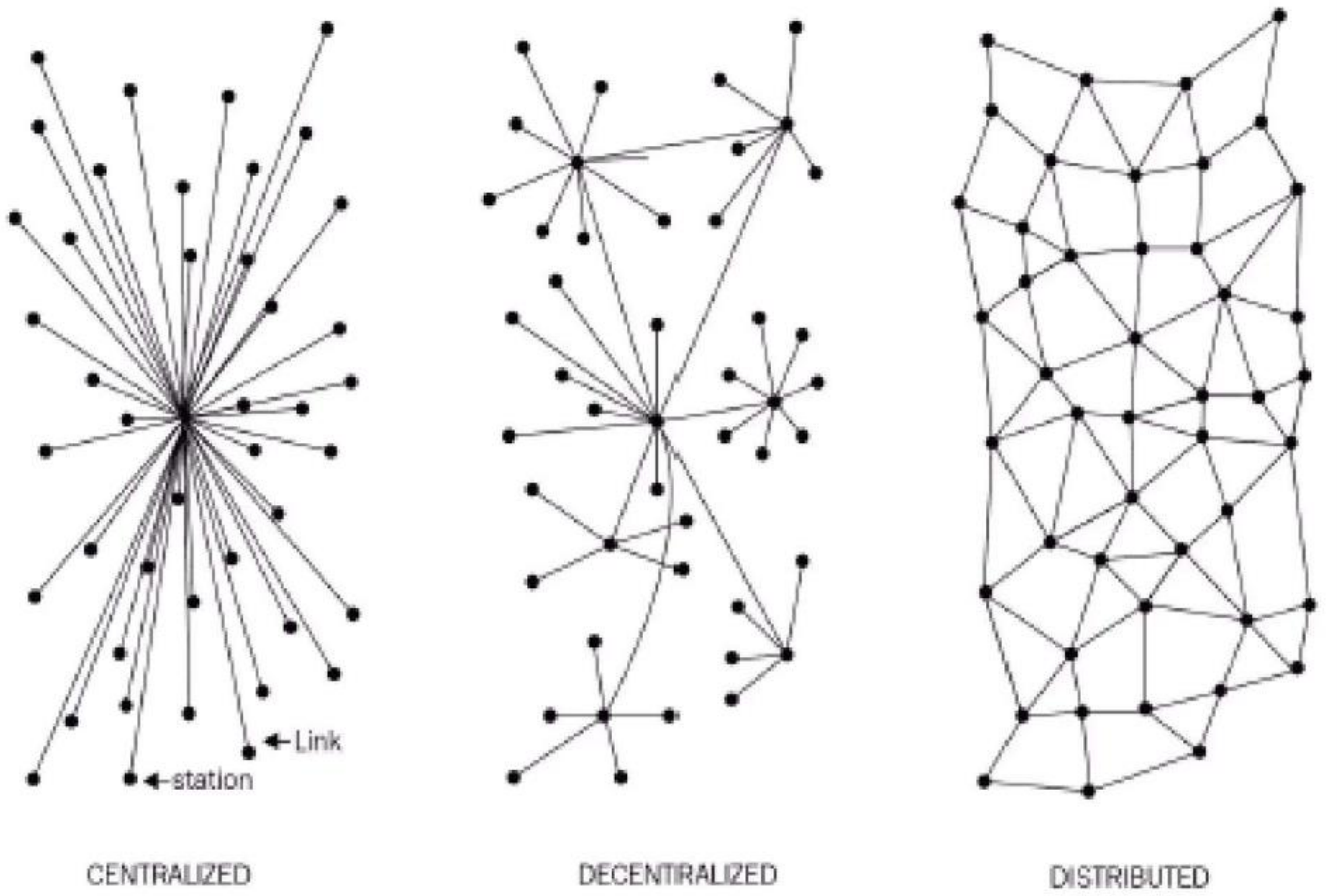
Decentralization

- **Decentralization** is not a new concept. It has been used in strategy, management, and the government, for a long time.
- The basic idea of decentralization is to distribute control and authority to the peripheries of an organization instead of one central body being in full control of the organization.
- This configuration produces several benefits for organizations, such as increased efficiency, expedited decision making, better motivation, and a reduced burden on top management.
- The fundamental basis of blockchain is that no single central authority is in control, and, here we present examples of various Methods of decentralization and Routes to achieve this.

Decentralization using Blockchain

- Decentralization is a core benefit and service provided by blockchain technology.
- By design, blockchain is a perfect vehicle for providing a platform that does not need any intermediaries and that can function with many different leaders chosen via consensus mechanisms.
- This model allows anyone to compete to become the decision making authority. This competition is governed by a consensus mechanism - Proof of Work (PoW).
- **Information and Communication Technology** (ICT) has conventionally been based on a centralized paradigm whereby database or application servers are under the control of a central authority, such as a system administrator.
- With Bitcoin and the advent of blockchain technology - which allows anyone to start a decentralized system and operate it with no single point of failure or single trusted authority.

- The following diagram shows the different types of systems that currently exist: central, decentralized, and distributed.



Different types of networks/systems

Centralized System

- Centralized systems are conventional (client-server) IT systems in which there is a single authority that controls the system, and who is solely in charge of all operations on the system.
- All users of a centralized system are dependent on a single source of service.
- The majority of online service providers including Google, Amazon, eBay, Apple's App Store, and others use this conventional model for delivering services.

Distributed system

- A Distributed system, data and computation are spread across multiple nodes in the network.
- Sometimes, this term is confused with *parallel computing.*
- The main difference between these systems is that in a parallel computing system, computation is performed by all nodes simultaneously in order to achieve the result.
- Example - weather research and forecasting, simulation and financial modeling.
- On the other hand, in a distributed system, computation may not happen in parallel and data is replicated across multiple nodes that users view as a single, coherent system.

Decentralized System

- The critical difference between a decentralized system and distributed system is that in a distributed system, there still exists a central authority that governs the entire system; whereas, in a decentralized system, no such authority exists.
- A Decentralized system is a type of network where nodes are not dependent on a single master node; instead, control is distributed among many nodes.
- A significant innovation in the decentralized paradigm that has given rise to this new era of decentralization of applications is decentralized consensus.
- This mechanism came into play with Bitcoin, and it enables a user to agree on something via a consensus algorithm without the need for a central, trusted third party, intermediary, or service provider.

Methods of Decentralization

- Two methods can be used to achieve decentralization:
  - Disintermediation and
  - Competition (Contest-driven decentralization)

1. Disintermediation

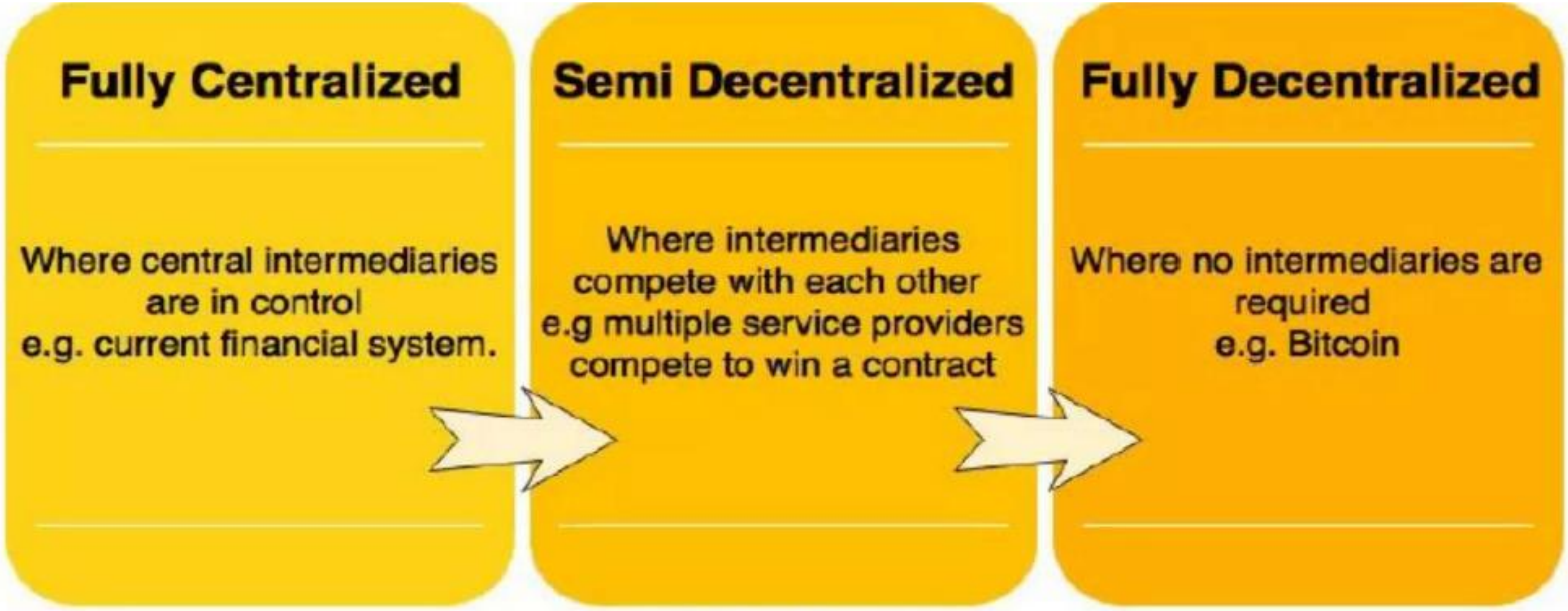
- The concept of disintermediation can be explained with the aid of an example:
  - Imagine that you want to send money to a friend in another country.
  - You go to a bank who, for a fee, will transfer your money to the bank in that country.
  - Here the bank maintains a central database that is updated, confirming that you have sent the money.
- With blockchain technology, it is possible to send this money directly to your friend without the need for a bank .
- All you need is the address of your friend on the blockchain.
- This way, the intermediary; that is, the bank, is no longer required, and decentralization is achieved by *disintermediation.*

2. Contest-driven decentralization

- In the method involving competition, different service providers compete with each other in order to be selected for the provision of services by the system.
- In the context of blockchain technology, a system can be envisioned in which smart contracts can choose an external data provider from a large number of providers based on their reputation, previous score, reviews, and quality of service.
- While there are many benefits of decentralization, including transparency, efficiency, cost saving, development of trusted ecosystems, and in some cases privacy and anonymity, some challenges, such as security requirements, software bugs, and human errors need to be examined thoroughly.

Scale of Decentralization

- Fully centralized
- Semi Decentralized
- Fully Decentralized



Fully Centralized

Where central intermediaries are in control
e.g. current financial system.

Semi Decentralized

Where intermediaries compete with each other
e.g multiple service providers compete to win a contract

Fully Decentralized

Where no intermediaries are required
e.g. Bitcoin

Scale of decentralization

Routes to Decentralization

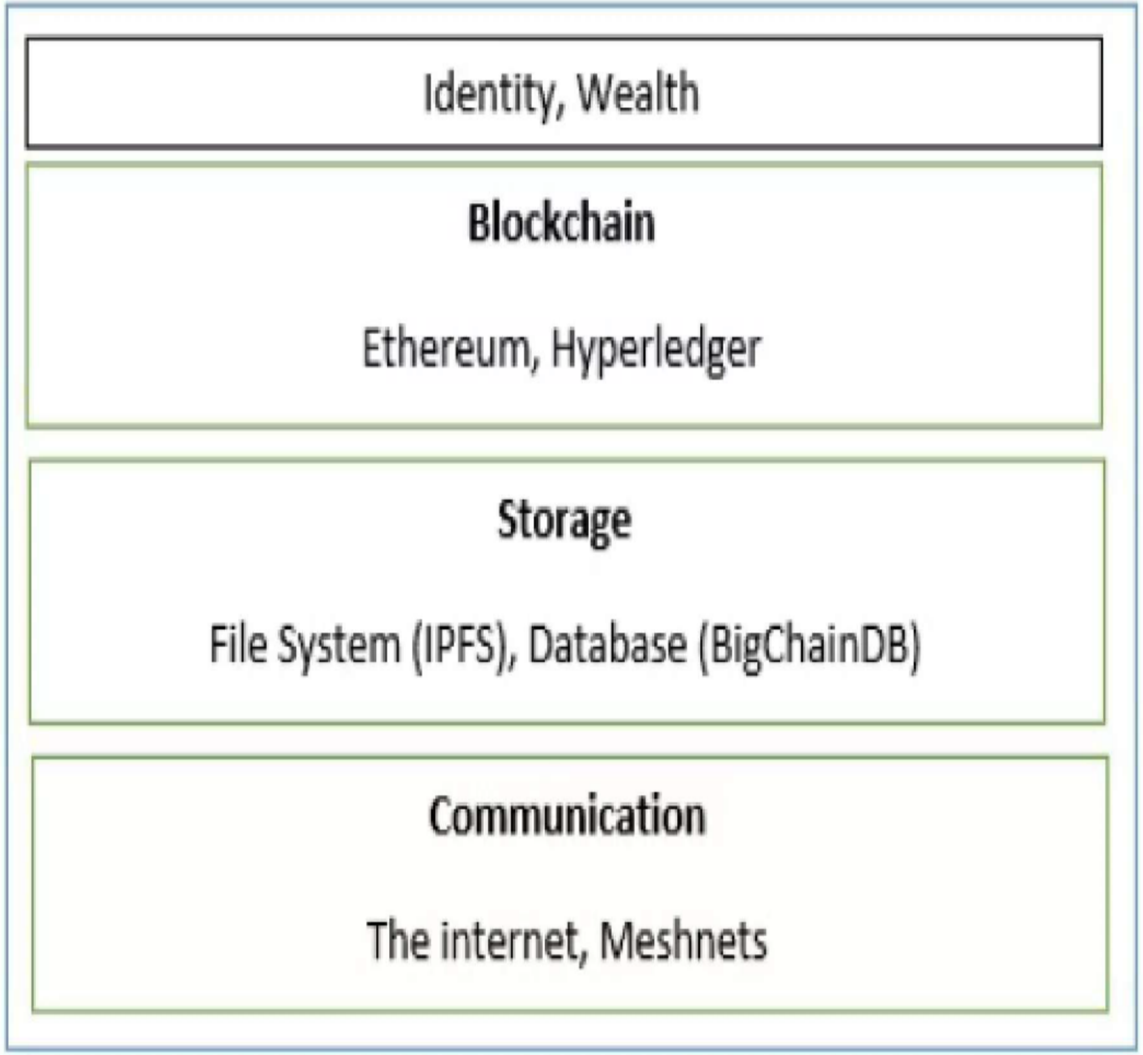
- Even though there were systems that pre-existed blockchain and Bitcoin, including BitTorrent and the Gnutella file sharing system, which to a certain degree could be classified as decentralized.
- However, with the advent of blockchain technology, many initiatives are now being taken to leverage this new technology for achieving decentralization.
- Example: First Choice - Bitcoin
- Alternatively, Ethereum - serve as the tool of choice for many developers for building decentralized applications.
- As compared to Bitcoin, Ethereum has become a more prominent choice because of the flexibility it allows for programming any business logic into the blockchain by using *smart contracts.*

How to decentralize??

- The framework raises four questions whose answers provide a clear understanding as how a system can be decentralized:
  1. What is being decentralized?
     - i.e type of system
  2. What level of decentralization is required?
     - Full / Partial Decentralization
  3. What blockchain is used?
     - What kind of Blockchain… Bitcoin/Etherium
  4. What security mechanism is used?
     - Atomicity based – transaction executes in full or not i.e Integrity of the system
     - Reputation – varying degrees of freedom

Decentralization Ecosystem

- To achieve complete decentralization, it is necessary that the environment around the blockchain also be decentralized.
- The blockchain is a distributed ledger that runs on top of conventional systems.
- These elements include:
  - storage,
  - communication, and
  - computation.



Decentralized ecosystem

Storage

- Data can be stored directly in a blockchain, and with this fact it achieves decentralization.
- However, a significant disadvantage of this approach is that a blockchain is not suitable for storing large amounts of data by design.
- A better alternative for storing data is to use Distributed Hash Tables (DHTs).
- DHTs were used initially in peer-to-peer file sharing software, such as BitTorrent, Napster, Kazaa, and Gnutella.
- There are other alternatives for data storage, such as Ethereum, Swarm, Storj, and MaidSafe.
  - Ethereum has its own decentralized and distributed ecosystem that uses Swarm for storage and the Whisper protocol for communication.
  - MaidSafe aims to provide a decentralized World Wide Web.
- BigchainDB is another storage layer decentralization project aimed at providing a scalable, fast, and linearly scalable decentralized database as opposed to a traditional file system. BigchainDB complements decentralized processing platforms and file systems such as Ethereum and IPFS.

Communication

- The internet (the communication layer in blockchain) is considered to to be decentralized .
- This model is based on unconditional trust of a central authority (the service provider) where users are not in control of their data.
- Even user passwords are stored on trusted third-party systems.
- Thus, there is a need to provide control to individual users in such a way that access to their data is guaranteed and is not dependent on a single third party.
- Access to the internet (the communication layer) is based on Internet Service Providers (ISPs) who act as a central hub for internet users.
- If the ISP is shut down for any reason, then no communication is possible with this model. An alternative is to use mesh networks.
- Even though they are limited in functionality when compared to the internet, they still provide a decentralized alternative where nodes can talk directly to each other without a central hub such as an ISP. **Example: Firechat - iphone**

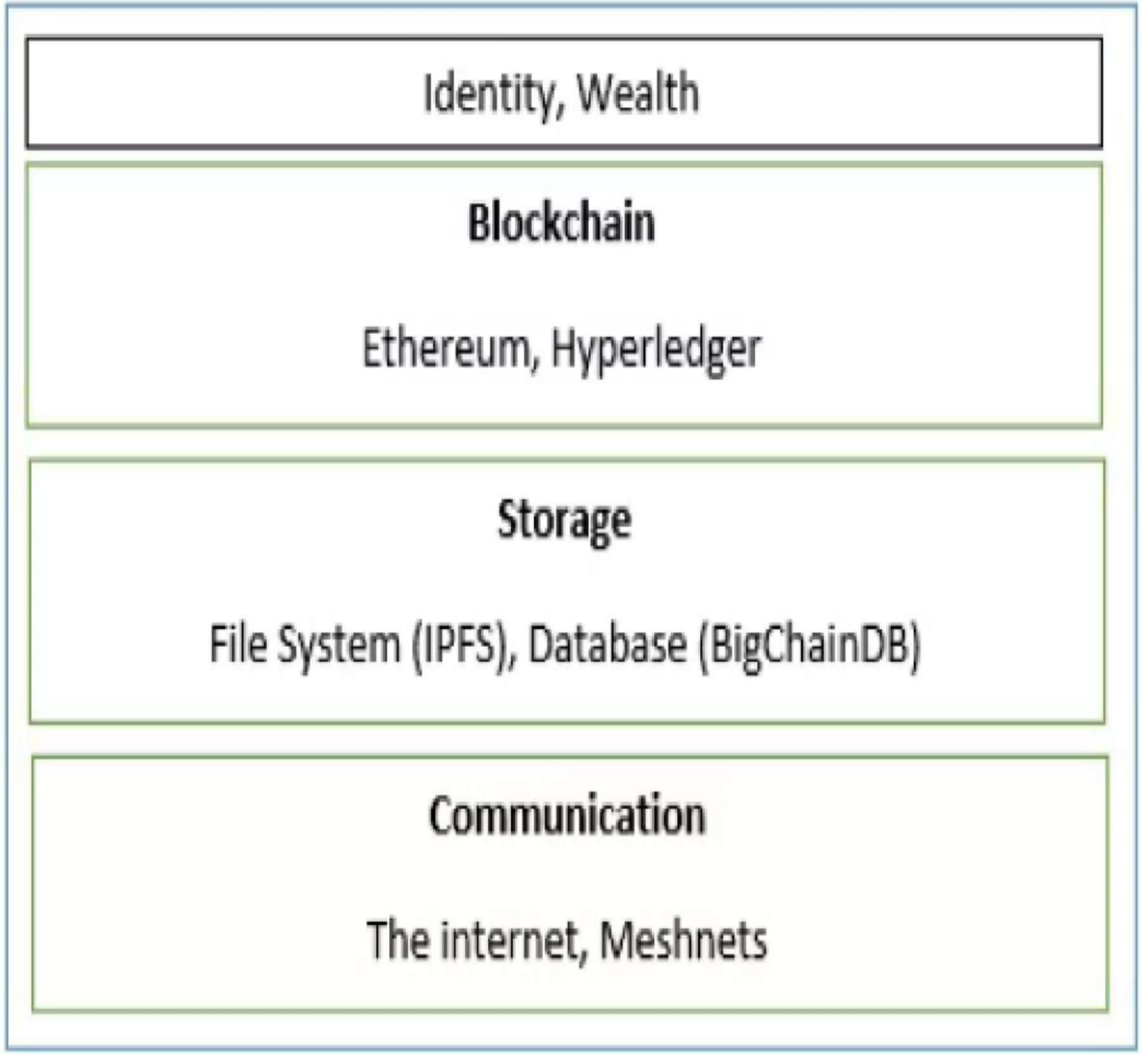
- Now imagine a network that allows users to be in control of their communication; no one can shut it down for any reason.
- This could be the next step toward decentralizing communication networks in the blockchain ecosystem.

Computing power and decentralization

- Decentralization of computing or processing power is achieved by a blockchain technology such as Ethereum, where smart contracts with embedded business logic can run on the blockchain network.
- Other blockchain technologies also provide similar processing-layer platforms, where business logic can run over the network in a decentralized manner.

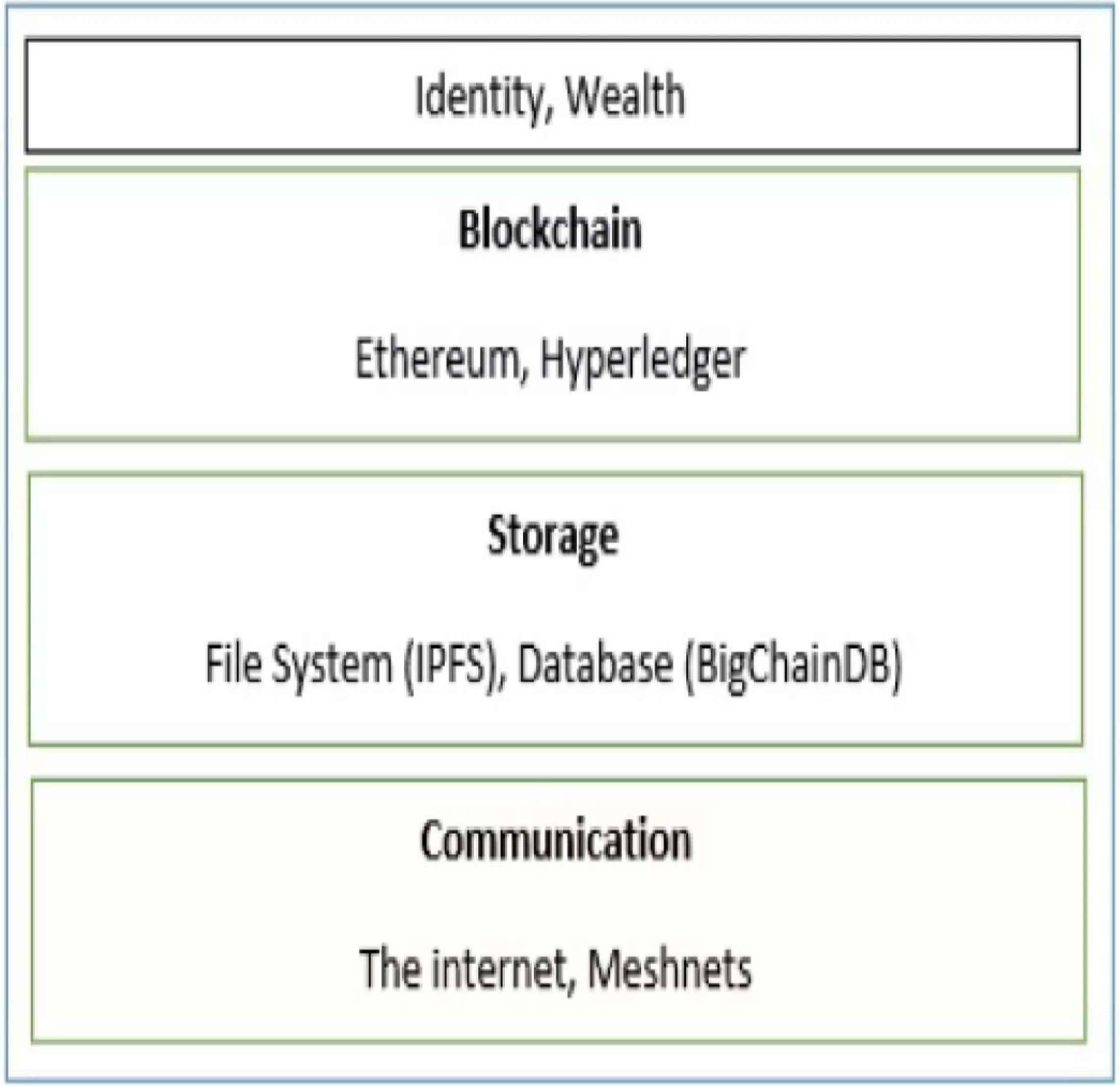
Decentralization Ecosystem

- At the bottom layer, the **internet or Meshnets** provide a decentralized communication layer
- On the next layer up, **a storage layer** uses technologies such as IPFS and BigchainDB to enable decentralization.
- Finally, at the next level up, you can see that blockchain serves as **a decentralized processing (computation)** layer. Blockchain in a limited way, provide a storage layer too, but that severely hampers the speed and capacity of the system.
- Therefore, other solutions such as IPFS and BigchainDB are more suitable to store large amounts of data in a decentralized way.



Decentralized ecosystem

- The Identity, Wealth layers are shown at the top level. Identity on the internet is a vast topic, and systems such as BitAuth and OpenID provide authentication and identification services with varying degrees of decentralization and security assumptions.
- The blockchain is capable of providing solutions to various issues relating to decentralization
- A concept relevant to identity known as Zooko's Triangle requires that the naming system in a network protocol be secure, decentralized, and is able to provide human-meaningful and memorable names to the users.



Identity, Wealth

Blockchain

Ethereum, Hyperledger

Storage

File System (IPFS), Database (BigChainDB)

Communication

The internet, Meshnets

Decentralized ecosystem

Pertinent Terminology

Smart contracts

- **A smart contract** is a decentralized program.
- Smart contracts do not necessarily need a blockchain to run; however, due to the security benefits it provides, blockchain has become a standard decentralized execution platform for smart contracts.
- A smart contract usually contains some business logic and a limited amount of data.
- The business logic is executed if specific criteria are met.
- Actors or participants in the blockchain use these smart contracts, or they run autonomously on behalf of the network participants.

Decentralized Organizations

- DOs are **software programs** that run on a blockchain and are based on the idea of actual organizations with people and protocols.
- Once a DO is added to the blockchain in the form of a smart contract or a set of smart contracts, it becomes decentralized and parties interact with each other based on the code defined within the DO software.

Decentralized Autonomous Organizations

- Decentralized Autonomous Organization (DAO) is also a computer program that runs atop a blockchain and embedded within it are governance and business logic rules.
- DAO and DO are fundamentally the same thing. The main difference, however, is that DAOs are autonomous, which means that they are fully automated and contain artificially intelligent logic. DOs, on the other hand, lack this feature and rely on human input to execute business logic.

Decentralized Autonomous Corporations

- Decentralized Autonomous Corporations (DACs) are similar to DAOs in concept, though considered to be a smaller subset of them.
- The definitions of DACs and DAOs may sometimes overlap, but the general distinction is that DAOs are usually considered to be nonprofit; whereas DACs can earn a profit via shares offered to the participants and to whom they can pay dividends.
- DACs can run a business automatically without human intervention based on the logic programmed into them.

Decentralized Autonomous Societies

- Decentralized Autonomous Societies {DASs) are a concept whereby an entire society can function on a blockchain with the help of multiple, complex smart contracts and a combination of DAOs and Decentralized Applications (DApps) running autonomously.
- This model does not necessarily translate to a free-for-all approach; instead, many services that a government commonly offers can be delivered via blockchains, such as government identity card systems, passports, and records of deeds, marriages, and births

Decentralized Applications (DApps)

- DApps, are software programs that can run on their respective blockchains, use an existing established blockchain, or use only the protocols of an existing blockchain.
- These are called Type I, Type II, and Type III DApps.

Requirements of a Decentralized Application

- The DApp should be fully open source and autonomous, and no single entity should be in control of a majority of its tokens. All changes to the application must be consensus-driven based on the feedback given by the community.
- Data and records of operations of the application must be cryptographically secured and stored on a public, decentralized blockchain to avoid any central points of failure.
- A cryptographic token must be used by the application to provide access and rewards to those who contribute value to the applications, for xample, miners in Bitcoin.
- The tokens must be generated by the DApp according to a standard cryptographic algorithm. This generation of tokens acts as a proof of the value to contributors (for example, miners).

Operations of a DApp

- Establishment of consensus by a DApp can be achieved using consensus algorithms such as PoW and PoS. So far, only PoW has been found to be incredibly resistant to 51% attacks, as is evident from Bitcoin. Furthermore, a DApp can distribute tokens (coins) via mining, fundraising, and development.

DApp examples

1. KYC-Chain

- This application provides the facility to manage Know Your Customer (KYC) data securely and conveniently based on smart contracts.

2. OpenBazaar

- This is a decentralized peer-to-peer network that enables commercial activities directly between sellers and buyers instead of relying on a central party, such as eBay and Amazon.
- DHTs are used in a peer-to-peer network to enable direct communication and data sharing among peers. It makes use of Bitcoin and various other cryptocurrencies as a payment method.

3.Lazooz

- This is the decentralized equivalent of Uber. It allows peerto- peer ride sharing and users to be incentivized by proof of movement, and they can earn Zooz coins.

Platforms for Decentralization

- Today, there are many platforms available for decentralization, in fact, the fundamental feature of blockchain networks is to provide decentralization.
- Therefore, any blockchain network such as Bitcoin, Ethereum, Hyperledger Fabric, or Quorum can be used to provide decentralization service.
- Many organizations around the world have introduced platforms that promise to make distributed application development easy, accessible, and secure.
- Some of these platforms are described below,
  - Ethereum
  - MaidSafe
  - Lisk

1. Ethereum

- Ethereum tops the list as being the first blockchain to introduce a Turing-complete language and the concept of a virtual machine.
- With the availability of its Turing-complete language called Solidity, endless possibilities have opened for the development of decentralized applications.
- This blockchain was first proposed in 2013 by Vitalik Buterin, and it provides a public blockchain to develop smart contracts and decentralized applications.
- Currency tokens on Ethereum are called **Ethers**.

2. MaidSafe

- MaidSafe provides a Secure Access For Everyone (SAFE) network that is made up of unused computing resources, such as storage, processing power, and the data connections of its users.
- The files on the network are divided into small chunks of data, which are encrypted and distributed randomly throughout the network.
- This data can only be retrieved by its respective owner.
- One key innovation of MaidSafe is that duplicate files are automatically rejected on the network, which helps reduce the need for additional computing resources needed to manage the load.
- It uses Safecoin as a token to incentivize its contributors.

3. Lisk

- Lisk is a blockchain application development and cryptocurrency platform.
- It allows developers to use JavaScript to build decentralized applications and host them in their respective sidechains.
- Lisk uses the Delegated Proof of Stake (DPOS) mechanism for consensus whereby 101 nodes can be elected to secure the network and propose blocks.
- It uses the Node.js and JavaScript backend, while the frontend allows the use of standard technologies, such as CSS3, HTML5, and JavaScript.
- Lisk uses LSK coin as a currency on the blockchain.
- Another derivative of Lisk is Rise, which is a Lisk-based decentralized application and digital currency platform.
- It offers a greater focus on the security of the system.