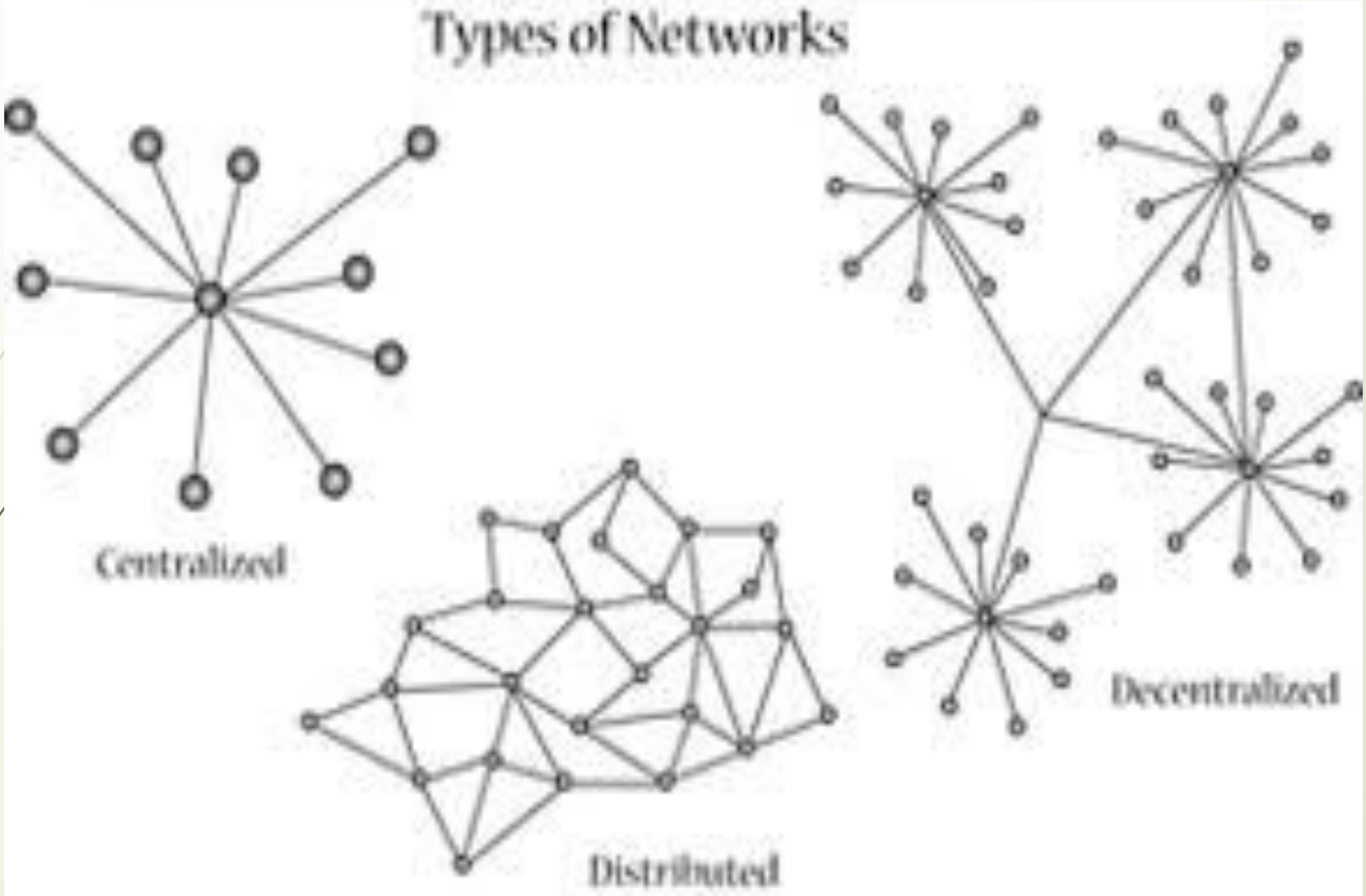
Decentralization

Decentralization using blockchain

- Decentralization is a core benefit and service provided by the blockchain technology.
- Blockchain does not need any intermediaries and 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 and **Proof of Work (PoW)**.

Decentralization using blockchain

- Decentralization is applied in varying degrees from semi-decentralized to fully decentralized depending on the requirements and circumstances.
- Example
  - Information and communication technology (ICT) has conventionally been based on a centralized paradigm
- With bitcoin and the advent of the blockchain technology, this model has changed and now the technology that allows anyone to start a decentralized system


Types of Networks
Centralized
Distributed
Decentralized

Centralized systems

- Conventional (client–server) IT systems whereby there is a single authority that controls the system and is solely in-charge of all operations on the system.
- Online service providers, such as eBay, Google, Amazon, Apple's App Store, and the majority of other providers, use this model of delivering services.

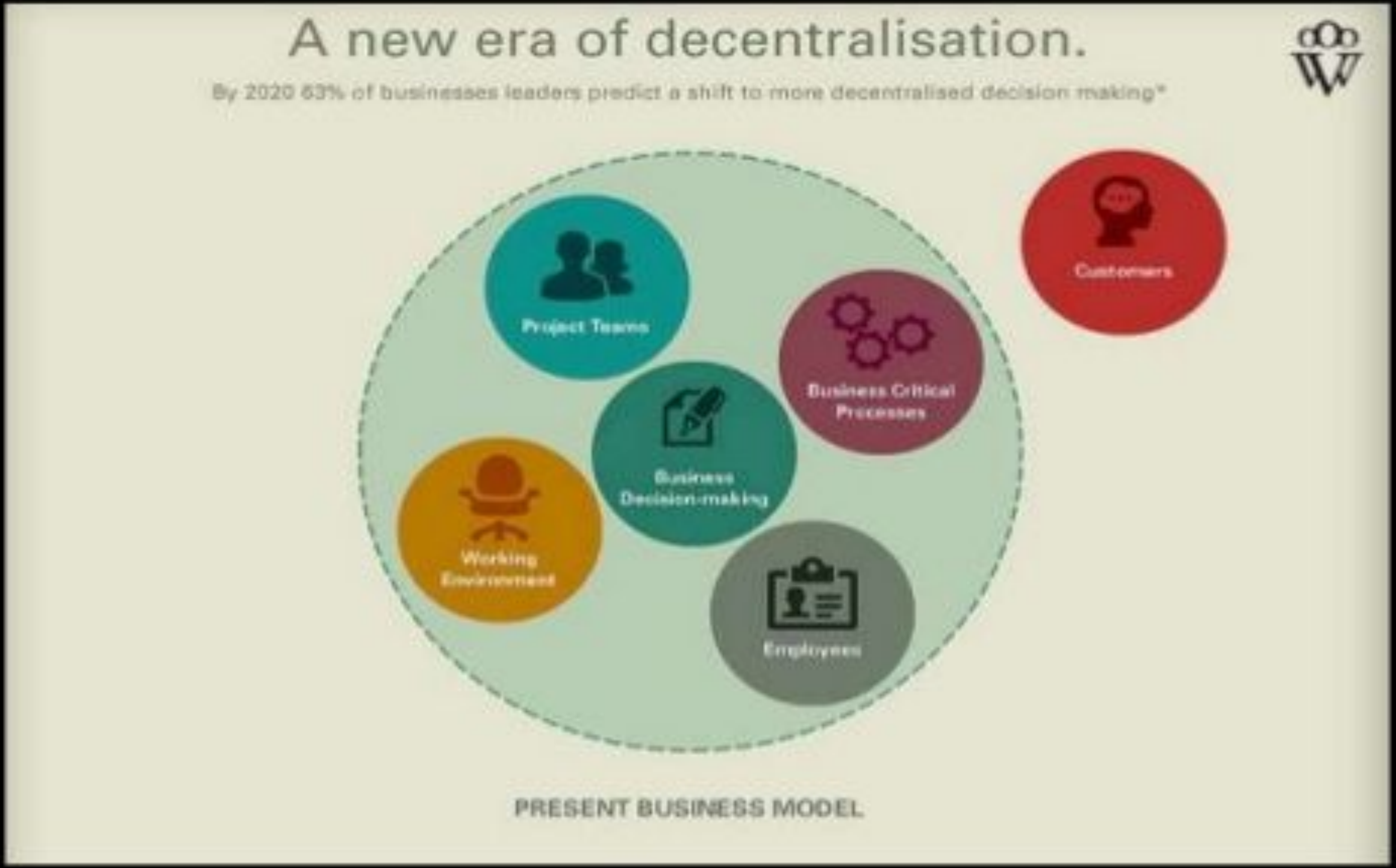
Distributed system

- Data and computation are spread across multiple nodes in the network.
- Parallel computing v/s Distributed system.
- Both of these models are used with variations in order to achieve failure tolerance and speed.
- In this model, there is still a central authority that has control over all nodes and governs processing.
  - This means that the system is still centralized in nature.

Decentralized system

- key difference between a decentralized system and distributed system
  - In a distributed system, there still exists a central authority that governs the entire system
  - In a decentralized system, no such authority exists.
- A decentralized system is a type of network whereby nodes are not dependent on a single master node;
  - instead, control is distributed among many nodes.
- User to agree on something via a consensus algorithm without the need for a central trusted third party, intermediary, or service provider
- **For example,**
  - Each department in an organization has its own database server
  - Taking away the power from the central server and distributing it to the sub-departments that manage their own databases.

“Decentralization” is a systematic delegation of authority at all levels of management and in all of the organization.



A new era of decentralisation.

By 2020 63% of businesses leaders predict a shift to more decentralised decision making*

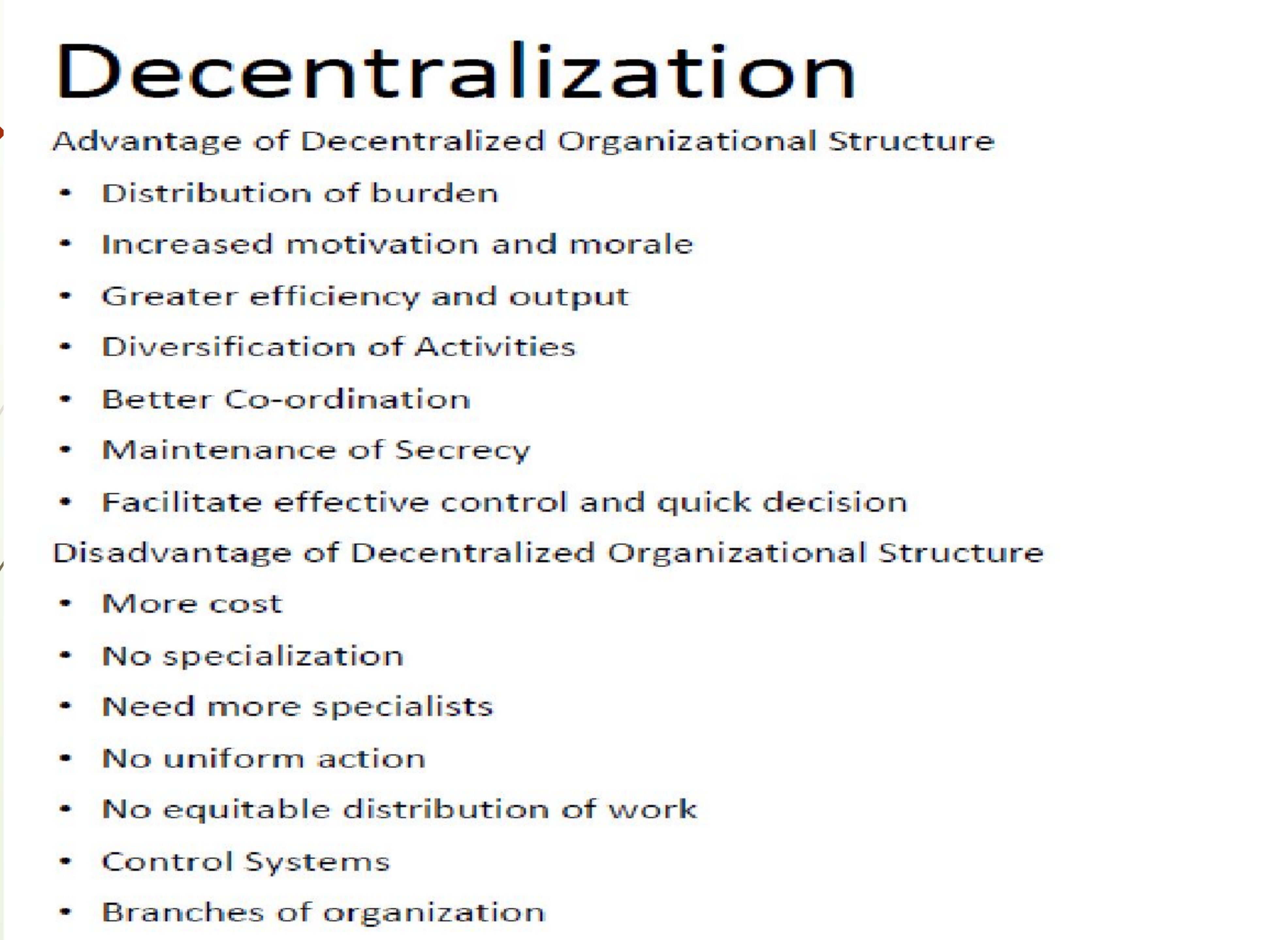
Decentralization

Advantage of Centralized Organizational Structure

- Reduced cost
- Uniformity in action
- Personal leadership
- Flexibility
- Improved quality of work
- Better co-ordination

Disadvantage of Centralized Organizational Structure

- Delay in work
- Remote control
- No loyalty
- No Secrecy
- No special attention



Decentralization

Advantage of Decentralized Organizational Structure

- Distribution of burden
- Increased motivation and morale
- Greater efficiency and output
- Diversification of Activities
- Better Co-ordination
- Maintenance of Secrecy
- Facilitate effective control and quick decision

Disadvantage of Decentralized Organizational Structure

- More cost
- No specialization
- Need more specialists
- No uniform action
- No equitable distribution of work
- Control Systems
- Branches of organization

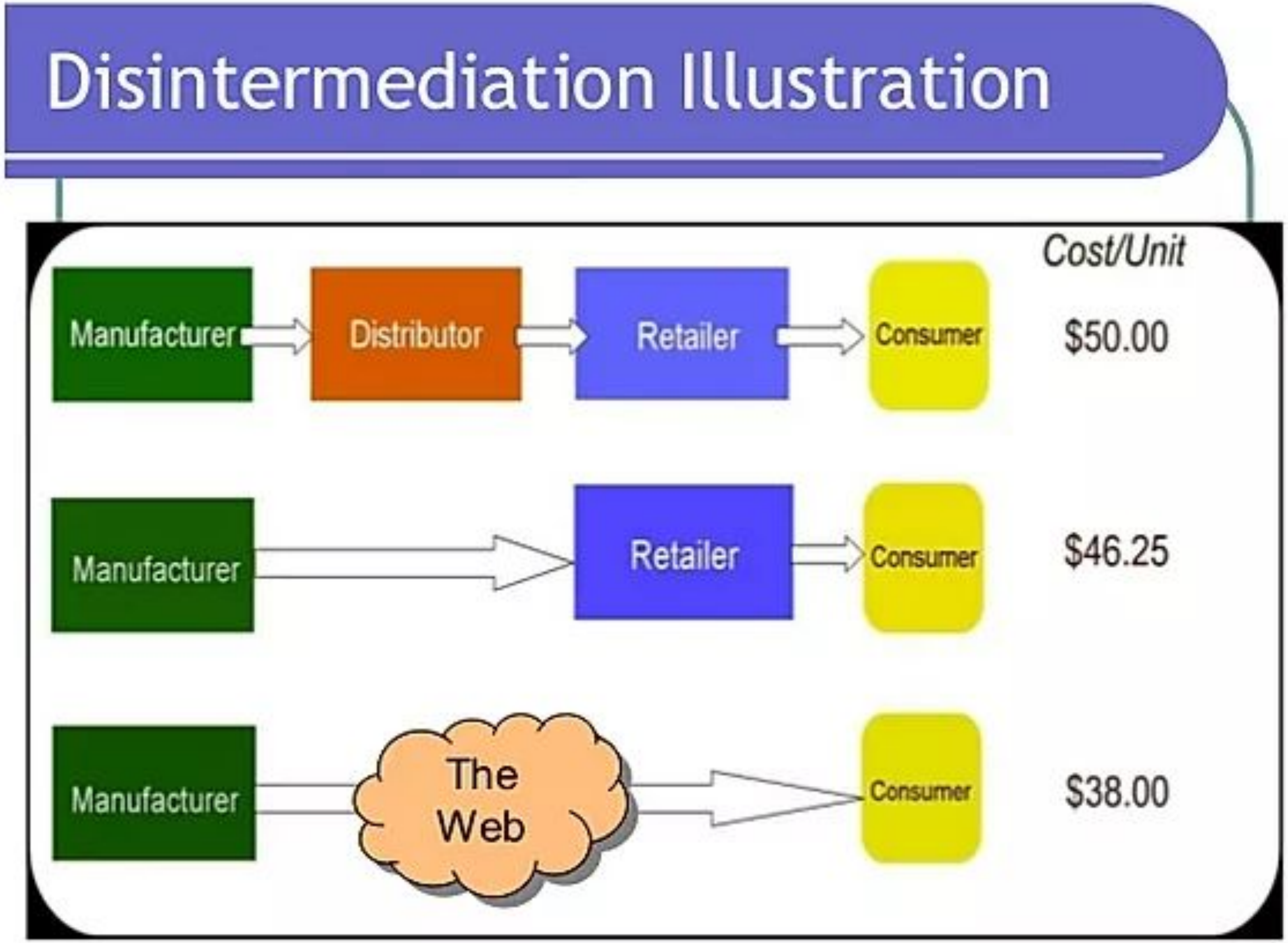
Methods of decentralization

- Disintermediation
- Through competition

Disintermediation

- **Example:** Imagine you want to send money to your friend in another country.
  - You go to a bank that will transfer your money to the bank for a fee.
  - Bank keeps 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.
- This way, the intermediary is no longer required and decentralization is achieved by disintermediation.
- This model can be used not only in finance but also in many other different industries.

Disintermediation Illustration



Cost/Unit

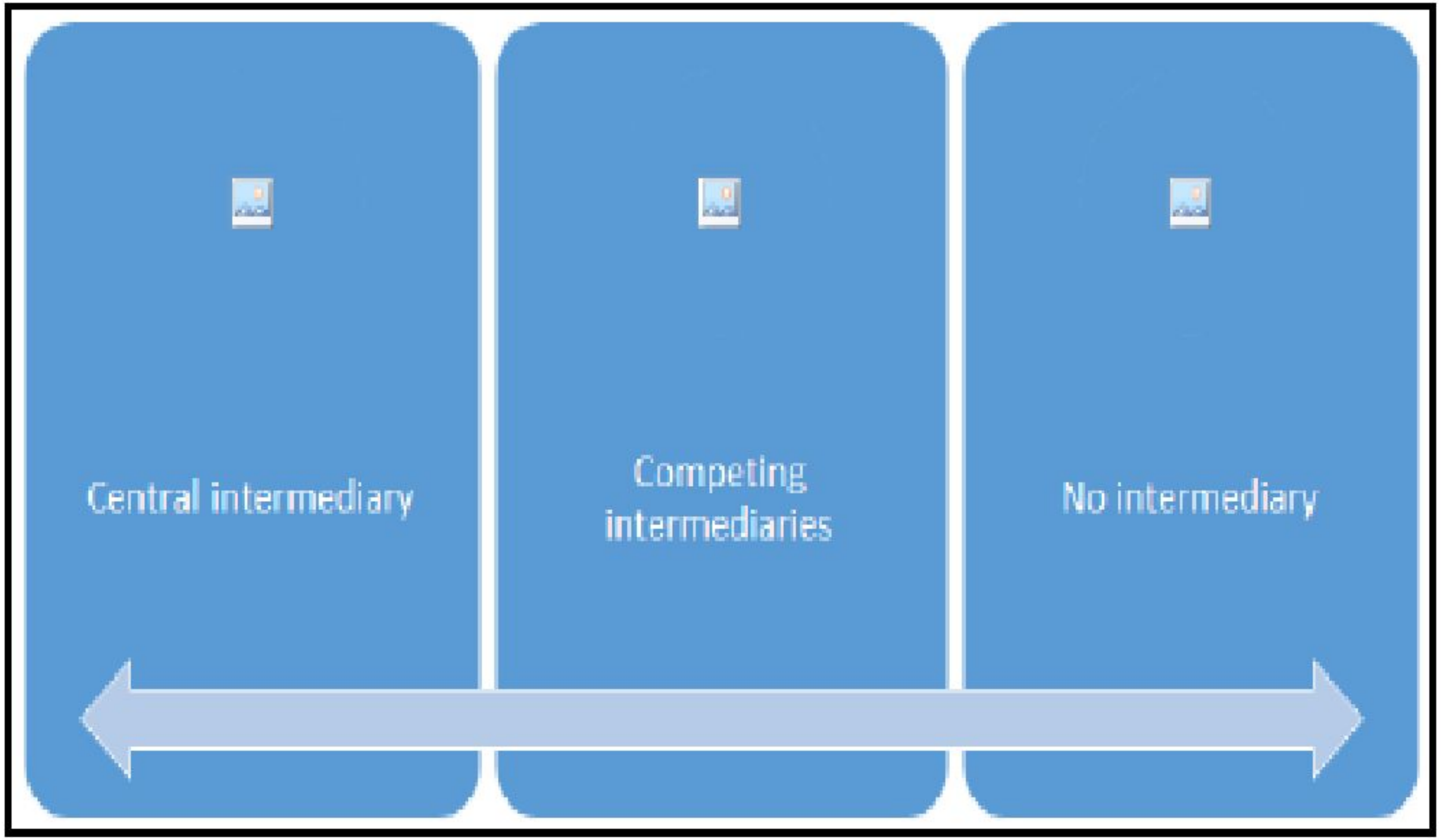
Manufacturer → Distributor → Retailer → Consumer $50.00

Manufacturer → Retailer → Consumer $46.25

Manufacturer → The Web → Consumer $38.00

Through competition

- Group of service providers compete with each other in order to be selected for the provision of services by the system.
- This paradigm **does not achieve complete decentralization**, but to a certain degree ensures that an intermediary or service provider is not monopolizing the service.
- In the context of blockchain technology
  - **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.
  - This will not result in full decentralization, but it **allows smart contracts to make a free choice** based on the criteria mentioned earlier.
- This way, an environment of competition is cultivated among service providers, whereby they compete with each other to become the data provider of choice.



Scale of decentralization

Benefits of decentralization

- Transparency
- Efficiency
- Cost saving
- Development of trusted ecosystems
- Privacy
- Anonymity

Challenges

- Security requirements
- Software bugs
- Human errors
- For example
    - In a decentralized system such as bitcoin or Ethereum, where security is usually provided by private keys
    - How can it be ensured that a smart property associated with these private keys cannot be rendered
    - Useless if, due to a human error, the private keys are lost or if, due to a bug in the smart contract code
    - Decentralized application is vulnerable to attack by adversaries

How to decentralize

- A framework has been proposed by ***Arvind Narayanan*** and others that can be used to evaluate the decentralization requirements of a variety of things in the context of blockchain technology.
- The framework basically proposes **four questions** that, once answered, provide a clear idea as to how a system can be decentralized.
  - **What is being decentralized?**
  - **What level of decentralization is required?**
  - **What blockchain is used?**
  - **What security mechanism is used?**

How to decentralize

- The first question simply asks **what system is being decentralized**.
  - Any system, for example an Identity system or trading.
- The next question can be answered by specifying the **level of decentralization** required by looking at the scale of decentralization.
  - full disintermediation / partial disintermediation.

How to decentralize

- Third question is quite straightforward, where developers can make a choice as to **which blockchain** is suitable for a particular application.
  - Bitcoin / Ethereum blockchain or any other blockchain
- key question needs to be answered about the **security mechanism** as to how the security of a decentralized system can be guaranteed.
  - Atomicity, for example, whereby either the transaction executes in full or does not execute at all. This ensures the integrity of the system.
  - Other mechanisms can include reputation, which allows varying degrees of trust in a system.

Examples

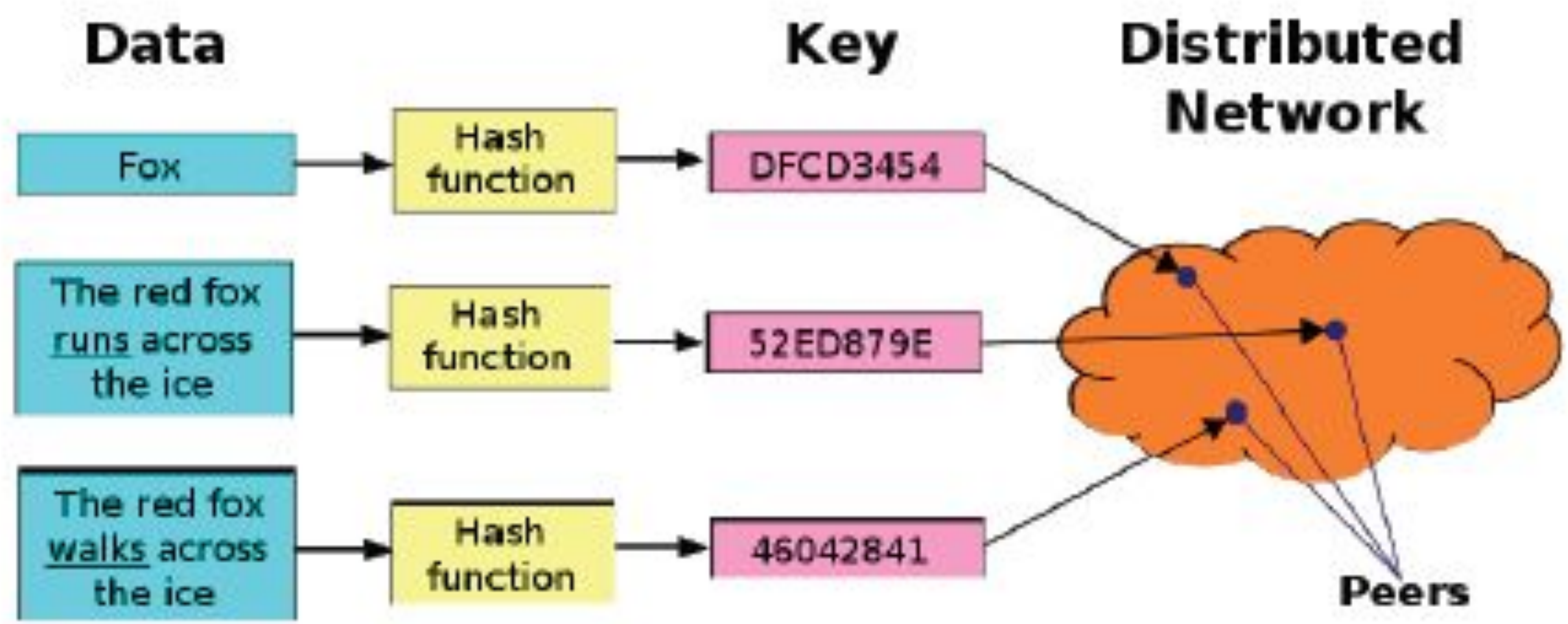
- Money transfer system -which is required to be decentralized
  - **Answer 1**:
    - Money transfer system.
  - **Answer 2**:
    - Disintermediation.
  - **Answer 3**:
    - Bitcoin.
  - **Answer 4**:
    - Atomicity.

Blockchain and full ecosystem decentralization

- In order to achieve complete decentralization, it is necessary that the environment around the blockchain is also decentralized
  - Storage
  - Communication
  - Computation

Storage

- Data can be stored directly in a blockchain, and with this, it does achieve decentralization,
- Major disadvantage of this approach is that blockchain is not suitable for storing large amounts of data by design
  - It can store simple transactions and some arbitrary data but is certainly not suitable for storing images or large blobs of data, as is the case in traditional database systems
- Alternative is to use distributed hash tables (DHTs).
- DHTs were originally used in peer-to-peer file sharing software, such as BitTorrent, Napster, Kazaa, and Gnutella.
- BitTorrent turns out to be the most scalable and fast network, but the issue is that there is no incentive for users to keep the files indefinitely



Distributed hash tables

Storage

- Users do not usually keep files permanentl
  - If nodes leave the network that has data required by someone there is no way to retrieve it except having the required nodes rejoin the network again so that the files become available once more.
- Two main requirements are **high availability** and **link stability**
  - Data should be available when required and network links should also always be accessible.

Storage

- **Inter Planetary File System (IPFS)** by *Juan Benet* possesses both properties and the vision is to provide a decentralized World Wide Web by replacing the HTTP protocol.
    - IPFS uses **Kademlia DHT** and **merkle DAG** (Directed Acyclic Graph) to provide the storage and searching functionality, respectively
    - The **incentive mechanism** is based on a protocol known as **Filecoin** that pays incentives to nodes that store data using the **BitSwap** mechanism.
    - The BitSwap mechanism allows nodes to keep a simple ledger of bytes sent or bytes received under a one-to-one relationship.
    - **Git-based version control mechanism** is used in IPFS to provide structure and control over the versioning of data.

Storage

- Ethereum has its own decentralized and distributed ecosystem that uses **Swarm** for storage and the **whisper** protocol for communication.
- **Maidsafe** is aiming 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 filesystem.
  - BigChainDB complements decentralized processing platforms and file systems such as Ethereum and IPFS.

Communication

- Services such as e-mail and online storage are all now based on a paradigm where the service provider is in control and users trust them to give them access to the service when required.
  - This model is based on the trust of the central authority (the service provider)
  - Users are not in control of their data; even passwords are stored on trusted third-party systems.
  - Access to user data is guaranteed and is not dependent on a single third party.

Communication

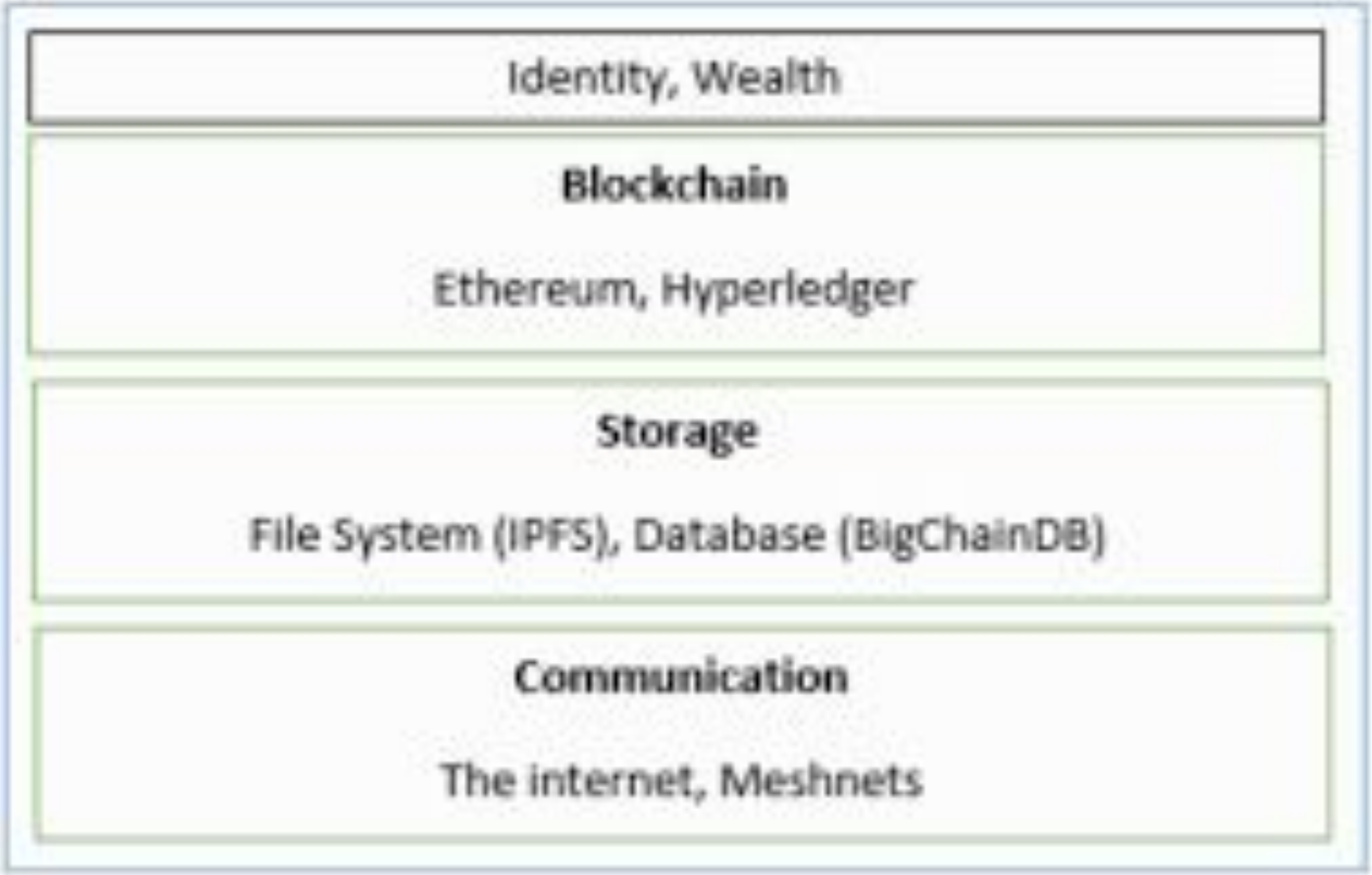
- Access to the Internet is based on Internet service providers (ISPs) that act as a central hub for Internet users.
  - If the ISP is shut down for any other reasons, then no communication is possible
- An alternative is to use mesh networks
  - Limited in functionality as compared to the Internet
  - Provide a decentralized alternative where nodes can talk directly to each other without a central hub such as an ISP.

Communication

- Original vision of the Internet was to build a decentralized network;
- Over the years, with the advent of large-scale service providers such as Google, Amazon, and eBay, the control is shifting toward the big players.
- For example, email is a decentralized system at its core; anyone can run an e-mail server with minimal effort and can start sending and receiving e-mails,
  - But there is a better alternative available that is already providing a managed service for end users,
- There is a natural inclination toward selecting a centralized service as it is more convenient and free
- Blockchain has once again given this vision of decentralization to the world

Computation

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



Identity, Wealth

Blockchain

Ethereum, Hyperledger

Storage

File System (IPFS), Database (BigChainDB)

Communication

The internet, Meshnets

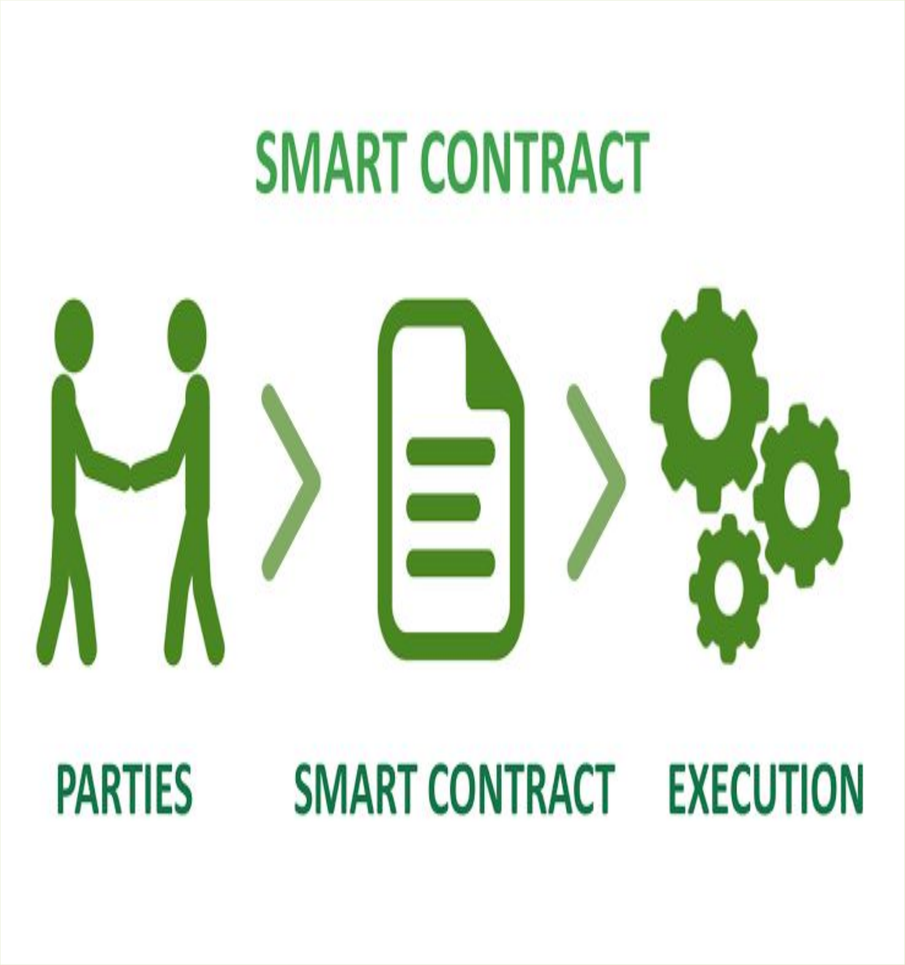
Decentralized ecosystem

Decentralized Ecosystem

- On the bottom layer, Internet or Meshnets provides a decentralized communication layer
- Storage layer uses technologies such as IPFS and BigChainDB to enable decentralization
- Blockchain that serves as a decentralized processing layer.

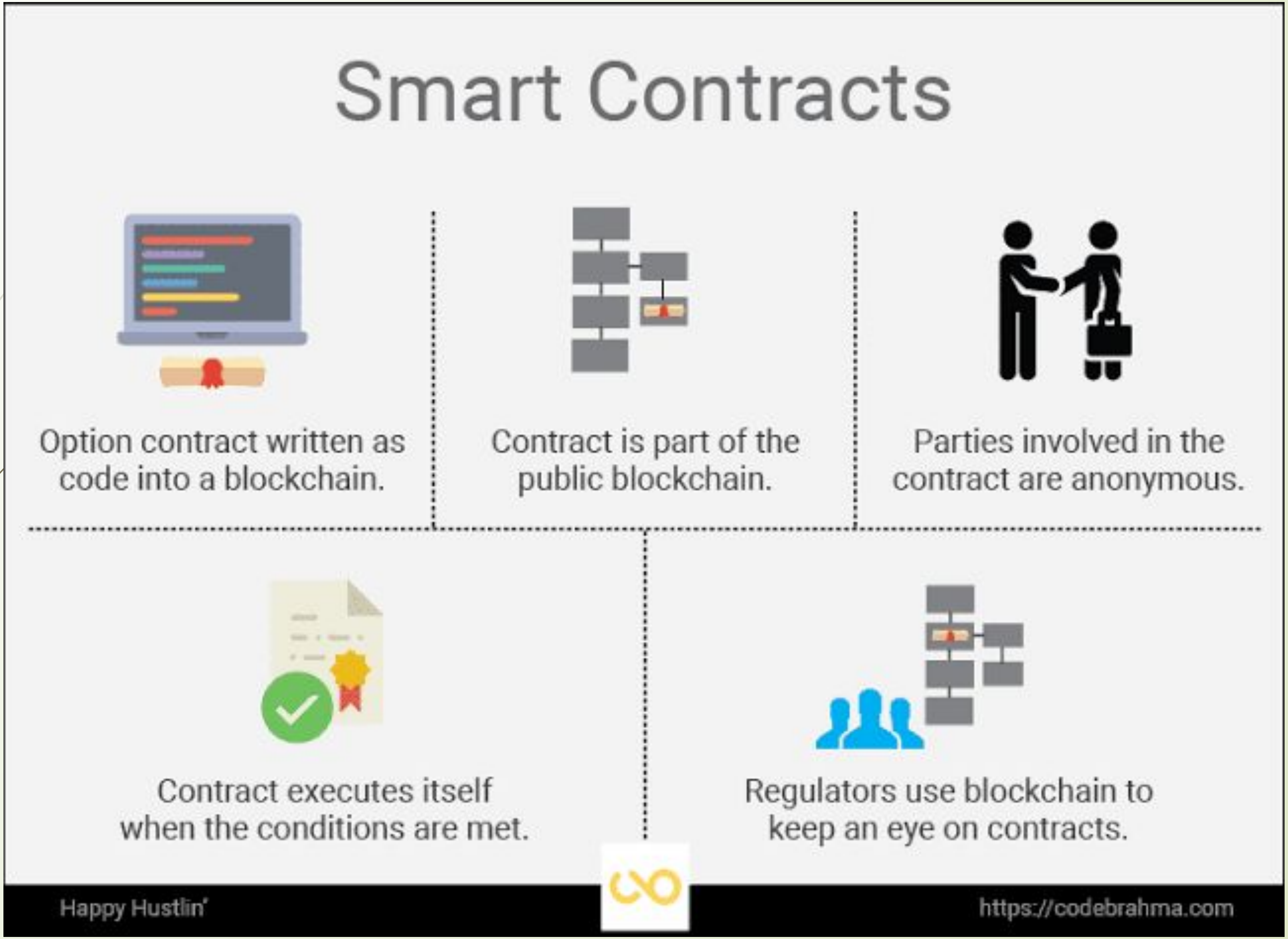
Smart contract

- A smart contract can be thought of as a small decentralized program.
- Smart contracts do not necessarily need a blockchain to run;
  - However, due to the **security benefits** that the blockchain technology provides, it is now becoming almost a standard to use blockchain as a decentralized execution platform for smart contracts.



Smart contract

- A smart contract usually contains some business logic and a limited amount of data.
- Actors or participants in the blockchain use these smart contracts or they run autonomously on behalf of the network participants.
- Small programs reside on the blockchain and execute business logic if some specific criteria are met



Smart Contracts

Option contract written as code into a blockchain.

Contract is part of the public blockchain.

Parties involved in the contract are anonymous.

Contract executes itself when the conditions are met.

Regulators use blockchain to keep an eye on contracts.

Decentralized organizations

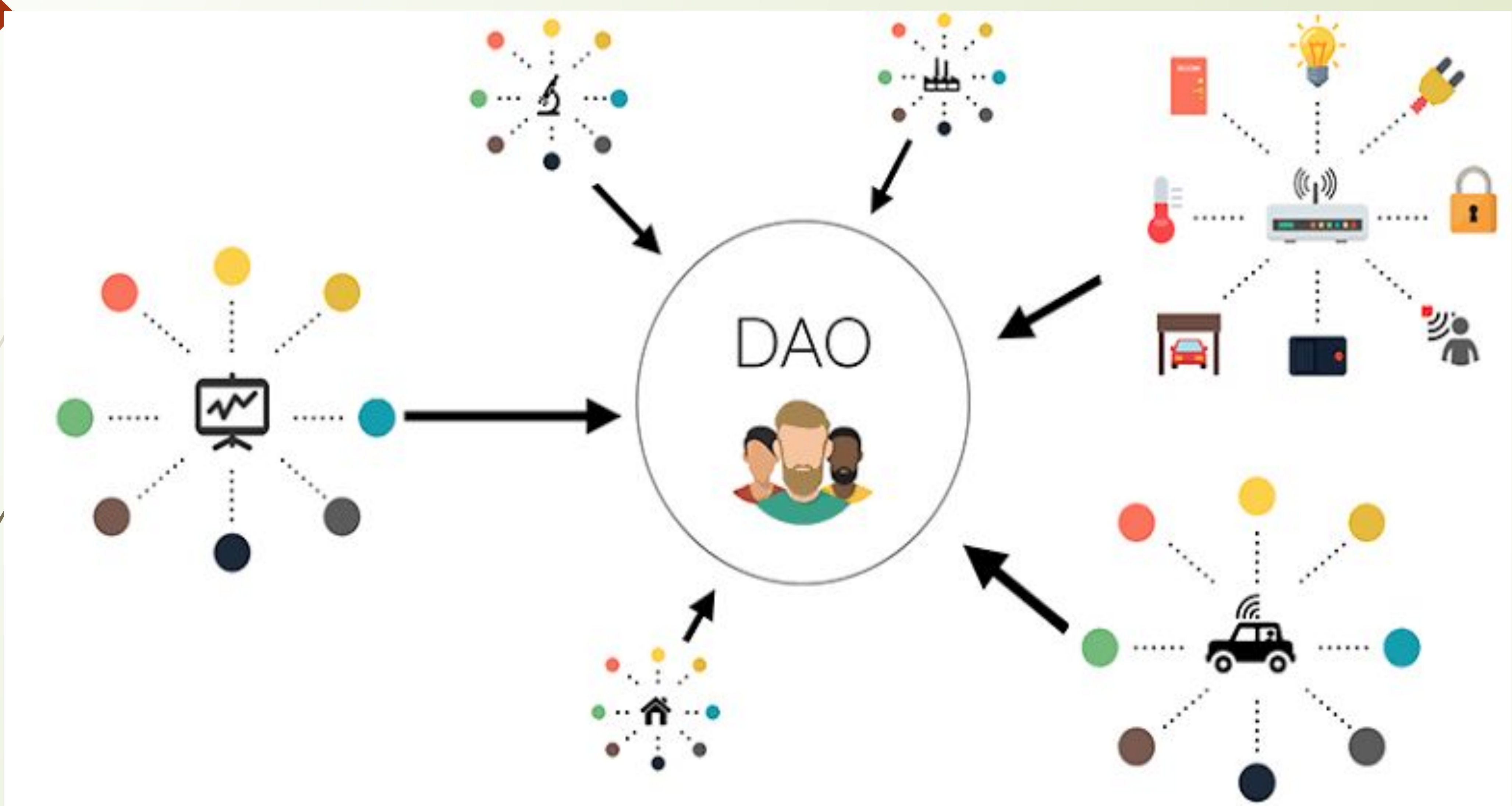
- **Decentralized organization (DOs)**
  - Software programs that run on a blockchain
  - Based on the idea of real human organizations with people and protocols.
- DO, in the form of a smart contract or a set of smart contracts, is added to the blockchain,
  - It becomes decentralized and parties interact with each other based on the code defined within the DO software.

Decentralized autonomous organizations

- Just like DOs, a **Decentralized autonomous organization** (**DAO**) is also a computer program than runs on top of a blockchain and embedded within it are governance and business logic rules.
- DAO and DO are basically the same thing, but the main difference is
  - DAOs are **autonomous**, which means that they are fully automated and contain artificially intelligent logic
  - DOs lack this feature and rely on human input in order to execute business logic.

Decentralized autonomous organizations

- Ethereum blockchain led the way with the introduction of DAOs for the first time.
- In DAO, the code is considered the **governing entity** rather than humans or paper contracts.
- ***Curator*,**, is a human entity that participates as someone who maintains this code and acts as a proposal evaluator for the community
- DAOs are capable of hiring external *Contractors* if enough input is received from the token holders (participants).


DAO

Decentralized autonomous organizations

- The most famous DAO project is *The DAO* (https://daohub.org) as it raised 168 million US dollars in its crowd-funding phase.
    - Venture capital fund which was aimed at providing a decentralized business model with no single entity as an owner.
    - Hacked due to a bug in the DAO code and millions of dollars' worth of **Ether currency** (**ETH**) were siphoned out of the DAO into a child DAO created by the hackers.
    - It required **a hard fork** on the Ethereum blockchain to reverse the impact of the hack and initiate the recovery of the funds.
- **hard fork**: is a radical change to the protocol that makes previously invalid blocks/transactions valid (or vice-versa).
    - A **hard fork** requires all nodes or users to upgrade to the latest version

Decentralized autonomous organizations

- DAOs **do not have any legal status** even though they may contain some intelligent code that enforces some protocols and conditions,
  - But these rules have no value in the current real-world legal system
- An **Autonomous Agent** (**AA**) is a piece of code that runs without human intervention.
- The fact that DAOs are purely decentralized entities makes it possible to run them in any physical jurisdiction.
  - Issue is how a current legal system would work with such a varied mix of different jurisdictions and geographies.

Decentralized autonomous corporations

- **DAOs** and **Decentralized autonomous corporations (DACs)** are a similar concept but are considered a smaller subset of DAOs.
- General difference is
  - DAOs are usually considered to be nonprofit,
  - DACs can make money via shares offered to the participants and by paying dividends.
- These corporations can run a business automatically without human intervention based on the logic programmed within them.

Decentralized autonomous societies

- **Decentralized autonomous societies** (**DASs**) are a concept whereby entire societies can function on a blockchain with the help of
  - multiple complex smart contracts
  - combination of DAOs and **Decentralized applications** (**DAPPs**)
- Many services that a government offers can be delivered via blockchain,
  - Government Identity Card systems, passport issuance, ,records of deeds, marriages, and births.
- if a government is corrupt and central systems do not provide the satisfactory levels of trust that a society needs
  - Society can start its own virtual blockchain that is driven by decentralized consensus and is transparent.

Decentralized applications

- All DAOs, DACs, and DOs are basically decentralized applications that run on top of a blockchain in a peer-to-peer network.
- Decentralized applications or DAPPs are software programs that can
  - Run on their own blockchain
  - Use another already existing established blockchain,
  - Use only protocols of an existing blockchain solution.
- 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 in order to avoid any central points of failure.
- A cryptographic token must be used by the application in order to provide access and rewards to those who contribute value to the applications, for example, miners in bitcoin.
- The tokens must be generated by the decentralized application according to a standard cryptographic algorithm.

Operations of a DAPP

- Establishment of consensus by a DAPP can be achieved using consensus algorithms such as Proof of Work and Proof of Stake.
- PoW has been found to be incredibly resistant to 51% attacks, as is evident from bitcoin.
- DAPP can distribute tokens (coins) via mining, fundraising, and development.

Examples -Decentralized applications

- **KYC-Chain**
  - Application to manage **Know Your Customer** (**KYC**) data in a secure and convenient way based on smart contracts.
- **OpenBazaar**
  - Decentralized peer-to-peer network that allows commercial activities directly between sellers and buyers instead of relying on a central party
    - as opposed to conventional providers such as eBay and Amazon.
  - It should be noted that this system is not built on top of a blockchain; instead, distributed hash tables are used in a peer-to-peer network in order to enable direct communication and data sharing between peers.
    - It makes use of bitcoin as a payment network

Examples -Decentralized applications

- **Lazooz**
  - Decentralized equivalent of Uber.
  - It allows peer-to-peer ride sharing
  - Users can be incentivized by *proof of movement* and can earn Zooz coins.

Platforms for decentralization-Ethereum

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

Platforms for decentralization-Maidsafe

- Maidsafe provides a **SAFE** (**Secure Access for Everyone**) 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 that are encrypted and distributed throughout the network randomly.
  - This data can only be retrieved by its respective owner.
- One key innovation is that duplicate files are automatically rejected on the network, which helps reduce the need for additional computing resources to manage the load.
- It uses **Safecoin** as a token to incentivize its contributors.

Platforms for decentralization-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 own 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 whereas 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 has more focus on the security of the system.

References

- Imran Bashir. “Mastring BlockChain”, Packt
- Web Materials