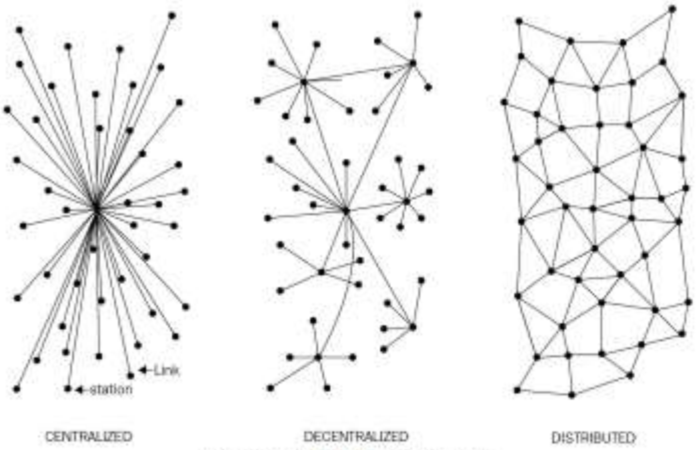
Decentralization using blockchain

Decentralization is applied in varying degrees from a semi-decentralized model to a fully decentralized one depending on the requirements and circumstances. Decentralization can be viewed from a blockchain perspective as a mechanism that provides a way to remodel existing applications and paradigms, or to build new applications, in order to give full control to users.



Different types of networks/systems

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 data and computation are spread across multiple nodes in the network. 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. Variations of both of these models are used with to achieve fault tolerance and speed. In the parallel system model, there is still a central authority that has control over all nodes, which governs processing. This means that the system is still centralized in nature.

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. This is analogous to a model where each department in an organization is in charge of its own database server, thus taking away the power from the central server and distributing it to the subdepartments who manage their own databases.

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.

Methods of decentralization

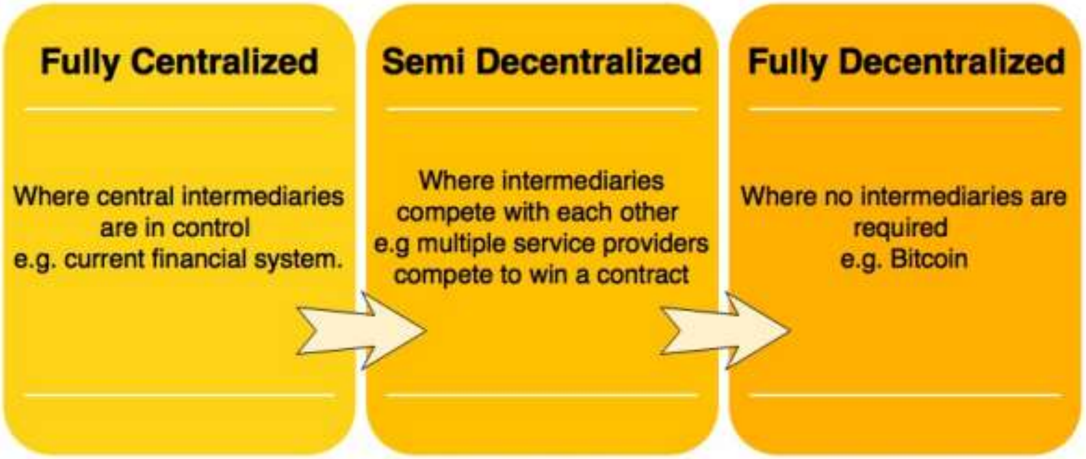
Two methods can be used to achieve decentralization: disintermediation and competition (Contest-driven decentralization). These methods will be discussed in detail in the sections that follow.

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. In this case, 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.

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. This paradigm does not achieve complete decentralization. However, to a certain degree, it ensures that an intermediary or service provider is not monopolizing the service. This method will not result in full decentralization, but it allows smart contracts to make a free choice based on the criteria just mentioned

In the following diagram, varying levels of decentralization are shown. On the left-hand side, the conventional approach is shown where a central system is in control; on the right-hand side, complete disintermediation is achieved as intermediaries are entirely removed. Competing intermediaries or service providers are shown in the center. At that level, intermediaries or service providers are selected based on reputation or voting, thus achieving partial decentralization.


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

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.

This view raises few fundamental questions. Is a blockchain really needed? When is a blockchain required? In what circumstances is blockchain preferred over traditional databases? To answer these questions, go through the simple set of questions presented here:

1. Is high data throughput required? If the answer to this question is yes, then use a traditional database.

2. Are updates centrally controlled? If yes, then use a conventional database.

3. Do users trust each other? If yes, then use a traditional database.

4. Are users anonymous? If yes, then use a public blockchain; if not, then use a private blockchain.

5. If consensus is required to be maintained within a consortium then use a private blockchain, otherwise use a public blockchain.

Answering all of these questions can provide an understanding of whether or not a blockchain is required.

Routes to decentralization

How to decentralize

The framework raises four questions whose answers provide a clear understanding as to how a system can be decentralized:

1. What is being decentralized?

2. What level of decentralization is required?

3. What blockchain is used?

4. What security mechanism is used?

The first question simply asks you to identify what system is being decentralized. This can be any system, such as an identity system or a trading system.

The second question asks you to specify the level of decentralization required by examining the scale of decentralization as discussed earlier. It can be full disintermediation or partial disintermediation.

The third question asks developers to determine which blockchain is suitable for a particular application. It can be Bitcoin blockchain, Ethereum blockchain, or any other blockchain

Finally, a fundamental question that needs to be addressed is how the security of a decentralized system will be guaranteed. For example, the security mechanism can be atomicity-based, where either the transaction executes in full or does not execute at all. This deterministic approach ensures the integrity of the system. Other mechanisms may include one based on reputation, which allows for varying degrees of trust in a system.

The decentralization framework example

The answers to these questions are as follows:

1. Money transfer system

2. Disintermediation

3. Bitcoin

4. Atomicity

The responses indicate that the money transfer system can be decentralized by removing the intermediary, implemented on the Bitcoin blockchain, and that a security guarantee will be provided via atomicity. Atomicity will ensure that transactions execute successfully in full or not execute at all. We have chosen Bitcoin blockchain because it is the longest established blockchain which has stood the test of time.

Blockchain and full ecosystem decentralization

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. It can store simple transactions and some arbitrary data, but it is certainly not suitable for storing images or large blobs of data, as is the case with traditional database systems.

Two primary requirements for storage systems are high availability and link stability, which means that data should be available when required and network links also should always be accessible.

InterPlanetary File System (IPFS) by Juan Benet possesses both of these properties, and its vision is to provide a decentralized World Wide Web by replacing the HTTP protocol. IPFS uses Kademlia DHT and Merkle Directed Acyclic Graph (DAG) to provide storage and searching functionality, respectively.

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

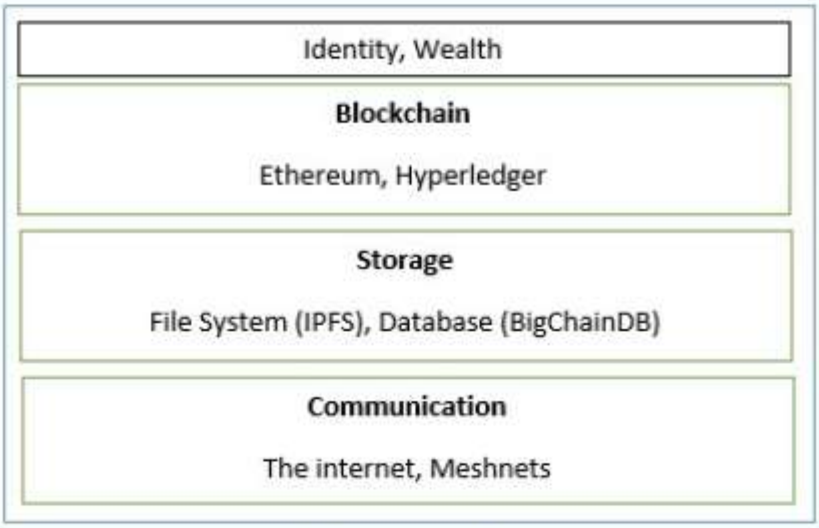
The **internet (**the communication layer in blockchain) is considered to be decentralized. This belief is correct to some extent, as the original vision of the internet was to develop a decentralized communications system. Services such as email and online storage are now all based on a paradigm where the service provider is in control, and users trust such providers to grant them access to the service as requested. 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

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.

The following diagram shows a decentralized ecosystem overview. 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 can, 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. 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.



Decentralized ecosystem

Pertinent Terminology

https://www.geeksforgeeks.org/important-blockchain-terminologies/