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.

In this chapter, we will discuss the concept of decentralization in the context of blockchain. The fundamental basis of blockchain is that no single central authority is in control, and, in this chapter, we will present examples of various methods of decentralization and routes to achieve this. Furthermore, we will discuss the decentralization of the blockchain ecosystem, decentralized applications, and platforms for achieving decentralization, in detail. Also, we will introduce you to numerous exciting applications and ideas that emerge out of the decentralized blockchain technology.

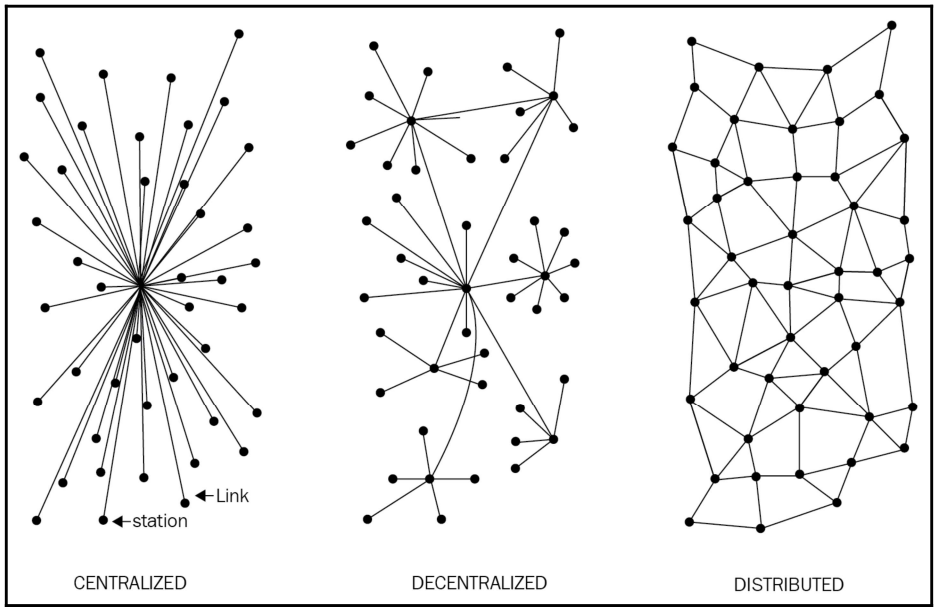
Decentralization using blockchain

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, and the most commonly used method is known as **Proof of Work** (**PoW**).

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.

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, this model has changed and now the technology exists, which allows anyone to start a decentralized system and operate it with no single point of failure or single trusted authority. It can either be run autonomously or by requiring some human intervention, depending on the type and model of governance used in the decentralized application running on blockchain.

The following diagram shows the different types of systems that currently exist: central, decentralized, and distributed. This concept was first published by Paul Baran in *On Distributed Communications: I. Introduction to Distributed Communications Networks* (Rand Corporation, 1964):



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.

A **distributed system**, data and computation are spread across multiple nodes in the network. Sometimes, this term is confused with *parallel computing*. While there is some overlap in the definition, 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; for example, parallel computing platforms are used in 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. 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.

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. 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.

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). These methods will be discussed in detail in the sections that follow.

Disintermediation

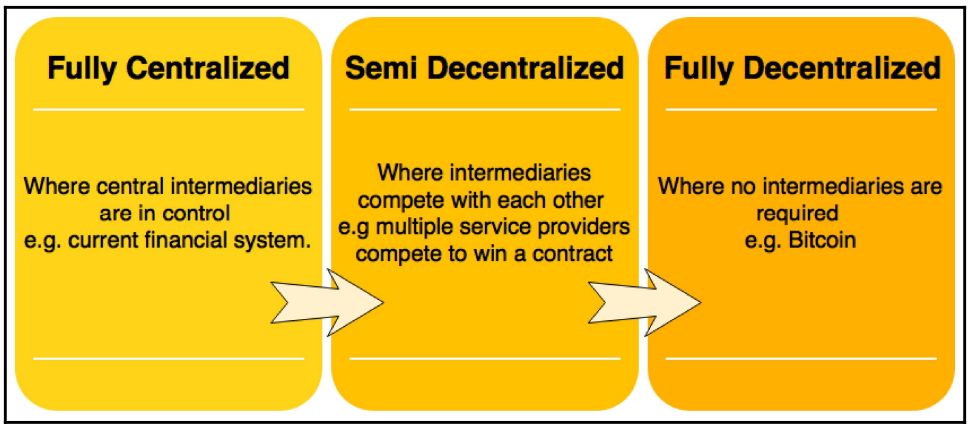
The concept of **disintermediation** can be explained with the aid of an example. Imagine that you want to send money to a friend in another country. You go to a bank who, for a fee, will transfer your money to the bank in that country. In this case, the bank maintains a central database that is updated, 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*. It is debatable, however, how practical decentralization through disintermediation is in the financial sector due to massive regulatory and compliance requirements. Nevertheless, this model can be used not only in finance but in many different industries as well.

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. 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.

This method will not result in full decentralization, but it allows smart contracts to make a free choice based on the criteria just mentioned. This way, an environment of competition is cultivated among service providers where they compete with each other to become the data provider of choice.

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.



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.

For example, in a decentralized system such as Bitcoin or Ethereum where security is normally provided by private keys, how can one ensure that a smart property associated with these private keys cannot be rendered useless if the private keys are lost or, due to a bug in the smart contract code or the decentralized application becomes vulnerable to attack? Before embarking on a journey to decentralize everything using blockchain and decentralized applications, it is essential that you understand that not everything can or needs to be decentralized.

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. Beyond the questions posed in this model there are many other issues to consider, such as latency, choice of consensus mechanisms, whether consensus is required or not, and where consensus is going to be achieved. If consensus is maintained internally by a consortium, then a private blockchain should be used; otherwise, if consensus is required publicly among multiple entities, then a public blockchain solution should be considered. Other aspects like immutably should also be considered while making a decision about whether to use a blockchain or a traditional database. If strict data immutability is required, then a public blockchain should be used; otherwise, a central database may be an option.

As blockchain technology matures, there will be more questions raised regarding this model. For now, however, this set of questions is sufficient to decide whether a blockchain-based solution is required or not.

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. The Bitcoin blockchain is typically the first choice for many, as it has proven to be the most resilient and secure blockchain and has a market cap of nearly $145 billion at the time of this writing. Alternatively, other blockchains, such as 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

Arvind Narayanan and others have proposed a framework in their book, *Bitcoin and Cryptocurrency Technologies*, *Princeton University Press*, that can be used to evaluate the decentralization requirements of a variety of issues in the context of blockchain technology. 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 that is deemed fit for the specific application.

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

Let's evaluate a money transfer system as an example of an application selected to be decentralized. The four questions discussed previously are used to evaluate the decentralization requirements of this application. 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.

Similarly, this framework can be used for any other system that needs to be evaluated in terms of decentralization. The answers to these four simple questions help clarify what approach to take to decentralize the system.

Blockchain and full ecosystem decentralization

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. There are other factors, such as identity and wealth, which are traditionally based on centralized paradigms, and there's a need to decentralize these aspects as well in order to achieve a sufficiently 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. 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.

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. DHT research was made popular by the CAN, Chord, Pastry, and Tapestry projects. BitTorrent is the most scalable and fastest network, but the issue with BitTorrent and the others is that there is no incentive for users to keep the files indefinitely. Users generally don't keep files permanently, and if nodes that have data still required by someone leave the network, there is no way to retrieve it except by having the required nodes rejoin the network so that the files once again become available.

Two primary requirements here 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. The concept of DHTs and DAGs will be introduced in detail in `Chapter 4`, *Public Key Cryptography*.

The incentive mechanism for storing data is based on a protocol known as Filecoin, which pays incentives to nodes that store data using the Bitswap mechanism. The Bitswap mechanism lets nodes keep a simple ledger of bytes sent or bytes received in a one-to-one relationship. Also, a Git-based version control mechanism is used in IPFS to provide structure and control over the versioning of data.

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. All of these projects are discussed later in this book in greater detail.

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. 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.

An example of a Meshnet is FireChat (`http://www.opengarden.com/firechat.html`), which allows iPhone users to communicate with each other directly in a peer-to-peer fashion without an internet connection.

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. It must be noted that this model may only be vital in a jurisdiction where the internet is censored and controlled by the government.

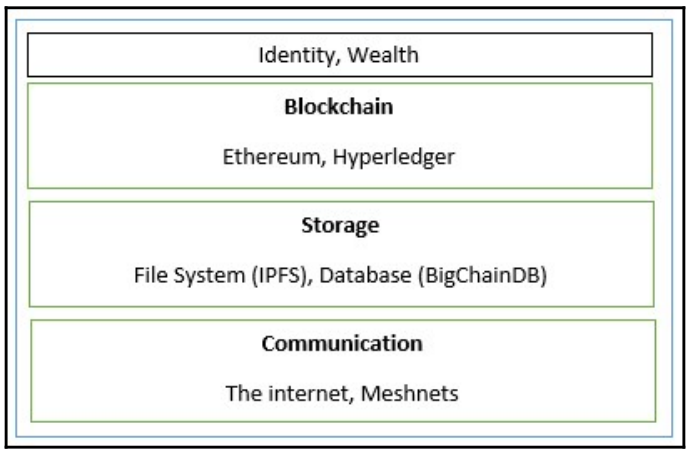
As mentioned earlier, the original vision of the internet was to build a decentralized network; however, over the years, with the advent of large-scale service providers such as Google, Amazon, and eBay, control is shifting towards these big players. For example, email is a decentralized system at its core; that is, anyone can run an email server with minimal effort and can start sending and receiving emails. There are better alternatives available, for example, Gmail and Outlook.com, which already provide managed services for end users, so there is a natural inclination toward selecting from these large centralized services as they are more convenient and free. This is one example that shows how the internet has moved toward centralization.

Free services, however, are offered at the cost of exposing valuable personal data, and many users are unaware of this fact. Blockchain has once again given this vision of decentralization to the world, and now concerted efforts are being made to harness this technology and take advantage of the benefits that it can provide.

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 assumptions:



Decentralized ecosystem

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. Conjecture has it that a system can have only two of these properties simultaneously. Nevertheless, with the advent of blockchain in the form of Namecoin, this problem was resolved. It is now possible to achieve security, decentralization, and human-meaningful names with the Namecoin blockchain. However, this is not a panacea, and it comes with many challenges, such as reliance on users to store and maintain private keys securely. This opens up other general questions about the suitability of decentralization to a particular problem.

Decentralization may not be appropriate for every scenario. Centralized systems with well-established reputations tend to work better in many cases. For example, email platforms from well reputed companies such as Google or Microsoft would provide a better service as compared to a scenario where individual email servers are hosted by users on the internet.

There are many projects underway that are developing solutions for a more comprehensive distributed blockchain system. For example, Swarm and Whisper are developed to provide decentralized storage and communication for Ethereum blockchain. We will discuss Swarm and Ethereum in more detail in `Chapter 11`, *Further Ethereum*.

With the emergence of the decentralization paradigm, different terminologies and buzzwords are now appearing in the media and academic literature. With the advent of blockchain technology, it is now possible to build software versions of traditional physical organizations in the form of **Decentralized Organizations** (**DOs**) and other similar constructs, which we will examine in detail shortly.

The following concepts are worth discussion in the context of decentralization.

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 that blockchain technology 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.

More information on smart contracts will be provided in `Chapter 9`, *Smart Contracts*.

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

Just like DOs, a **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.

The Ethereum blockchain led the way with the initial introduction of DAOs. In a DAO, the code is considered the governing entity rather than people or paper contracts. However, a human curator 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).

The most famous DAO project is The DAO, which raised $168 million in its crowdfunding phase. The DAO project was designed to be a venture capital fund aimed at providing a decentralized business model with no single entity as owner. Unfortunately, this project was hacked due to a bug in the DAO code, and millions of dollars' worth in **Ether currency** (**ETH**) was siphoned out of the project and into a child DAO created by hackers. A hard fork was required on the Ethereum blockchain to reverse the impact of the hack and initiate the recovery of the funds. This incident opened up the debate on the security, quality, and need for thorough testing of the code in smart contracts in order to ensure their integrity and adequate control. There are other projects underway, especially in academia, which are seeking to formalize smart contract coding and testing.

Currently, DAOs do not have any legal status, even though they may contain some intelligent code that enforces certain protocols and conditions. However, these rules have no value in the real-world legal system at present. One day, perhaps an **Autonomous Agent** (**AA**); that is, a piece of code that runs without human intervention, commissioned by a law enforcement agency or regulator will contain rules and regulations that could be embedded in a DAO for the purpose of ensuring its integrity from a legalistic and compliance perspective. The fact that DAOs are purely-decentralized entities enables them to run in any jurisdiction. Thus, they raise a large question as to how the current legal system could be applied to such a varied mix of jurisdictions and geographies.

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, nor is it based on an entirely libertarian ideology; 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. Another theory is that, if a government is corrupt and central systems do not provide the satisfactory levels of trust that a society needs, then that society can start its own virtual one on a blockchain that is driven by decentralized consensus and transparency. This concept might look like a libertarian's or cypherpunk's dream, but it is entirely possible on a blockchain.

Decentralized Applications (DApps)

All ideas mentioned up to this point come under the broader umbrella of DApps. DAOs, DACs, and DOs are DApps that run on top of a blockchain in a peer-to-peer network. They represent the latest advancement in decentralization technology. DApps, on the other hand, 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

For an application to be considered decentralized, it must meet the following criteria. This definition was provided in the whitepaper by Johnston and others, *The General Theory of Decentralized Applications, Dapps*:

- 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 example, 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

Examples of some decentralized applications are provided here.

KYC-Chain

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

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. It should be noted that this system is not built on top of a blockchain; instead, 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.

Lazooz

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

Many other DApps have been built on the Ethereum blockchain and are showcased at `http://dapps.ethercasts.com/`.

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 next.

Ethereum

Ethereum tops the list as being the first blockchain to introduce a Turing-complete language and the concept of a virtual machine. This is in stark contrast to the limited scripting language in Bitcoin and many other cryptocurrencies. 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**.

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.

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.

A more practical introduction to these platforms and others will be supplied in later chapters.

Summary

In this chapter, we introduced the concept of decentralization, which is the core service offered by blockchain technology. Although the concept of decentralization is not new, it has gained renewed significance in the world of the blockchain. Consequently, various applications based on a decentralized architecture have recently been introduced.

We began the chapter with an introduction to the concept of decentralization. Next, we discussed decentralization from the blockchain perspective. Moreover, we introduced you to ideas relating to the different layers of decentralization in the blockchain ecosystem and to the several new concepts and terms that have emerged with the advent of blockchain technology and decentralization from the blockchain perspective, including DAOs, DACs, and DApps. Finally, we looked at few examples of decentralized applications.

In the next chapter, we will present the fundamental concepts necessary to understanding the blockchain ecosystem; principally, we will introduce you to cryptography, which provides a crucial foundation for blockchain technology.