**LFS170x - Linux FoundationX**

Blockchain: Understanding Its Use Cases and Implications



Welcome to LFS170x: Blockchain - Understanding Its Use Cases and Implications

Linux FoundationX - LFS170x

Once you complete this course, you will have a good understanding of what blockchain is and its impact and potential for change around the world. You will also be familiar with some of the immediate blockchain use cases in technology, business, and enterprise products and institutions.

LFS170x is part of the [Blockchain for Business Professional Certificate](https://www.edx.org/professional-certificate/linuxfoundationx-blockchain-for-business). Skills in blockchain are being reported as the top job-skill in demand. This program is designed for the business professional who needs to understand the potential (or threat) of blockchain to their company and industry. Armed with better information of the blockchain landscape, this program will help you rise to new challenges in your current role by giving you a new dimension on which you can add value to your employer.

[Welcome!](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@f8765c952674412ab9fe9e185d56cfbb)

# **Chapter 1. Introduction to Blockchain**

* 1. [Introduction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@d63d14d2b81a45e2886828c2b89b8ca1)
  2. [Introduction to Blockchain and The Early Internet](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@4ee4f8bc0dad4e09ad99b376b061b0c9)
  3. [Blockchain Basics](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@7c07cfafff4943d7af3f883c18082724)
  4. [Career Opportunities in Blockchain](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@31aac67795644f13bd993a27072e4902)
  5. Who is Using [Blockchain](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@b5d8fe9812784047954a2e6fcf3eba66)?
  6. [Summary](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@a401d966ab5a4a04a9fdb4a8290d563d)

# **Chapter 2. Blockchain Mechanics**

* 1. [Introduction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@1088154e18e0450f9bb3a418121008c1)
  2. [Understanding Ledgers](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@47866c822c894049af4a2213c7a9d469)
  3. [Cryptography](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@5f4fa5704bd0432aad3727d0fb33c66a)
  4. [Transparency and Immutability](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@b2327e4750bc4beda267bf03132fbe6c)
  5. [Summary](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@3351e649f41b433f9bd4243c67c3f697)

# **Chapter 3. Blockchain Functions**

* 1. [Introduction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@ebc40eedf3f24ac6af007fe3d04f93c5)
  2. [Smart Contracts](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@f412320eace9423fb674eadd8118084c)
  3. [Blockchain Security](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@b51fe96ee70c460d94db5d7d2f1959b5)
  4. [Public and Permissioned Blockchains](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@9891087256c440f3bfc65d7492893a24)
  5. [The Blockchain Transaction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@f43ac8b873a74859af3de0a87f61337a)
  6. [Consensus](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@177e1191bc254b33aac28ac2d4ce45fd)
  7. [Summary](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@ce8663a813bb4af38f4785b86ebd88a3)

# **Chapter 4. Blockchains and Governance**

* 1. [Introduction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@fd421df72f0848b1a7bf96e602450141)
  2. [Open Source Code](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@da506b1cceb54093af75a07845fb5a36)
  3. [Governance](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@43e86826079c4284852c1bed6e11186b)
  4. [Identity and Anonymity on Blockchain](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@9ebbad69d6be4e7e9180f8e86ff2c1bc)
  5. [Summary](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@da27a79d56404477b3925c255eddf94a)

# **Chapter 5. Blockchain Problem Solving and Future Trends**

* 1. [Introduction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@c8a9ccbd46b748b88d7c2867f42ea0d0)
  2. [Problems Blockchain Solves](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@ed004881d34343899d18744ba074c9ee)
  3. [Digital Currencies](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@8ec45efd8fb04b75b6268e0b18f06410)
  4. [Future Trends](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@af775e511d8f47d49a698b07e7164386)
  5. [Summary](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@295e06b2437946df9a58b5ec475c88ea)

# Chapter 6. Blockchain Use Cases

* 1. [Introduction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@160833e7ed3848079dfea0f73128f459)
  2. [Blockchain in Practice](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@dae16c3b9a8b4a84a427752af12cd165)
  3. [Enterprise Solutions](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@e1cdd90003f34a3395a52438d3d5d318)
  4. [Public Sector Solutions](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@f35e0c4e6550431ea09ba040f0b53bf2)
  5. [Social Impact Solutions](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@561e3635558e41b1a49d4a1accbda125)
  6. [Future of Blockchain](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@1693a69f91cf4e349b8467d6048958f4)
  7. [Summary](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@6e8e2af862604b129e957f5eb1fd1889)

# Introduction to Blockchain

## [Learning Objectives](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+1T2020/block-v1:LinuxFoundationX+LFS170x+1T2020+type@sequential+block@aebb38d0b0e44fdc8ab82f3fa11cc9aa)

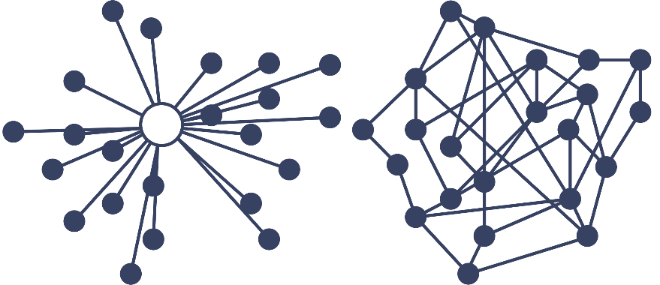
By the end of this chapter, you should be able to:

* Discuss blockchain technologies and the early Internet.
* Explain the difference between blockchain and the cryptocurrency Bitcoin.
* Discuss blockchain characteristics.
* Explain blockchain components.
* Explain what the block in blockchain is.
* Explain how blocks are chained together.
* Discuss the concept of immutability in a blockchain.
* Discuss about the roles and users in a blockchain community.
* Discuss use cases for general blockchain solutions.

## What is Blockchain

Blockchain is a peer-to-peer ledger system that allows peers to transact directly with each other eliminating the need for a central authority.

At its core, blockchain is a system for recording information about a transaction in a new decentralized way that makes it difficult or impossible to alter. These transactions are stored on sheets or blocks in a digital ledger that is shared among the participants of the network. Consensus on the transactions, brings the peer-to-peer network into agreement. Once the agreed-upon transactions blocks are recorded in the immutable ledger, trust becomes a fundamental component built into the system.



## The Early Internet

What started as a [DARPA](https://www.darpa.mil/) (Defense Advanced Research Project Agency) experiment in decentralized computing communications between two university labs in California in 1970, became the Transmission Control Protocol/Internet Protocol, INTERNET PROTOCOL SUITE (TCP/IP) developed as a standard in networking protocol or computer communication standards, and it is the backbone of today’s Internet.

With the TCP/IP protocols in place, users had the ability to link hypertext documents in an information system accessible from any node or computer using the TCP/IP protocol. The resulting information system or database is today’s World Wide Web.



With the birth of the World Wide Web, expanded usages of this new technology arose along with expanded business opportunities. Web servers, people who host and store the documents and web browsers, companies set up to help you view linked documents, help create a household need for this technology and the Internet explosion began.

## The Growth of the Internet

The Internet can be grouped into three distinct segments characterized by the way people interact with this new technology.

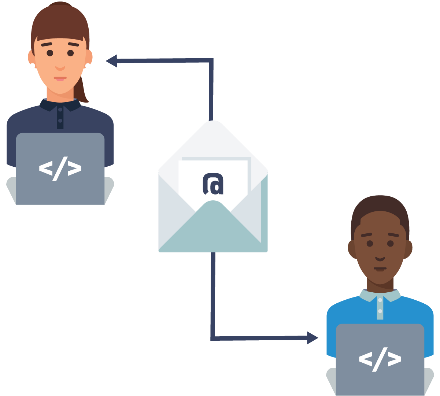
* Web 1.0 - Internet of Connection
* Web 2.0 - Internet of Information
* Web 3.0 - Internet of Value

Let’s discuss them in more detail.

## Web 1.0 - Internet of Connection

Characteristics of Web 1.0:

* Development of a host of web-based applications, which fostered in online services, such as email.
* Content from administrator.
* Managed by a central authority.
* Read-only, information was “pushed” to users.
* Email was the first widely adopted application on the Internet.



**Email, Electronically Transferring Information**

Computers and items for connection became necessities. Technology advancements in computers brought on changes, floppy disks became hard drives that stored MB that turned into GB that turned into TB. Internet speeds switched from kilobits to tens of megabits per second, to gigabits per second and RAM grew from hundreds of kilobytes to gigabytes and the dot-com bubble began. Companies appeared attempting to cash in on this new technology, most notable was a company called [Netscape](https://isp.netscape.com/) which developed the first commercial Web browser.



## Web 2.0 - Internet of Information

Characteristics of Web 2.0:

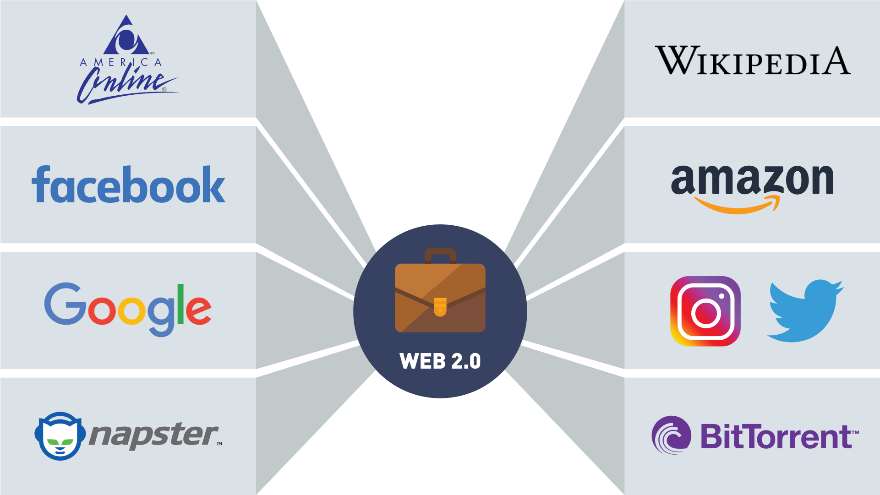
User-generated content.

Read-write, individuals can interact with information.

Information became siloed.

Data became a commodity.

Web 2.0 saw emerging marketplaces that brought together unrelated buyers and sellers in a seamless low-cost way. Data became a commodity collected, siloed and sold; we were giving up our information at a frenzied pace. Websites let users generate content, social networks became part of our lives.



**Social Networking**

## Real World Examples of File Sharing

**Use Case: Music Sharing Companies**



Approach: Music stored on many computers connected peer-to-peer. [Napster](https://us.napster.com/) software supplied its users with a centralized index of all music files and directed users to where these files were located on the connected peers' computers.

Result: The industry cracks down music sharing companies copyright infringement. Napster is forced to take down its index, shutting down the platform.



Approach: Music stored on many computers connected peer-to-peer. [BitTorrent](https://www.bittorrent.com/)'s software was purely decentralized, the files were stored as packet on the peers' computers and when a request was made for a song, the software would find the packet and send it to the user.

Result: The industry cracks down music sharing companies copyright infringement. BitTorrent is asked to shut down their platform. Since they do not control the software once downloaded to a peer, if two computers are running the software sharing can still occur.

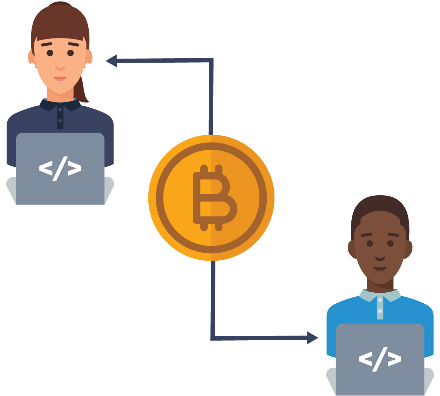
Music sharing companies gave us the first glimpse into peer-to-peer networking. Besides copyright infringement, the main challenge for the music sharing companies was file integrity. You could never be sure the file you requested was the file you would get and there was no one to complain to. Both Napster and BitTorrent are operating today, with different business models.

## Web 3.0 - Internet of Value

Characteristics of Web 3.0:

* Community interaction.
* More connected, open, and intelligent.
* Distributed ledgers or blockchain technology, smart contracts, machine learning and artificial intelligence.
* Identity and information will be held by the individual, breaking data silos.

Bitcoin is the first widely accepted application for the Internet of Value (just as email was the first big application for the Internet of Information).



**Cryptocurrencies, Electronically Transferring Value**

The Internet of Value represents a world where value is exchanged at the speed in which information moves today. The Internet is still the basic platform that these new technologies operate from. The new Web 3.0 browsers are being built to help you manage your cryptocurrency, keys, passwords and other blockchain features. Let’s now dive into blockchain basics.

## What Is Blockchain?

There's a new technology that has the power to revolutionize how you, businesses, and the world interact!

You've probably heard of it: it's called Blockchain!

But what is it? How does it work? How does it affect you?

Hearing the word "blockchain" is comparable to hearing the word "internet" in the early 90s.

It seemed elusive, like something that wasn't going to impact your daily life.

But here we are, more than 20 years later. Think about how the Internet has transformed businesses, commerce, communication, even music and video.

And that's not even touching on how the Internet has affected you.

We all carry the Internet in our pocket.

We can transfer money at the touch of a button, check the weather, get directions, and even have food delivered to our door.

The next technology to have that kind of impact isn't some of the buzzwords you hear.

It's not big data. It's not artificial intelligence. It's not even social media.

It's BLOCKCHAIN!

Now, let's discuss the vast promise blockchain has for every business, every society, and for everyone listening today.

And let's begin with an example we are all familiar with.

When you attach a file, a Word document, an Excel sheet, a PDF to an email, you aren't sending an original.

You are actually sending the recipient a copy, and that's a great way to move information around.

But it's not so great when it comes to things like money, stocks and bonds, music, loyalty points, intellectual property, tickets to a game or concert.

Then, sending a copy is suddenly a very bad idea.

Let's look at an example.

If I send you tickets to a concert, it's important that I don't send you a copy.

You now own the original asset and I can no longer use or sell those tickets.

Similarly, if I send you $100, it's important that I still don't own the $100, or have the ability to send it to anyone else.

Both of these examples illustrate a double spend problem, and those can be eliminated with blockchain.

So now, in this exciting time in history, every kind of asset, from tickets, to money, to music, can be stored, moved, exchanged, and transacted without an intermediary.

People everywhere can transact peer-to-peer and trust each other by using collaboration and cryptography.

How did we get here, to this place of trust and collaboration?

It began when Satoshi Nakamoto, whose true identity is still unknown, released a white paper in 2008, introducing a purely peer-to-peer version of electronic cash known as Bitcoin.

It is here that blockchain technology made its debut.

Even today people believe Bitcoin and blockchain are one and the same.

They are not!

Bitcoin, another alternative currency, utilize blockchain technology.

While an important one, Bitcoin is only one use case for blockchain.

Blockchain allows people to exchange assets and perform transactions without a third party.

Imagine a world where you don't need intermediaries.

While traditionally we have needed central authorities to trust one another and fulfill contracts, blockchain makes it possible to have our peers guarantee that for us. But how?

Assets, like we've discussed, are no longer stored in a central place, but distributed across a global ledger, using the highest level of cryptography.

When a transaction is conducted, it's posted across tens of thousands of computers around the globe.

These transactions are recorded as blocks.

Let's imagine a sheet of paper that has 25 lines.

When a sheet is filled up with 25 transactions, the block is validated via group consensus.

Once the page has been validated, it is added to a stack of previously validated sheets.

Each sheet on the stack can be assumed to be trustworthy because, once a sheet is validated, it can't be changed.

Because at this point, all the sheets are linked together.

And to link our sheets together, we embed information from the previous sheet of paper into the new, recently validated sheet.

In blockchain, our sheet of paper is equal to a block.

The act of embedding a previous block of information into the current block of information is called chaining, hence, the name blockchain.

In order to compromise or hack a blockchain network, someone would have to gain control of the majority of computers in that network.

This is extremely difficult to do.

There is no longer a single point of failure, and this is what makes blockchain infinitely more secure than what we have today.

Blockchain isn't just for assets, though. It extends to contracts.

These are called Smart Contracts.

And what are they exactly? What they sound like.

A smart contract self-executes and handles enforcement, the management, and performance of agreements between people.

Examples of smart contracts include insurance policies, copyrighted content, escrow and lending, wills, and trusts.

Smart contracts will revolutionize how we do business.

There are so many possibilities with blockchain; not just in the now, but with things we haven't begun to think about yet.

## Blockchain Is NOT Bitcoin

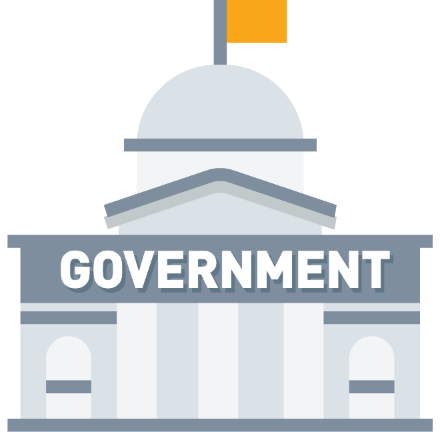
Bitcoin is a digital currency running on top of the Bitcoin blockchain. We will develop the concept of cryptocurrencies in later sections. Bitcoin has no borders and was created as a decentralized payment system, an alternative to currencies issued by governments. Let us look at what it means to be a currency.



 Purpose of currency:

* Medium for exchange
* Store of value over time
* Accepted as a measure of worth

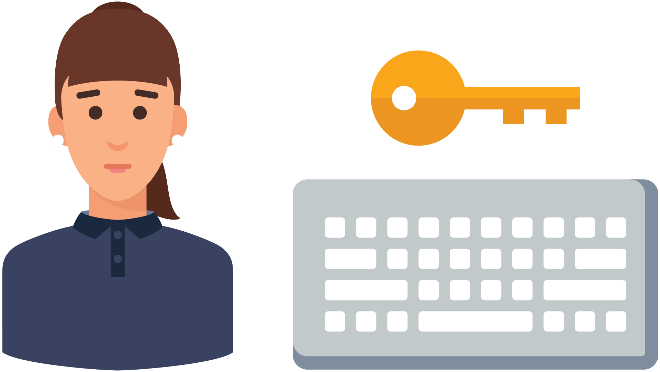
According to [Investopedia](https://www.investopedia.com/terms/f/fiatmoney.asp), “Fiat currency is money a government issues that is not backed by a commodity like gold. Fiat money is backed by the government and it has value because the government says so and the citizens believe it. The dollar is an example of the United States fiat currency”.



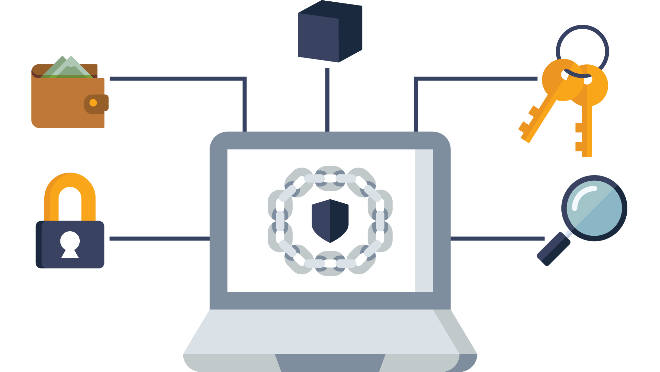
Apart from the government issuing Fiat, a centralized authority needs to keep track of assets. Banks, credit card companies’ stockbrokers are companies that represent a centralized authority that controls your money.



Bitcoin is transacted over the Bitcoin network, which is an open, public blockchain network. If you have an Internet connection and a Bitcoin wallet application, you can receive and send the cryptocurrency Bitcoin. Cryptocurrencies like Bitcoin have value because it can be proven with math. Unlike banks offering centralized services, you are responsible for your cryptocurrency.



[Bitcoin](https://bitcoinfoundation.org/) and cryptocurrencies are great use cases for blockchain, but they are just one component of the technology. Some privately run blockchains do not use cryptocurrencies as a function of their blockchains. Blockchain technology can easily transfer anything from property rights, stocks, and even artwork. There are many more use cases that utilize blockchain technology far reaching than currency transfer.



## Blockchain - Let’s Cover the Basics

In this section, we're gonna talk about what blockchain is: a real simple introduction to the basic concepts and principles behind blockchain.

When you hear about blockchain, you probably think of new, high-emerging tech.

Well, really, all blockchain is, is a combination of technologies that have existed for a long time.

They're simply combined in a new and creative way to give us an amazing new platform on which we can start to build solutions.

Blockchains are often referred to as digital decentralized ledgers.

And when you think of that, all you can think of is something we're all familiar with: a simple notebook.

When we talk about blocks and blockchain, all we're really talking about is a page of data.

We fill up this page with any kind of data imaginable, and, while most of the time today, we're talking about recording financial transactions on this page, or this ledger, or this block, we can record any kind of data we want.

In fact, you can think of a block as being exactly like this piece of paper, in that the paper doesn't know or care what kind of information you're recording on it.

And just like the paper doesn't know or care, neither does the block in a blockchain.

So, while most of what we're recording today are financial transactions, we could also record things like voting records and results, land titling, medical records, or even the opening notes to a Beethoven symphony.

What makes this blockchain notebook incredibly powerful is that all the pages are linked together.

So that if I go back and try and change any data on any page anywhere in this notebook, I break a link in a very obvious and easy-to-determine way.

This gives blockchain a key property known as immutability.

And it's what gives blockchain the security that we've come to know and depend on.

Blockchains also give us an incredible technology called smart contracts, which allow us to programmatically define the rules and steps that should be performed any time a certain type of event is recorded in our blockchain or in our magic notebook.

So, when you think about blockchain, don't get intimidated thinking it's something high tech, and new, and cutting-edge.

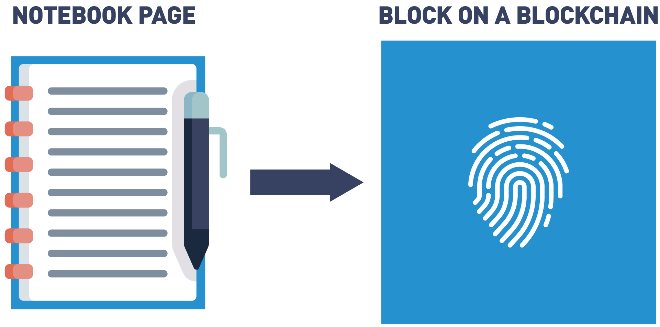
It's simply a new and creative way of combining old ideas together to give us an incredible new solutions platform.

And the rest of this series will take a deeper dive into these basic concepts and principles, but if the idea of this unchangeable linked notebook makes sense, congratulations!

You already understand all the major principles and concepts required to understand what blockchain is and why it's so powerful.

## Let’s Review an Analogy

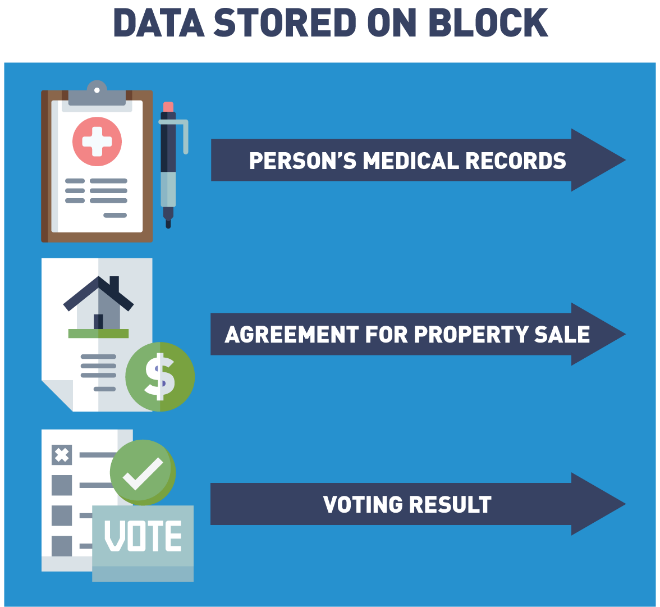
A block on a blockchain can be thought of much like a page in a notebook. Data is stored on a block, just like data is written on a page of a notebook. Similar to a sheet of paper, the digital ledger doesn't care what kind of information you're putting on it. So, while most of what we're recording today are financial transactions, we could also record things like voting records and results, land titling and medical records, etc. What makes this blockchain notebook incredibly powerful is that all the pages are linked together. So that if you go back and try and change any data on any page anywhere in this notebook, you break a link in a very obvious and easy-to-determine way.



## Let’s Review an Analogy: Data Stored

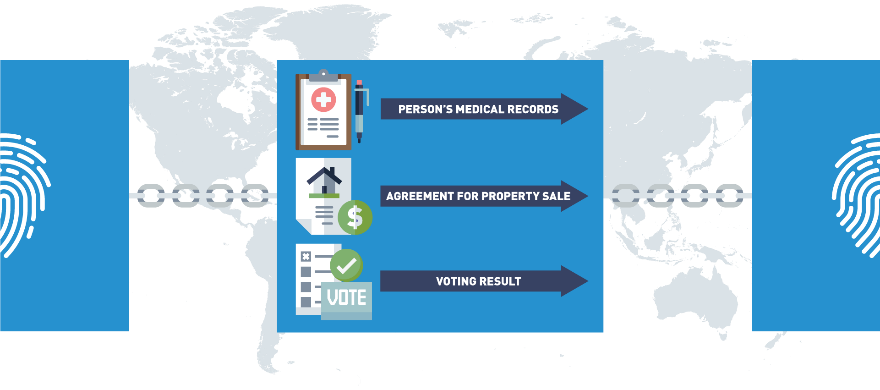
Any data can be stored on the same block. Examples of stored data include:

* Medical records
* Property agreements
* Voting



## Let’s Review an Analogy: Blocks Are Chained Together

Each block is chained or tied to the previous block by embedding the block with information from the previous block (we will go through this in depth later in the course).



## Let’s Review an Analogy: Blockchain Is Immutable

If the data is tampered with anywhere in the chain, the links will break in a very obvious way:



This provides immutability and security.

## Blockchain Features

Blockchain is a combination of several other underlying technologies that have never been combined so successfully. Here are some features that make this new technology so revolutionary.

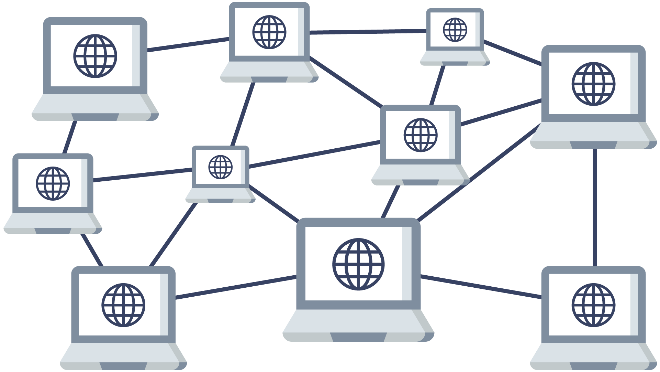
## Blockchain Features

## Blockchain Features: Distributed Ledger

A ledger is a collection of transactions. It is not a collection of assets. Assets are part of a transaction, but the ledger records the transaction. With a digitally distributed ledger or a blockchain, no one owns the ledger. The ledger is distributed among participants in the network, all running the same blockchain protocols. It is decentralized in that an identical copy of the ledger exists on every node/computer on the network. In 2009 with the publishing of Satoshi Nakamoto’s whitepaper [*“Bitcoin: A Peer-to-Peer Electronic Cash System”*](https://bitcoin.org/bitcoin.pdf) , [Bitcoin](https://bitcoinfoundation.org/) became the first application to leverage blockchain technology by recording the first asset transfer on a public blockchain ledger.

## Blockchain Features: Peer to Peer Network

The ledger is stored, updated, and maintained by a peer network. Nodes form the infrastructure of a blockchain network. They store, spread and preserve the blockchain data, so a blockchain exists on nodes. All nodes on a network follow the same rules of operation or protocols, but nodes have different roles. A full node contains a copy of the blockchain protocol, transaction history of the blockchain and aids in the maintenance of the blockchain. User node interacts with the ledger. With blockchain technology, a lack of a centralized authority is replaced with a peer-to-peer network.



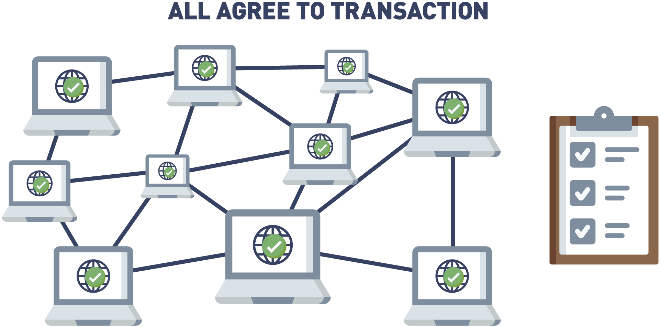
Blockchain networks can be public or private. A public blockchain is open to anyone with an internet connection and the appropriate application. A private blockchain grants access and rights to its users before they can interact.

## Blockchain Features: Transparency

In a blockchain, we can see all the transactions that have occurred on the shared or distributed ledger. A blockchain stores details of every transaction that occurred since the first transfer. This first transfer, along with some system information that we will discuss later, becomes the first block in our chain and is referred to as the genesis block. Since every node shares a copy of the agreed-upon ledger, there is no friction about the transactions, everyone has the same agreed-upon copy. Centralized systems are not transparent, the information about the ledger is controlled by one authority.

## Blockchain Features: Consensus

Blockchain ledgers are different from centralized ledgers because network participants have an agreement upon what is in the identical ledger. In order for the blocks to be added, all the nodes in the system come to agree as to what transactions are accurate and should be added to the chain of blocks. Since there is no central authority telling the nodes which transactions are valid, a new way to reach agreement or come to consensus is needed.



The way in which each blockchain comes to consensus is built into the protocol, they are the rules built into the code that determine how the nodes will add ledger transactions. The Bitcoin network uses a proof of work consensus model. This process of building agreement among a group of mutually distrusting participants is a benefit of blockchain consensus.

## Blockchain Features: Encryption

Encryption and cryptography are combined with blockchain technology to assure the information on the blockchain is authentic. In our previous real-world example, the music sharing companies not only had legal issues from copyright infringement, they also could not solve the data integrity problem. Music downloaded from these platforms was only as reliable as the anonymous person storing and sending it. The data had no integrity. Cryptography and blockchain offer a secure way to prove something is authentic. Instead of relying on third-party, trust is put into cryptographic algorithms that prove the provenance and authenticity of an attestation.

## Blockchain Features: Programable

Some blockchains offer an additional feature, smart contracts, that impose logic into the system. If you think of the Bitcoin blockchain as a calculator recording financial transactions, you can think of these blockchains as computers. The first of these blockchains is [Ethereum](https://ethereum.org/en/), created by Vitalik Buterin, Joe Lubin and team. Ethereum runs the EVM, Ethereum Virtual Machine, which has the ability to impose digital agreements or smart contracts. A smart contract is a program that runs on a blockchain that can impose contractual agreements. Typically, they work as digital agreements that enforce a specific set of rules. These rules are predefined by computer code, which is replicated and executed by all network nodes. Blockchain smart contracts allow for the creation of trustless protocols. This means that two parties can make commitments via blockchain, without having to know or trust each other. They can be sure that if the conditions aren't fulfilled, the contract won't be executed. Other than that, the use of smart contracts can remove the need for intermediaries, reducing operational costs significantly.

## Blockchain Actors (Career Opportunities In Blockchain)

With new technology comes new opportunities and this holds true for blockchain. As this nascent technology matures, more positions are needed to fill this increased demand. A few of these new positions are listed here:

Entry Level and Internship Positions  
Mentorship programs and internships include assisting in the designing and developing blockchain distributed ledgers based on both public and private or permissioned blockchains. With open-source, development and success depend on an active community, Working Groups and Hackatons are available for the newcomer. Skills include basic blockchain knowledge and some familiarity with basic programming languages.

Blockchain Architect  
For a blockchain solution to be functional, it first needs to exist. The blockchain architect is the person or group who designs and implements the backend code of the blockchain. The blockchain architect works with blockchain engineers and technical leaders to identify the blockchain structure for specific use cases. Architects understand consensus mechanisms, cryptography systems, key management techniques and smart contract management. Qualifications include Go, Java, Javascript, or any modern programming language plus project management skills.

Blockchain Developer  
Developers design, write and upload smart contracts to the blockchain. Developer design workflows that operate with blockchains and smart contracts. Responsibilities can include project design, smart contract development and implementation, front end applications design and application deployment. Skills a developer needs can include Microsoft SQL Server, Visual Studio, .NET, MVC, AJAX, SQL, C, Python, Solidity, C++, C#, Javascript, Node.js, JQuery, SOAP, REST, FTP, HTML, XML, XSLT, XCOD, Neural-networks, Regression, Agile Scrum, MYSQL. Solutions are developed for Hyperledger Fabric, Ethereum, Quorum Ripple, Corda and other distributed ledger solutions.

Blockchain Operator  
Once the blockchain solution is designed and built, operators can join to create the peer network mentioned previously. The role of operators (nodes) is to store copies of the ledger and keep their copy up to date by distributing transactions and new blocks throughout their network via peer-to-peer communications.

Blockchain Regulator  
Many businesses operate under regulations regarding how their data should be stored and processed. This is the same for blockchain solutions. Regulators rarely interact with the blockchain directly, rather oversee regulatory requirements that need to be considered in blockchain development. With governments researching Central Bank Digital Currencies, governing these blockchains will become increasingly more complex.

Blockchain Project Managers  
Project managers are the first persons in an organization who are contacted when a company wants to bring blockchain in house and adapt it to their technology platforms. Responsibilities include deciding if a blockchain solution is a good fit for a business situation. If the decision is to move forward, Project Managers would organize key players and resources needed to execute the blockchain project.

Data Storage and Processing Managers  
The blockchain provides distributed, immutable storage with built-in integrity checking, but certain limitations exist that have to be managed. Data decisions need to be made dealing with maximum capacity based on the standard block size and block rate. Policies need to address how to provide integrity verification for large amounts of data, should data be stored off-chain with a hash of the data stored on-chain. eMembers of the peer network must execute the code to remain in sync with the current state of the network. If smart contracts commonly require large amounts of processing power to complete, devices external to the peer network may be used to augment the processing power of the network.

Blockchain Data Scientists  
Blockchain has the ability to collect large amounts of data. The Blockchain Data Scientist collects, interprets, analyzes and manages data. Developing algorithms that can analyze patterns in large data sets, the data scientist provides insight into the data collected.

Blockchain Quality Engineer  
This position is responsible for ensuring quality in all areas of blockchain development, such as automation frameworks and tests, manual testing and dashboards to support mobile, web and platform engineering. A quality engineer will need to research and advise on blockchain tools and develop quality assurance (QA) automated test standards, as well as define, write and implement test automation strategies for load performance tests. Applicants may also need an engineering management MBA degree.

Blockchain Legal Consultant or Attorney  
A blockchain legal consultant is responsible for advising companies on how to structure blockchain endeavors. Advise on how to structure and govern initial coin offerings, some of which are now coming under greater regulatory scrutiny. Attorneys will also be tasked with developing legal partnerships and contracts as blockchain technology offers "smart contracts", which are self-executing based on previously agreed terms. Duties can include designing legal partnerships that would connect the crypto ecosystem with existing financial structures, and supporting various merger-and-acquisition activities, such as negotiating and drafting legal agreements and performing due diligence on blockchain projects.

Blockchain Web Designer  
A decentralized community needs to keep the community that supports it informed. When including the use of cryptocurrencies in your business and when launching blockchains, there will be a greater need for websites to inform customers what a company is offering. A blockchain web designer will need to come up with original concepts, creative graphics and "mind blowing" user interfaces and dashboards to engage a diverse and inclusive community.

Blockchain Consultants  
Blockchain consulting companies and blockchain consultants are tasked with advising companies on designing and implementing blockchain solutions. This includes the documentation and maintenance of solutions, as well as their initial implementations.

NFT Graphics Designer  
NFT stands for a non fungible token, a special token that represents a unique ID that is linked to a piece of crypto art that cannot be replicated and is used to verify ownership of a piece. The collectable world is jumping in head first and creating non fungible tokens that represent art, music, memorializing events, newspaper articles and record releases. Designers are needed to turn these moments/media into art for the thirsty NFT market.

## Who Is Using Blockchain?

There are a lot of really interesting use cases being explored with blockchain right now.

When you first get into blockchain, one of the areas you'll see people immediately jump to are healthcare, how can we manage our personal health information on the blockchain, and voting an election reform, and both of these are really, really interesting ideas.

The goal behind the folks looking at blockchain for healthcare is the idea that it would be great if your medical records could be accessible with your permission to anyone else, anywhere on the planet.

If you're halfway across the world on vacation and you fall ill and end up in a hospital, wouldn't it be great if the doctor treating you had full insight into your medical records, knew any allergies you had, or knew any prescriptions that you were already on?

That's a very, very big area, and this ties a lot into blockchain and Identity Management.

How do we safely identify and protect people's personal data on blockchain?

A lot of interesting challenges there that are being worked out...

Blockchain for voting and election reform is a big topic right now, especially with all the conversation lately about how do we ensure the integrity of elections and demonstrate that our results haven't been tampered with or altered.

This is an area where blockchain could add a lot of value.

And then, of course, we hear a lot about traditional use cases, areas that are getting a lot of traction in blockchain right now.

Probably one of the biggest are supply chain, value chain relationships, which are very, very common in today's economy.

We have very, very few products or services that are offered completely and solely by one organization, without the involvement of other vendors, partners, suppliers, manufacturers, third-party organizations, etc.

Blockchain to track the supply, the origin of the goods and services that we consume is a big use case.

Walmart is really pioneering this right now with a blockchain solution that they're using to identify the provenance of meat, where does the meat that is sold in a Walmart store come from, and the ultimate goal here is that, when we do have contaminated foods, and we have to issue a recall, currently, because we just don't have good insight into that supply chain, we recall and destroy a lot more food than we really need to, which is tremendously wasteful, especially with all the people on the planet that we could be giving that good food to.

These are some real, real exciting areas that we see being pursued in blockchain right now.

On the public sector, there's a lot of interest in blockchain for law enforcement purposes.

How do we allow different law enforcement agencies at the federal, state, county, city level, all to share data seamlessly, in a safe, secure fashion, which also protects people's personal privacy and anonymity, when appropriate.

Another area where blockchain is getting explored and is generating a lot of excitement is with artists, with people who produce content.

If you're an author, if you're a musician, if you're an artist, traditionally, you've only been able to get your work out to the public, in the hands of the public, by going through a third-party intermediary.

If I'm an author, traditionally, the only way I've been able to share my creation with the general public has been going to a publishing company and getting my works published.

Blockchain enables lots of interesting scenarios where I can sell that work directly to consumers, create new subscription models, and this is having very interesting effects on the work itself.

One of the things we're seeing is that traditional book publishing, there's anywhere between 12 to 18 months delay between when the author finishes the last word of a book and when it actually ends up into the consumers hands.

Well, if we can use blockchain to enable consumers to purchase this material or subscribe directly to the content creator, we take that lag time completely out of it.

And this allows authors and content creators to do some really interesting things.

You could write a fictional story and have one of your characters respond real-time to a news story that actually happened last week.

It makes for very compelling reading and it's just something we're not able to do today in the traditional publishing world because of that delay.

We also see a lot of interest in blockchain for fractional asset ownership scenarios.

We know we're 10-15 years away from having self-driving cars be a very regular thing, and when we all get our own self-driving car, if we're smart, we're gonna have that car take us to work and then turn around and perform ride-sharing services throughout the day, when we're not using it, in order to recoup some of that investment.

Well, in a blockchain world with coins and tokens, we can fractionalize that asset ownership, and I can take that same money I used to buy one self-driving car which operates in one city, and I could buy one percent of a hundred self-driving cars in the hundred's biggest cities on the planet.

And so, if they're ever weather conditions, where maybe my car couldn't operate locally, that's okay.

I have a much more diversified investment, which continues to offer returns, because I have a virtual guarantee that any major city that I have one percent of my car ownership in is currently in rush-hour right now, in peak times of people needing a ride.

There are lots of very interesting use cases for blockchain in the real world right now.

I would encourage all of you to dig in a little bit more, and see some of the interesting things that are going on with blockchain in healthcare, in public sector, in insurance, in supply chain, value chain and more, see what other folks are doing, and then go out and make your own blockchain dreams a reality.

## Blockchain Users: Business to Consumer (B2C)

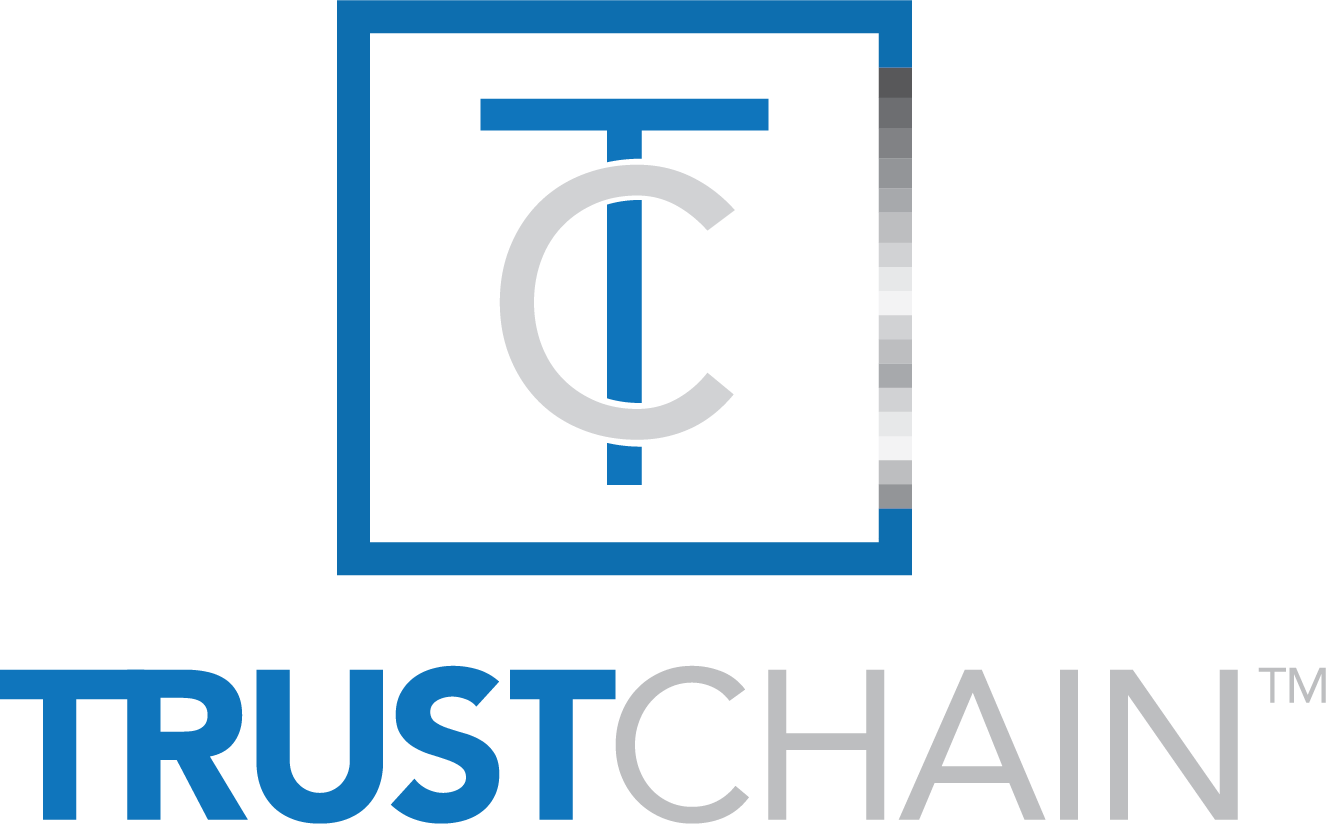
A Business to Consumer (B2C) is business or transactions conducted directly between a company and consumers who are the end-users of its products or services. Services being provided to the consumer is an area of interest to companies. Benefits to the consumer are transparency to the consumer, accountability from suppliers, ethical sourcing validation, labor verification and an immutable shared view.



Vertical markets see the advantage to the transparency feature in blockchain. Financials, logistics, charity funding, agriculture and ethical sourcing tracking are all markets leveraging blockchain to offer new insights to the customer.

## Real World Example of Supply Chain Business to Consumer

#### ****Use Case: Diamond Tracing****



Approach: The blockchain collaboration, known as [TrustChainTM](https://www.trustchainjewelry.com/), will track and authenticate diamonds, precious metals and jewelry at all stages of the global supply chain, from the mine to the retailer/consumer.

Result: The jewelry industry can now track and authenticate diamonds and precious metals through every stage of the supply chain. Blockchain provides physical product verification, process verification and servers as an ethical oversight.

## Blockchain Users: Business to Business (B2B)

With a decentralized approach, blockchain removes the middleman (such as banks and brokers) to facilitate faster and less expensive payments. The shared ledger approach also eliminates the need for multiple paper copies that need to be verified and updated frequently.



Industries like finance, international trade and commerce, food supply chains are taking a serious look at blockchain.

## Real World Example of Business to Business Transaction

#### ****Use Case: Multi-party Invoicing DLT Labs****



* *Approach:* [DLT Labs](https://www.dltlabs.com/) along with Walmart Canada initiated a tracking program tackling the enormous problem in the freight and shipping industry of dispute resolution in disparate invoicing systems. The solution connects all points on the supply chain with a shared trusted ledger. This eliminates the root problems that cause invoice disputes. The carriers are a vital link in Walmart's supply chain backbone, and the DLT solution ensures invoicing systems run smoothly.
* *Result:* Demonstrable transformation of freight management and carrier relationships by implementing a shared DLT invoicing system with trust and transparency build-in, reduces disputes among organization by 95%.

## Unintended Use Cases

One of the coolest things about blockchain is some of the unintended consequences a good blockchain solution might have.

Let's look at an example.

Right now, there is a lot of attention being given to how blockchain might be used, in general, for supply chain relationships and, specifically, in the food supply chain.

Let's pretend that you have a very young child and your child has a serious pesticide allergy.

Of course, when you go to the grocery store, you make sure that you only buy the produce in the produce section that has the USDA organic label.

It's just a little sticker that goes on the produce.

You buy your produce and you stand in the checkout line, and you feel pretty good that the produce you're buying actually is organic and has been treated with all-natural pesticides, and won't make your young child sick.

But sometimes you wonder, standing in line, how do I really know? How do I really know that someone didn't just print up a bunch of these stickers in their basement and apply them at the last minute?

The blockchain can go a long way to solving that problem and providing much greater insight.

Let's say, you're standing in the grocery store one day, and instead of the easily forged stickers, you're able to pull out your phone and scan a QR code.

When you scan that QR code, instantly on your phone the entire lifecycle of that piece of produce pops up.

You can see the date that it was planted on the orchard.

You can see after it was planted that an organic pesticide company came along and treated it with an all-natural pesticide.

You can even verify that the pesticide is natural by seeing the ingredient list in that pesticide.

And finally, you may see who actually delivered that produce to the store.

Let's say that there's a new green electric trucking company out there - Ed's Electric Trucking.

Ed has seen all the fancy new Tesla semis. He thinks they're great and he is committed to providing a transportation and logistics company which is also environmentally friendly.

Now, in today's world, you don't have a way of knowing about someone like Ed and his electric trucking company.

There just aren't good ways for folks in the B2B space to communicate their business value directly to consumers.

This is an interesting potential byproduct of using blockchain and smart contracts as a business solution.

Not only would I, as a consumer, have greater insight into the origin of that produce and feel much better standing in the checkout line, but maybe what Ed's doing resonates with me personally.

Maybe I'm a very green-conscious consumer.

I didn't know there was such an organization as Ed's.

And I have to buy a few more things while I'm at the store, besides produce. I have to buy some deodorant, some shaving cream, and some laundry detergent.

When I buy that deodorant, shaving cream, laundry detergent, I only buy the ones that were delivered by Ed's Electric Trucking.

This gives Ed and other B2B players a new and exciting way to establish brand and gain mindshare with the consumer that they currently don't have.

Certainly, it was not the original problem we went to solve with blockchain, but many times, when we apply blockchain to a real-world problem, we find out there are a lot of unexpected benefits just like this.

Look for blockchain not just to transform the areas that we're aware it might make a difference in, but also to provide some new exciting and unintended benefits.

## Blockchain Users: Government to Consumer (G2C)/Government to Government (G2G)

The public sector is the part of the economy composed of both public sector and private sector enterprises that are operating on behalf of the public. It is the business of taking care of the people. Public sector includes all government, military, police, public health and welfare, infrastructure, etc. Public sector organizations leverage blockchain technology to move away from siloed and inefficient centralized systems. Current systems are inherently insecure and costly, with duplicated and in-efficient workflows. Blockchain networks offer more secure, agile, and cost-effective structures.



## Dubai Use Case

So, when people first start getting into blockchain, one of the areas they really start to look at is where is blockchain being used in the real world, what examples do we have of a blockchain being deployed and at what scale.

And there's really no better example of this right now than what's going on in Dubai.

Dubai, the largest city in the United Arab Emirates, is piloting a very ambitious program called smart Dubai 2021.

And what Smart Dubai 2021 aims to do is to move all governmental operations and record-keeping on the blockchain by the year 2021.

The goals of this program are increased transparency in the government operations, increased efficiency, and by proxy, providing better service to city residents and constituents and establishing Dubai as a thought leader, an industry leader in the blockchain space.

There are lots of really cool applications that tie into this.

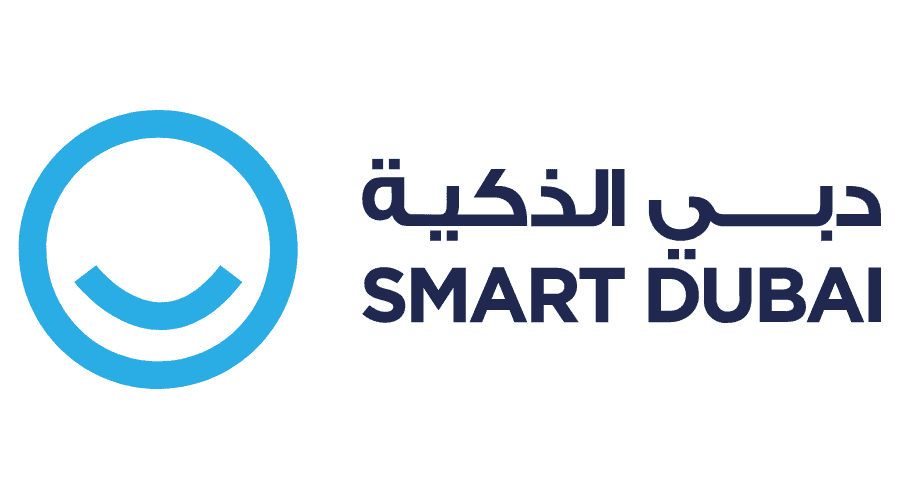
Blockchain is becoming the enabling layer for a lot of other Smart Dubai initiatives around creating a smart city.

So, projects like automated traffic signals, registration of citizens for governmental services, etc. are all being pioneered on blockchain.

So, if you want to see some of the really exciting use cases in blockchain right now, be sure to check out Dubai and what's going on with their Smart Dubai 2021 initiative.

## Real World Example of Public Sector Government to Government/Citizens

#### ****Use Case: Public Sector - Smart Dubai****



* *Approach*: To make Dubai the happiest city on Earth by recreating everyday experiences for residents and visitors of Dubai, making them more personalized seamless, efficient and impactful. The [Smart Dubai](https://www.smartdubai.ae/) strategy will be using three essential pillars: government efficiency, industry creation and international leadership
* *Result*: By the end of 2021, Dubai government will go completely paper-free, eliminating more than one billion pieces of paper used for government transactions every day. When successful, Dubai will be the first blockchain-powered government driving the future economy.

## More Use Cases

Blockchain is having far reaching effects in major industries. Let’s take a look at three major industries having a positive influence from this new way to organize our information:

* Supply chain  
  Blockchain is used in supply chains to gain transparency and traceability. This has a special advantage for global health when used in traceability to the food supply chain. By tracking food on a blockchain, you are building trust into the system through the transparency feature. In the event of a problem, blockchain technology can pinpoint the exact location and cause of a food health issue. By instantly tracing food issues back to the source, all contaminated lots can be tracked and dealt with instantly.
* Global trade  
  Blockchain is making headway in the global trade markets with transparency and immutability that offer new relationships among distrusting parties. Blockchain makes sure all relevant parties have access to the same information. Trade barriers are reduced, from settlement issues, to compliance and regulation, information is being shared and accessed in new secure ways. A distributed ledger technology (DLT) opens up a new avenue for securely sharing data that guarantees accuracy while removing banks as deal facilitators. Smart contract and microfinancing alternatives allow all size companies to seamlessly trade across borders.
* Digital identity (self-sovereign identity and verifiable credentials)  
  Users of the Internet were all but unaware that all the information given so freely when interacting with companies online, was being stored and sold. Data became a siloed commodity owned by everyone but you. With new blockchain technology, individuals can reclaim their identity information breaking the need for data silos, endless passwords and hackable databases. Self-sovereign identity (an individual identity holder controls their credentials and can use them without permission) gives secure identity verification designed to bring trust and personal control so people can prove things about themselves using trustworthy verifiable digital credential.

## Chapter Summary

In this chapter, we discussed:

* The history of the Internet and how blockchain technology relies on Internet technology as the foundation for building the future of the blockchain evolution.
* The difference between blockchain and Bitcoin.
* How blockchain functions.
* Blockchain concepts and characteristics: distributed ledger, peer to peer, transparent, consensus, encryption, immutability, programmable.
* Blockchain users and their roles.
* Emerging general use cases.

# [2. Blockchain Mechanics](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@chapter+block@90a929834b3b4bc18c6b3e7c662f152c) / [Introduction](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block-v1:LinuxFoundationX+LFS170x+2T2021+type@sequential+block@1088154e18e0450f9bb3a418121008c1)

## Chapter Overview

In this chapter, we will discuss distributed ledger technology, some of its basic components and how it differs from previous ledger storage techniques. We will gain an understanding of how previous computer technologies like file sharing, data storage and cryptography are wrapped into the blockchain foundations. We will also see how hashing functions and Merkle tree data structures help us immutably store and prove facts without revealing all the details.

Next, we will learn how these blockchain techniques are fundamental in public-key cryptography where key pairs support privacy and authenticity by only exposing the public key while keeping the private key secure. We will examine how this agreed-upon, append-only distributed ledger guarantees transparency and immutability, where trust in the information contained in the ledger is a given.

## Learning Objectives

By the end of this chapter, you should be able to:

* Discuss how cryptography allows for distributed ledgers to work on a global scale.
* Explain how blockchain is using cryptography.
* Define key terms of cryptography and understand basic concepts.
* Explain the concept of zero-knowledge proofs (ZKPs) and Merkle trees and how they are used in blockchain technologies.
* Discuss how blockchain utilizes transparency.
* Explain what it means for blockchains to be immutable and how chaining provides this capability.

## 2.1 Introduction to Blockchain Components

In this section, we're going to discuss the core components of the blockchain, starting with a high-level view of the blockchain components.

The first blockchain component that we're going to look at it's the ledger.

However, before we discuss the ledger, let's discuss briefly the history of the ledger.

The story of blockchain is tightly coupled with the story of accounting.

Historically, humans started off with no way to prove ownership and we began with a single entry accounting system.

The single entry accounting system for the first time in human history allowed us to prove ownership of the asset.

The ledger was associated with an owner.

The single entry accounting worked for centuries.

The issue with single entry accounting is that it mandated that there was a single authority, which is the reason why there was the necessity for a king or a queen to control the ledger.

In order to have trade, right, at the international level, we needed to have at least two authorities.

For instance, for England to do trade with France, we had the owner of the ledger, the single entry ledger, in England for instance, doing trade with the king or queen of France, who also had their ledger.

And so, we needed a new form of accounting, and that's where double entry accounting came in, which was in use up until very recently, now, within the last 40 years.

What blockchain is? Blockchain is the very first implementation of triple entry accounting, where we have an asset being recorded on the ledger in the context of a transaction.

The third entry and triple entry accounting is cryptography, where we have a cryptographic account of the transaction stored permanently and immutably on the ledger.

That's what the ledger is. A ledger is a collection of transactions.

It is not a collection of assets. Assets are part of a transaction, but the ledger records the transaction.

In blockchain, the differentiator is that no one owns the ledger, or all of the participants own the ledger.

The ledger is distributed. It is, in other words, it's decentralized. So, there's a copy of the ledger that exists on every node that exists on the network.

Said simply, the ledger is a distributed immutable record of a collection of transactions.

Bitcoin is the most popular asset.

It was the first asset to be recorded as a transaction on a blockchain ledger, and it remains the most popular, at least in terms of market share.

That's what the ledger is.

As we move to more modern blockchains, we start to look at blockchains such as Ethereum, which not only records the asset on the blockchain,

Ethereum and other public blockchains like Ethereum, they also allow you to have a permanent and immutable collection of code, also known as a smart contract, that runs on the blockchain.

The ledger stores the assets, the transactions that are on the blockchain, and it also holds the code.

The code that's stored on the blockchain is a smart contract.

Again, a smart contract is a program that runs on the blockchain.

The blockchain is a network.

The blockchain is a ... A public blockchain is equivalent to the Internet, complete with its own set of protocols, etc.

Private blockchains are more synonymous with an intranet.

It is... just like we have a use case for public blockchains and public internet, we also have use cases for private blockchains and an intranet, if we're gonna stay with that analogy.

On each of these networks there are nodes. The nodes are going to be synonymous with the computers that make up the network.

On the nodes, they are put together by a collection of protocols.

Each blockchain has its own set of protocols that defines not only the nodes, but how those nodes communicate with each other.

So, when you hear the term "peer network", that's what we're talking about; we're talking about how that blockchain is put together, what are the protocols that define the peers, and how those peers interact.

Those peer networks, they store the ledger, they provide the updates, they effectively, they maintain the ledger.

That's what a peer is on a peer network.

On a public blockchain, it's public, and, by definition, that means that anyone is allowed to join and participate in that public blockchain.

On the private blockchain, however, the situation is a little different.

On the private blockchain, we have to control who can access your network.

Just like no company would allow... no company would allow anyone to access their private intranet, in a private blockchain you have to be asked to join, or you have to have permission to join.

A membership service is a gateway that allows users and components to enter a private blockchain.

A membership service or a membership service provider provides the services of user authentication, user authorization, component authentication, component authorization, more specifically Identity Management.

If we're talking about a private blockchain, then we have to control who the members are, and not only the members.

We have to also control the nodes that access the blockchain.

As we're talking about membership, one of the key components of membership is we have to allow certain users to access the blockchain.

In order to do that, we have to have a definitive identity for each user.

In the blockchain, that's achieved in two ways.

One, we use PKI, to provide a public key. And that public key represents the identity of the user.

But we also need a private key that each user can hold to prove their identity.

That private key is stored in a wallet. And a wallet is a collection of the user credentials. It is effectively ... it encapsulates private keys.

Additionally, in the blockchain... blockchains are self-contained, or they should be self-contained.

And so, one of the key aspects for developing on a blockchain or using a blockchain is we have to have a way to interact with the blockchain.

And one of the ways that we do that is through events.

So, when something occurs on the blockchain, either public blockchains... most public blockchains anyway, and certainly all private blockchains, they have events that are fired when certain key actions are triggered.

This allows end-users, other systems, other users, different components to be able to act off of the events that come from an update on a blockchain.

## Basic Terms

Some terms that are mentioned in the video we will get familiar with in later chapters, but are worth a brief description for clarification:

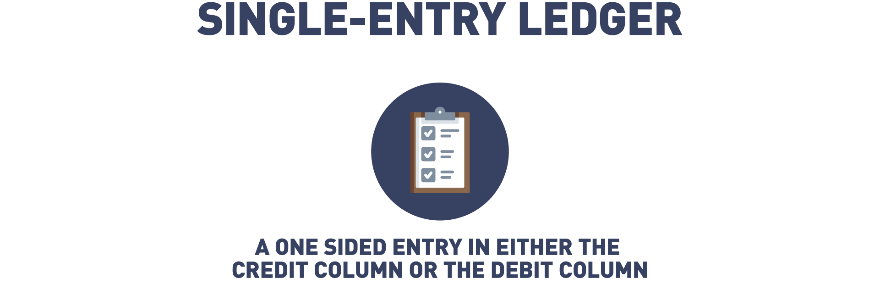
* *Ethereum*  
  Ethereum, like Bitcoin, is a decentralized open-source blockchain. Unlike the Bitcoin Network, the Ethereum Protocol has the ability to run smart contracts. The cryptocurrency running on the Ethereum network is called Ether.
* *Smart Contracts*  
  A smart contract is computer code that can be run on a blockchain that executes the conditions of an agreement.
* *Public Blockchains*Public blockchain has no barrier to entry. Anyone with a cell phone and a digital wallet can transact on the blockchain.
* *Private Blockchains*  
  Private blockchains or permissioned blockchains have a Membership Services piece that grants access to users before they can interact with the blockchain.
* *Digital Wallet*A digital wallet is a computer application that represents a traditional wallet. It gives the user the ability to store and transact cryptocurrencies through the Internet.
* *Public Key Infrastructure (PKI)*  
  Public Key Infrastructure is the identity management system for instilling trust into the electronic transfers of information or value. It is the technology used to authenticate users and information by issuing a set of key pairs (public and private).

## 2.2 Understanding Ledgers and Basic Accounting Systems

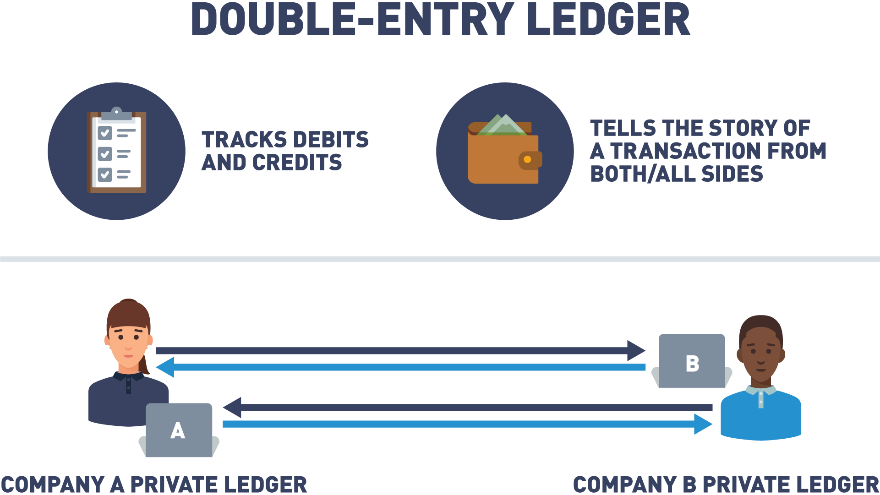
To understand how blockchain came about, we must first understand the following key principles:

* Ledgers
* Basic accounting principles in history

## History of Ledgers



* Ledgers first appeared around 3,000 B.C.
* Single-entry only.
* Chanakya, an Indian leader, creates the first documented accounting standards.



* Double-entry ledger appears in 1340 A.D.
* Tracks debits and credits.
* Tells the story of a transaction from both/all sides.
* The Italian Luca Pacioli, recognized as the father of accounting and bookkeeping, was the first person to publish a work on double-entry bookkeeping and introduced the field in Italy.



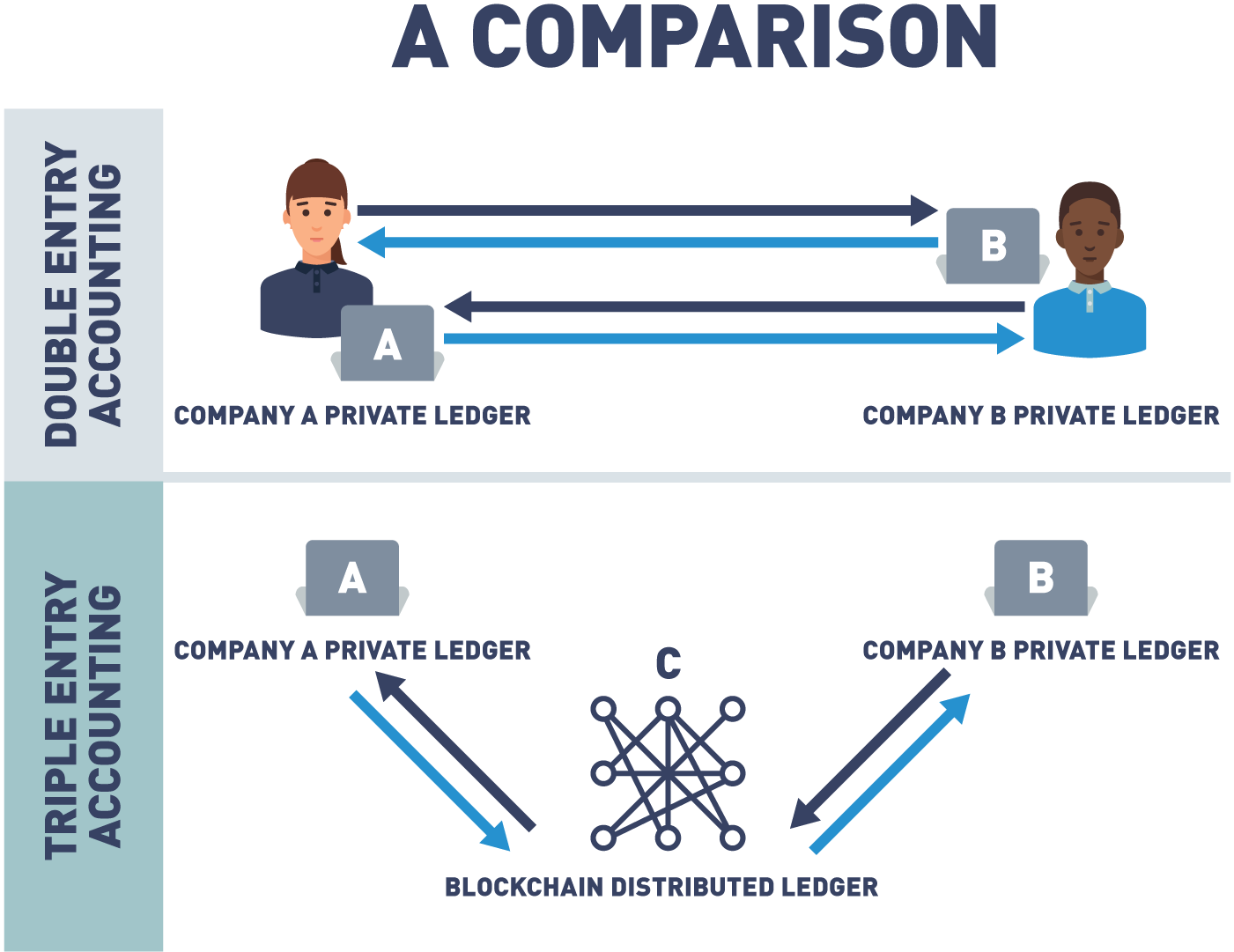
* Triple-entry accounting is an enhancement to the traditional double-entry system, in which all accounting entries involving outside parties are cryptographically sealed by a third entry.
* Debits, credits, and an immutable link to all past debits and credits.
* Triple-entry ledger appears in 2008 in a white paper by Satoshi Nakamoto (a.k.a., Blockchain).
* Some features include: tamper-proof records, distributed ledgers, double-entry+cryptography, validated, secure, and private, digitally signed receipts.

## History of Ledgers (Triple-Entry Example)

As described in the [Reddit post](https://www.reddit.com/r/Accounting/comments/2biy4h/triple_entry_bookkeeping_using_cryptocurrencies/),

"A seller books a debit to account for cash received, while a buyer books a credit for cash spent in the same transaction, but in separate sets of accounting records. This is where the blockchain comes in: rather than these entries occurring separately in independent sets of books, they occur in the form of a transfer between wallet addresses in the same distributed, public ledger, which creates an interlocking system of enduring accounting records. Since the entries are distributed and cryptographically sealed, falsifying them in a credible way or destroying them to conceal activity is practically impossible".

## Double vs. Triple-Entry Accounting Comparison



## Island of Yap

Idea for the following was obtained from the LinkedIn article [*"Explaining Blockchain: The Distributed Ledger of the Island of Yap"*](https://www.linkedin.com/pulse/explaining-blockchain-distributed-ledger-island-yap-riva/) by Anthony (Tony) Riva.

The concept of distributed ledge's has been around for hundreds of years.

To understand the basics of blockchain, it's important to understand how distributed ledgers work.

A distributed ledger is a collection of data with no central administrator that has been agreed upon by consensus.

To understand more details, let's take a trip way back, back into 500 AD on the island of Yap.

The Yapese people used a very unique form of currency: the Rai stone.

Each of these stones weighed around 200 kilos, making them difficult to move.

To exchange them as money for goods or services, they divided the stones into sections and then, they would announce to every adult on the island who owned what part of each stone.

Each adult had to keep a mental ledger of ownership.

Every time any Yapese conducted a trade, an announcement was made to the entire tribe.

Each member of the tribe would then update their mental ledger.

In today's description, this would be called a distributed ledger.

All Rai stone ownership was known to everyone, and that knowledge was updated whenever a transaction was made.

So why didn't just one member of the tribe keep track of the Rai stones?

What if that main recordkeeper was sick, unable to do their job, or was found to be dishonest?

If the only copy of the ledger was changed by any means, wealth would be lost or gained unfairly.

The Yapese knew their distributed ledger system safeguarded it from tampering.

Since all the Yapese knew who owned what, it would be very difficult to fool everyone on the island.

Even if one tribe member moved away, the tribe still had multiple copies of their mental ledger.

In this regard, the ledger was fault tolerant and could not be easily changed, corrupted, or lost.

The tribe also decided that stones didn't have to be on the island to hold value.

One day, a stone fell into the ocean and the Yapese decided that this stone, even though it could not be seen, still held value and could still be traded.

This system of consensus by the majority of the adults on the island with no central administrator is one of the first examples of distributed ledger.

## Island of Yap: Recap



The group shared the ledger.



The group agreed to the ledger.



 All changes or transactions to the ledger were announced to the group.



The group agreed to update all ledgers.

Let's review an example on Yap Island:

Alice agrees to trade Bob her stone by the pond in exchange for all of his cattle.

Alice and Bob announce their transaction to the tribe.

Everyone updates their mental ledger.

From this point on, they agree that the stone by the pond is owned by Bob.

## Island of Yap: Corruption Is Near Impossible

Alice tries to corrupt Carol, so that Carol’s ledger shows that Alice never gave up ownership of the stone.

* Centralized ledger, only one place to cheat.
* Decentralized ledger, Carol will be outvoted by the rest of the tribe, and her version of the ledger will not be accepted.

If Alice wants to cheat, she will need a way to convince 51% or more of the tribe to accept an alternative ledger.

## The Evolution of Distributed Ledgers

We've gone through history and seen how ledgers have evolved from stone tablets to double entry ledgers.

We even took a look at the earliest known example of distributed ledgers.

Now, let's discuss the evolution of the ledger in the modern world.

Over the last few decades, ledgers have moved from the written form to the digital form, also known as computers and digitalized databases.

This has allowed us to be interconnected - a truly global economy.

Today, this recordkeeping system is being revolutionized again, going from the digital realm or centralized databases keeping track of transactions to information being stored across different locations across the globe.

This system of record, information across a global network, is what we call decentralized ledgers.

A decentralized ledger can be described as a ledger of any transactions or contracts supported by a decentralized network from across different locations and people, eliminating the need of a central authority.

When a recording is made, every participant is notified of that recording.

They now own an identical copy of the record of transactions, identical to every other node on that network.

Every piece of information on a blockchain can be traced back to the exact moment when it was created.

So, if an audit is necessary, information can be found and deemed reliable.

This allows blockchain to serve as a truly reliable storage of public records and transactions, and therefore eliminating the need for a centralized authority of database of records.

Now that we understand the foundational principle of blockchains - distributed ledgers, it's important to understand another important key element that makes blockchain so revolutionary: trust.

Trust is created through two key principles: collaboration and cryptography, both of which will be discussed shortly.

## Decentralized Ledger

As we can see by looking at the evolution of the ledger, we are entering a new phase where no one centralized authority has control of the details in the ledger, everyone does. Transactions are only added to the ledger if everyone agrees. Once consensus is reached, no one can go back and deny a transaction. So essentially you are not trusting one person or entity to control the ledger, you're trusting everyone. Let's look a little further into how that trust is achieved.

## 2.3 From Distributed Ledgers to Cryptography

A great way to think of blockchain is to think of blockchain as another layer of the Internet, a layer that enables secure and trusted records and transactions to occur, which is why a lot of people associate the word blockchain with the word trust.

Blockchain creates a layer of trust between untrusted parties.

Without blockchain to create trusted records and transactions, a third party intermediary is necessary.

Blockchain eliminates the need for a centralized institution to act as intermediary, and instead uses cryptography and collaboration to create that trust.

In an earlier chapter of this course we spoke about collaboration through distributed ledgers.

Now, we will be taking a further look at how cryptography is used in blockchain to create the second element necessary for blockchain to be a source of trust.

Information on the blockchain is stored on the ledger using cryptography.

It can be accessed using keys and cryptographic signatures.

Now, let's take a look into some of the key concepts of cryptography that are utilized with blockchain.

## Rose Greenhow

So, one of the reoccurring themes in blockchain is that while blockchain itself may be new and cutting-edge, it's built out of nothing more than very old tried-and-true technology.

And one of the areas this is most true is in cryptography.

When a lot of people first get introduced to cryptography they think it's a very new cutting-edge science.

And while there are new developments being made everyday, cryptography itself is a very, very old science.

One great example of this is the story of Rose Greenhow.

Rose Greenhow lived in the Washington DC area during the Civil War, and she was actually an undercover spy for the Confederate Army.

Rose Greenhow was a wealthy socialite, and she threw many fancy, elaborate parties, and was also invited to many, many high-end social events.

Many of these events were attended by members of the Union Army, generals and strategists, who Rose pretended that she didn't know much about military strategy and wasn't too interested in the war in general.

In secret, at all these events she was soaking up all the information she could.

Rose actually developed her own method of encrypting data.

She came up with her own encryption scheme and she used this scheme to mail letters down to the Confederate Army, revealing the plans of the Union Army, troop positions, general high-level strategy, etc.

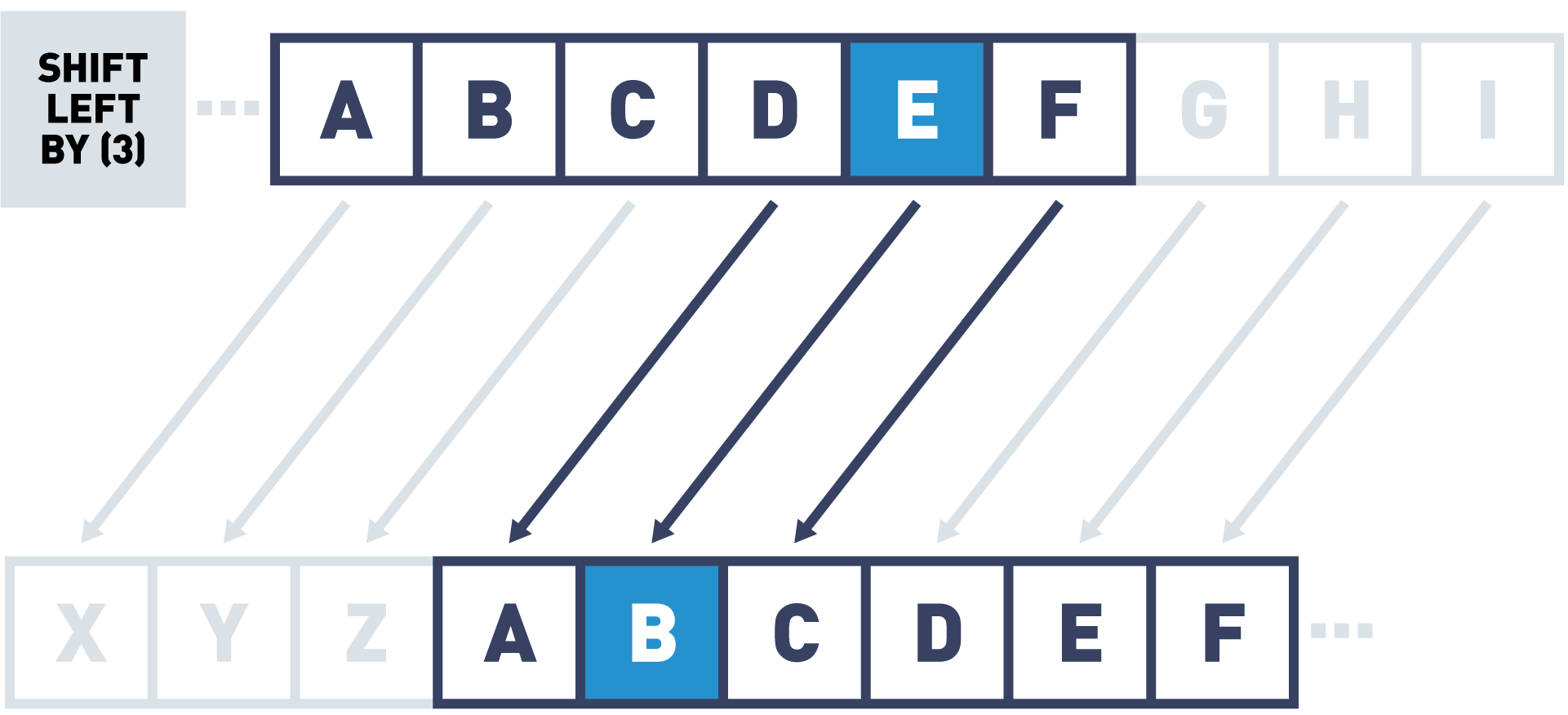
Rose did this for a number of years, until finally her encryption method was broken and she was actually one of the very first people who were arrested and prosecuted by the Pinkertons, who later went on to form the Secret Service.

So, when you hear about blockchain and all the new cutting-edge things that it's doing, don't forget that it has its roots in very old technology, and we're just combining old technology in new and creative ways to create a brand new solutions development platform.

## Early Use of Cryptography: Caesar Cipher

As described in the [*"Ancient Uses of Cryptography: Four Examples that Pre-Date the Internet"*](https://medium.com/tokenring/ancient-uses-of-cryptography-four-examples-that-pre-date-the-internet-14679ae4f509) article by Melanie Shapiro,

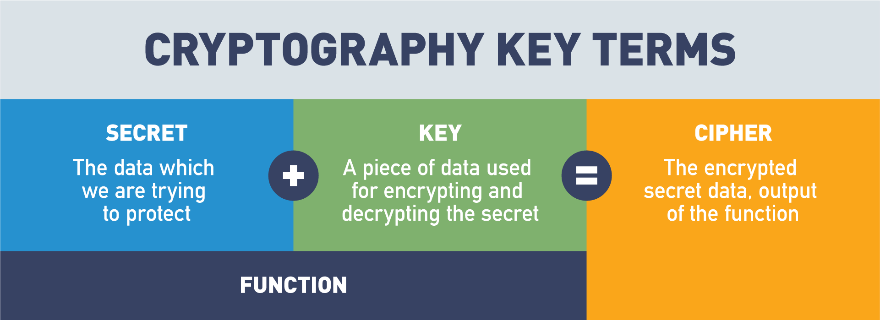
"A little over 2,000 years ago, Julius Caesar developed a simple system to send secure information to his troops. It was all about substituting certain letters for others, typically by shifting the letters by a predetermined number. That algorithm is what we would call a cipher, and since Caesar’s invention, cipher keys are much more secure and advanced. If you want to encrypt and decrypt information, you are going to have to choose a kind of cipher to do so".



## Cryptography Key Terms

Let's explain the key terms used in cryptography:

* Cryptography  
  Cryptography is a technique used to secure the communication between two parties from a third. The term cryptography is derived from two ancient greek terms, “kryptos” which means “hidden” and “graphein” which means “to write”.
* Secret  
  The data which we are trying to protect.
* Key  
  A piece of data used for encrypting and decrypting the secret.
* Function  
  The process or function used to encrypt the secret.
* Cipher  
  The encrypted secret data, the digital secret, the output of the mathematical function or a cryptographic algorithm.
* Encryption  
  This is the process from plain text (ordinary text) to cipher text (random sequence of bits).
* Decryption  
  Encryption is the reverse process of converting ciphertext into plain text.



 The Secret and the Key are passed into the Function to create the Cipher.

## Cryptography Basics

So, one of the technologies that plays a pivotal role in blockchain and making blockchain secure and immutable is cryptography.

If you've never heard of cryptography before, cryptography is simply designed defined as the science of sending messages back and forth from one party to another, in the presence of adversaries or bad actors, participants who may wish to corrupt or change the contents of a message.

And there's some key concepts you should understand about cryptography before we really dive in and talk about how cryptography protects the data on the blockchain.

Most cryptographic functions are what we refer to as two-way functions, meaning that we can take a secret and we can encrypt it, and then we can use that same process to decrypt the secret at the other end.

Some of the key objects or concepts to be aware of in cryptography:

first of all are the secret, what data are we trying to protect, what is the message we're sending back and forth that we want to do so in a safe, secure fashion, and try and guarantee that it hasn't been tampered with.

We take our secret and we combine it with a key, a piece of data that is consumed by a function, our third component.

When the function receives the key and the secret, the function uses the key to change the data in the secret, to create the fourth and final component, which is known as the cipher.

And the cipher is simply the encrypted message, the thing that, if it were intercepted, if it were seen by anybody else, any non-participants or bad actors, they wouldn't know what the secret was, they wouldn't know what the message was, and they wouldn't know how to decrypt that cipher back into the secret.

Now again, most cryptographic functions are two-way, meaning it doesn't do me a lot of good to encrypt data if the receiving party at the other end can't decrypt it.

And oftentimes, all this involves is using the same key or a reverse key into the same function, with the cipher's input to get the secret back out.

So, when we talk about cryptography, keep in mind those four basic components: the secret, the key, the function, and the cipher.

Then, understand that cryptographic hashing is a very special class of cryptographic functions, which, unlike all their cousins, are only one way, meaning that in a cryptographic hash I can put information or a secret into it, the key and the function are contained as one entity, and what I get back out is encoded data.

I get what's called a hash or a hash result, that is an encryption based on the data that I put in.

That is mathematically impossible to reverse-engineer and this is what makes it a one-way function.

If you put any data into a cryptographic hash and you share that hash with me, there's absolutely nothing I can do above and beyond random guessing to try and recreate that input to tell me what your original secret was.

Cryptographic hashes are used in scenarios where we want to prove a piece of data without sharing that data.

So, password management systems use this all the time.

We don't want to store a username and password…we want to store a username and the hash output of a password.

That way, I don't know what any of my users' passwords are, but I do know that if they put the wrong password in, they're going to get the wrong hash back out, and I can easily validate that a user's password is correct or incorrect, without having to know what it is.

We're going to dive in a lot deeper in a later module, to show you exactly through a demo how cryptographic hashing works, and how it provides security and immutability on the blockchain.

But just understand these two big takeaways:

Number one, that cryptography is normally a two-way function with four components: the secret, the key, the function, and the cipher, and then finally, there are a subclass of cryptographic functions called cryptographic hash functions, which exist as one-way functions, which can only encrypt the secret, and again, which are mathematically impossible to decrypt the secret in any other method other than randomly guessing input until you're able to recreate that hash output.

These are key components which enable security and immutability on the blockchain.

## Cryptographic Functions

Simple example function:

* Secret = "Blockchain technology is transformative"
* Function = Swap each letter in the secret with a new letter according to the Key
* Key = "+2"
* Cipher = "Dnqemejckp vgejpqnqia ku vtcpuhqtocvkxg".

As mentioned in the [*"Ancient Uses of Cryptography: Four Examples that Pre-Date the Internet"*](https://medium.com/tokenring/ancient-uses-of-cryptography-four-examples-that-pre-date-the-internet-14679ae4f509) article by Melanie Shapiro,

"(...), in the 1970s cryptologists [*Whitfield Diffie and Martin Hellman*](https://news.stanford.edu/2016/03/01/turing-hellman-diffie-030116/) made a landmark invention: asymmetric key encryption. It’s the concept that both HTTPS (the popular protocol used to access a secure web server discussed previously) and the secure element within a token rely on to keep your information completely private.

The principles behind it are genius. Instead of a shared key that codes and decodes information, the key for encrypting the information is different from the key that decrypts it — that way there is no longer a shared, secret key. With this invention, in order to share a secret message, you no longer even have to know the person you are sending it to. Most importantly, for people like us who care deeply about safe authentication and identity protection, the private key itself is never communicated at all, and that means no more shared secrets".

## Byzantine Fault Tolerance

As you start to get more and more into blockchain, one term that you're gonna hear a lot is Byzantine Fault Tolerance.

And if you're wondering what that means, that very strange, cryptic sounding term, that can be explained with a story.

In 1982, a mathematical problem was formulated called the Byzantine Generals Problem, and without getting too detailed into the mathematics behind it, essentially, with the Byzantine Generals Problem was a story about two empires fighting a battle.

One Empire exists within the confines of a walled city, the second Empire has several generals surrounding that walled city, each with their armies waiting to attack.

And the balance of power is very, very evenly matched between these two empires.

And it is such that if all the generals agree to attack at the same time, they will have enough power to overcome the empire in the city and win the campaign.

If they, for whatever reason, they're not able to coordinate their attacks simultaneously, and even one general misses the message, well then, the Empire surrounding the walled city is going to lose the campaign and the war.

So, the Byzantine Generals Problem explored a really key area of cryptography, in fact, the heart of what cryptography is, which is how do I exchange messages with someone in an environment where they may become corrupt.

You have to understand the only way these generals had to communicate was to send a disguised messenger through the city with a message to deliver to the other generals, and so, this always posed the risk, if you're a general and you're getting amessage from one of these messengers, how do you know or how can you believe with greater than random certainty that the message you're getting is reliable and it hasn't been tampered with.

And this, again, was a problem that was postulated back in 1982 and went unsolved until 2008, when the anonymous Satoshi Nakamoto proposed a solution to this problem.

Essentially, what the solution entails is all of the generals hiring as many mathematicians as they can.

When we talk about Byzantine Fault Tolerance, we're talking about the generals having more access, having more mathematicians, or more computing power on their side than the empire within the city.

So, if I'm the generals and I can hire more mathematicians, then that means that I can encrypt my messages going through the city with greater and greater complexity, and if the balance of power becomes greatly tipped in the favor of the generals outside the city, they can use encryption methods which are so complex, that there really is no real chance, or a very small chance that any of the mathematicians inside the city will be able to intercept that message, decrypt it, change the contents, re-encrypt it, and do so in a time quick enough that the generals don't notice anything has happened.

And so, this is Byzantine Fault Tolerance.

This is the fault tolerance mechanism that we see used in most public blockchain solutions right now, including Bitcoin, including Ethereum, although Ethereum is working on transitioning to a system called Proof of Stake, which we'll talk about in a later section.

But, when you hear Byzantine Fault Tolerance, often abbreviated as BFT, all we're talking about is this idea that blockchains become secure if they have more computing power, more hash power in the chain than off the chain.

Solutions like Ethereum, 16,000 plus nodes, or Bitcoin, the largest blockchain network that there is, with over 30,000 nodes, offer us a high degree of security and immutability, because the computing power on those networks is so great that there's really no reasonable chance that an adversary could ever control as much or more computing power to attack the data on that blockchain.

And if someone ever were to, chances are the economics behind it would be such that they would spend more to simultaneously harness all that computing power, than they could possibly stand to gain.

And so, this is Byzantine Fault Tolerance.

It is the root of cryptography, which is simply the study of how do we send information back and forth securely in the presence of adversaries and bad actors, and it's what underlies all the security and immutability that we get in blockchain.

## Types of Cryptography in Blockchain

To understand cryptography in blockchain, you must be able to differentiate between various cryptographic techniques used. There are four main ways blockchain leverages cryptography:

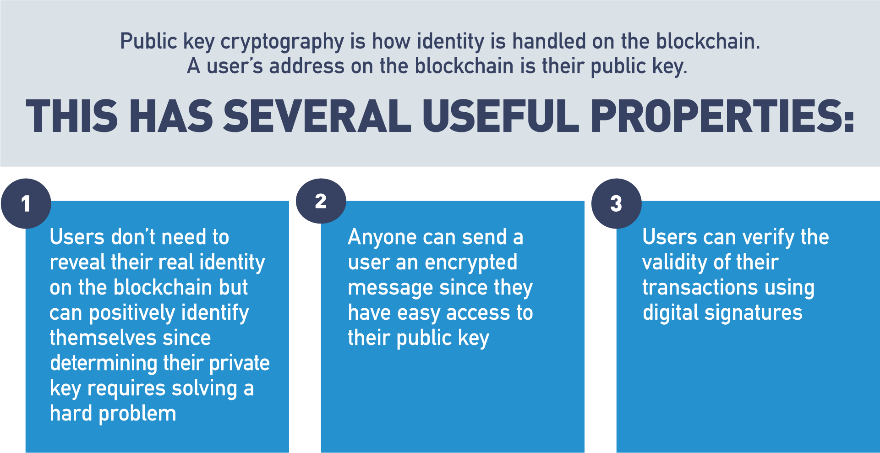
* Public Key Cryptography  
  This encryption method uses a pair of keys: an encryption key, and a decryption key, named public key and private key, respectively. The key pair generated by this algorithm consists of a private key and a unique public key that is generated using the same algorithm.
* Zero-Knowledge Proofs  
  A new approach to protecting digital secrets that prove knowledge of a secret without revealing it.
* Hash Functions  
  This type of encryption doesn’t make use of keys. It uses a cipher to generate a hash value of a fixed length. The function converts plain text (no matter the size) into a hash of fixed size. It is nearly impossible for the contents of plain text to be recovered from the cipher text. Think of it like trying to recreate a human from a fingerprint, a fingerprint uniquely represents a human no matter the size of the human and you can’t reverse engineer a fingerprint to recreate the human.
* Merkle Trees  
  A data storage technique that compresses or packs data for storing blockchains with a tamper-free component built in. Merkle trees are built upon hashing principles in that each hash becomes a part of the next hash to build a tamper resistant data storage model.

## Public Key Cryptography

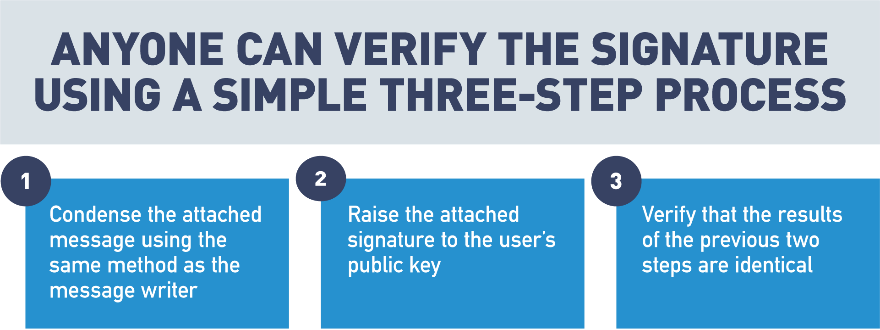
Identity in the blockchain is based on public key cryptography. A person’s address on the blockchain is their public key.

Transactions on the blockchain include their public key and are digitally signed with the sender’s private key:

* A digital signature verifies that someone in possession of the private key authorized the transaction.
* Digital signatures can be easily verified using the corresponding public key, which is included in the transaction.



## Identity: RSA Public Key Cryptography



## Identity: Specific Identity Implementations

Ethereum is a public blockchain that anyone can participate in. [Hyperledger](https://www.hyperledger.org/) is an example of an enterprise blockchain where participants must be granted access to engage in the blockchain.

* Ethereum  
  A user’s identity is an address based on their public key.
* Hyperledger  
  Identity is managed by X.509 certificates. Certificates are only shared with parties involved in the transaction.

Public key cryptography uses a pair of a public key and a private key to perform different tasks. Public keys are widely distributed, while private keys are kept secret.

Using a person's public key, it is possible to encrypt a message so that only the person with the private key can decrypt and read it. Using a private key, a digital signature can be created so that anyone with the corresponding public key can verify that the message was created by the owner of the private key and was not modified since.

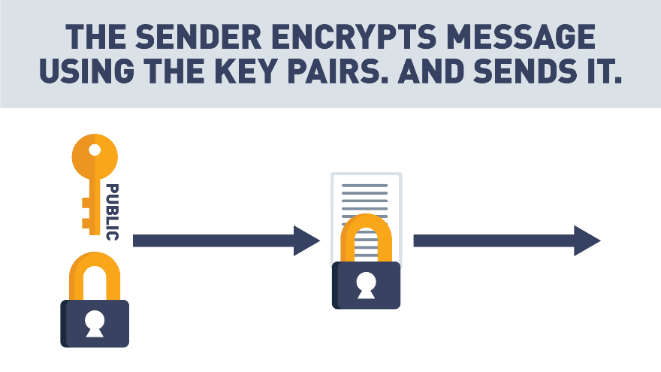


Digital Signatures and Key Pairs

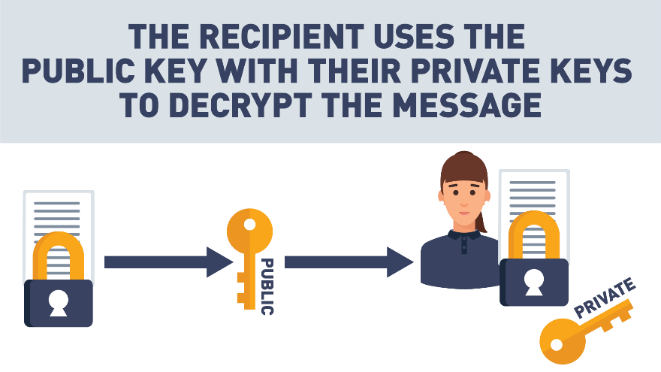
Step 1:



 Step 2:



 Step 3:



## Private/Public Key Cryptography

So, I want to talk a little bit about cryptography and some cryptography principles.

The first is easy and hard problems, and this is really what public - private key cryptography is based off of.

There are some problems that are very easy one way, but difficult another way.

And a great example of this is multiplication.

So, if I give you a pen and paper and a lot of time, I can ask you to multiply any two numbers, and you can probably come up with an answer fairly easily.

What's a lot more difficult is if I give you the product of two numbers and ask you to factor that and find out all the numbers you can multiply together to get that result, that's a much harder problem.

This is how public - private key cryptography works.

We use an easy mathematical problem to generate a message, but we make it very, very hard for that message to be decrypted by someone who shouldn't decrypt it, and public and private keys play a big role in blockchain.

I want to show you right now.

I've got two different wallets. I've got a wallet that you're probably used to, that you keep money in, and then I've got a hardware wallet, a digital wallet that you'd use to trade something like bitcoin or ether.

Now, what you're used to, in your regular wallet, is putting money in here and you keep your money in here, and if you lose this, whoever finds it gets your money and they get to spend it.

In blockchain, with cryptocurrencies, it's a little bit different.

The only thing that ever gets kept in here is your private key.

And a private key - public key work together so that I can use a private key to sign, digitally sign, any message.

You can then take the public key, which anyone can know, and use that to verify that my specific private key was the one that actually signed that message.

And so, you can know without a doubt that I'm the one who created that message,

that no one was pretending to be me sending this message.

And this is how it works trading digital currencies back and forth.

If I decide I'm going to pay you three bitcoins and I'm gonna do it out of this hardware wallet or any software wallet, any kind of digital currency, the only thing that's kept on this device is my private key and it never leaves, and so, that means if I want to send you some money, all I'm doing is accessing the private key on this device to sign a message that gets transmitted to the blockchain, that says I'm paying you some bitcoin or some ether or some litecoin, and my public key is used to verify that that message actually did come from the wallet that says it did.

And this is how we trade cryptocurrencies back and forth, and that's what makes the concept of a digital wallet a little bit different.

If I happen to lose this, I haven't lost the money that's in it, because there's no money ever in it.

All that money is is just a record on the blockchain, and, as long as I can recover that private key somehow, I can just get a new device, start using my private key again and keep right on trading.

So, that's how public and private keys fit into blockchain; a very key component just to understand that they're used to sign and verify any transactions that you make.

## Zero-Knowledge Proof (ZKP)

Zero-knowledge proofs authenticate parties without the need to widely transmit private information online. A zero-knowledge proof (ZKP) is a cryptographic method that allows a party (the prover) to prove to another party (the verifier) that a given statement is true, without conveying any additional information.

Let's review an example. Let's say there are two toy cars, identical in shape and size, except, one is red and one is blue. Jerry, who is color-blind, holds the toy cars behind his back. Jerry then shows one of the cars to Sam. Jerry then hides that car behind his back and shows Sam the other car. Sam can consistently detect the switch because the cars are different colors, but he never has to reveal the color of the cars to Jerry in order to prove the secret.

## Zero-Knowledge Proof (Cave Example)

In this section, we're going to talk about a cybersecurity idea in blockchain known as "Zero-Knowledge Proofs".

Zero-Knowledge Proofs are exactly what the name implies - they allow me to prove to another party that I have a certain piece of knowledge without revealing what that knowledge is.

Zero-Knowledge Proofs are often referred to as zk-SNARKs, which stand for "Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge", or zk-SNARKs for short, or, if you want to be simple, we can just call them Zero-Knowledge Proofs.

A great example of a Zero-Knowledge Proof is what we call the cave door analogy.

Pretend that there's a circular cave, with only one entrance or exit and at the back of this circular cave there's a door which can be unlocked using a secret code entered onto a keypad.

If I want to prove to you that I know the unlock code without revealing that unlock code to you, all I need to show is that I can walk into one end of the cave, open the door, and come out the other end.

If I've successfully demonstrated that, then you know without a doubt I've been able to unlock that door, but yet I haven't revealed that unlock code to you.

This simple cave door analogy is a Zero-Knowledge proof, and if you can remember this cave door analogy, then you'll understand why Zero-Knowledge Proofs are so important in blockchain.

For example, a user may make a request to send another user some money.

The blockchain naturally wants to make sure, before it commits this transaction, that the user sending the money has enough to send.

However, the blockchain doesn't really need to know or care who is spending the money, or how much total money they have.

Being able to answer a question of "Does a user have enough money to send to another user" without knowing who the user is, or exactly how much they have, is one of the primary use cases for Zero-Knowledge Proofs in blockchain.

So, when you hear about zk-SNARKs, don't get intimidated.

It's not a complex idea. Just think of Zero-Knowledge Proofs and the cave door, think about how important it is in blockchain to be able to prove a claim without actually revealing the information behind that claim, and you'll understand Zero-Knowledge Proofs.

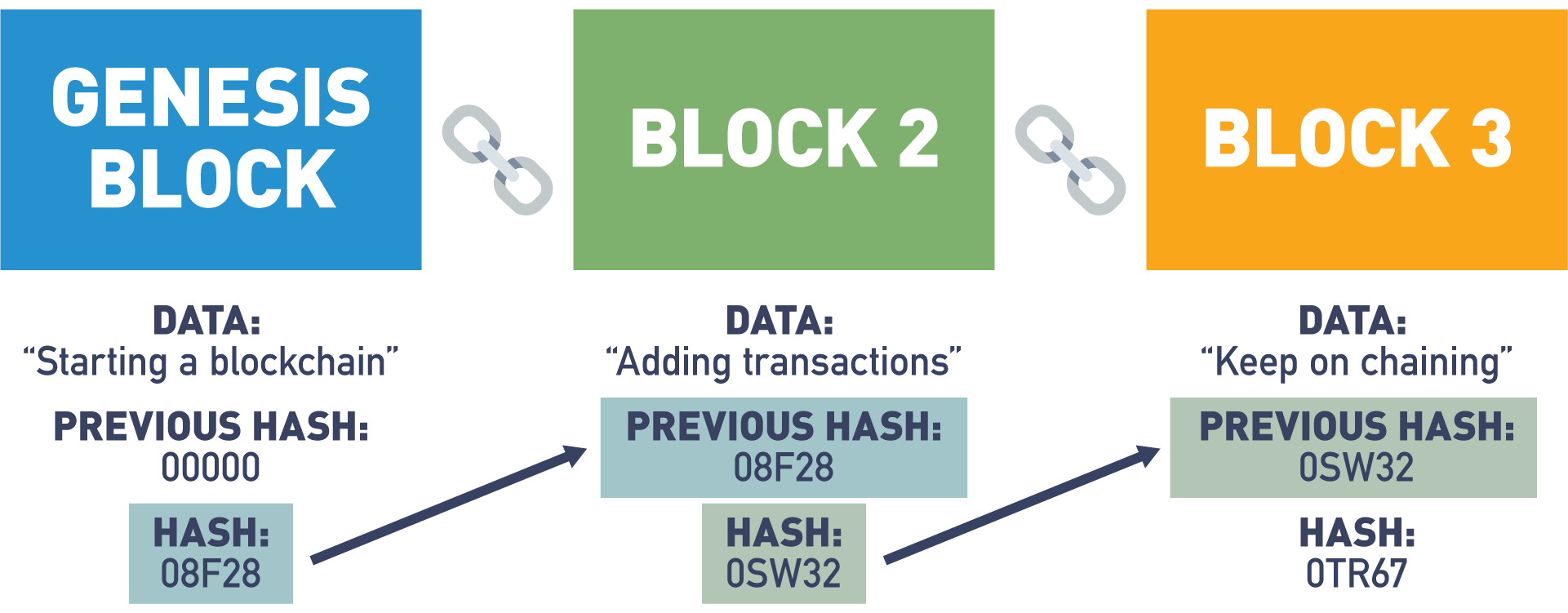
## Hash Functions in Blockchain

When using blockchain, the need to trust a central authority to verify the accuracy of data is removed and replaced by trust in a cryptographic hashing function. With data integrity guaranteed by algorithms, trust becomes part of the system.

Blockchain provides users with data integrity in a trustless environment. This is accomplished using cryptography in a way that moves the burden of trust from data processors to cryptographic algorithms.

Hash functions are featured heavily in blockchain. A hash function is a mathematical equation with four important properties:

1. Hash functions can take anything as input and create an output with a fixed size. This makes it possible to condense anything into a piece of data of a fixed size and is how messages are condensed for digital signatures.
2. It’s easy to calculate a hash, but hard to determine a hash input from the output. The best option is to keep trying inputs until one produces the desired output.
3. Inputs that differ by a single bit produce hashes that differ by half of their bits on average. This prevents someone from finding a desired hash input using a “hill climbing”.
4. It is infeasible to find two inputs that produce the same output when hashed. Since a hash can take any input and produce a fixed output, it makes sense that multiple different inputs will create the same output. A good hash function will make it so that you have to try a large number of inputs before finding two that produce the same output.



## Cryptographic Hashing Demo

In this section, we're going to talk about cryptographic hashing.

A cryptographic hash is a special kind of cryptographic function known as a one-way function, whereas most cryptographic functions are two-way, meaning that data cannot only be encrypted, but can be decrypted at the other end.

Hashes, or cryptographic hashes, are very unique in that once data is encoded, it can never be decoded.

Let's look at a small example of this.

If we take a simple sentence, "Let's eat, grandma!", this input sentence will generate a unique 32-character hash output.

This hash output can be thought of as an identifier for this input data.

In other words, I can input this data into a hash function to generate this output, and I can share this output with anybody, anywhere, safe in the knowledge that it is mathematically impossible for anyone to reverse-engineer the original input from this hash output.

In fact, the only possible way that anybody could ever determine what this input was, was by randomly inputting data into a hash function until they were able to recreate the same output.

Another unique function of a cryptographic hash is that any small change to a dataset, no matter how small, will result in an entirely different hash.

If I remove the comma from this sentence, not only do I entirely change the meaning of the sentence,

I also generate a new 32-character hash output.

This 32 character hash output remains a fixed length no matter how big the input dataset is.

To demonstrate this, let's take the entire first book of Tolstoy's War and Peace, and paste it into our hash function.

You'll see that the most time-consuming part of this is not generating the hash, but simply moving all the data from the clipboard into the input text box.

I've generated a unique 32-character output or identifier for this input text.

You'll notice that this is the same length hash that I got when I had a short one sentence input, and if I change anything in this extremely large dataset, even one character, I will generate an entirely new hash output.

Let's take a look at this by removing the period at the end of this sentence, and replacing it with a question mark.

You'll see that by doing so, I've generated a completely different and unique 32-character hash output.

Hash functions not only play a critical role in blockchain security by enabling blocks to be linked together in creating immutability between data on the blocks, they can also be used as a great way to identify and verify large sources of data.

Let's look at some other use cases.

If I want to build a system which authenticates users, but I don't want to store their password directly in a database where it might be stolen or corrupted, a hash function can be a great solution.

Let's say I have a very simple password, password123, but I don't want to store that password inside my authentication database.

I can simply ask the user to type in their password and store the hash output from that password.

Any subsequent time a user tries to log on, I don't need to know their password. I just need to verify that they're able to recreate this hash output.

If they can't do that, because they have the wrong password, then I can simply choose not to authenticate them into my system.

Cryptographic hashes can also be used to validate source code or real large datasets in the real world.

Let's look at self-driving cars for an example.

Let's say we've developed a self-driving car with the intelligence to hash the source code every time it starts up.

My self-driving car, every time I start the car, can take its source code, run it through a hash and generate a unique identifier.

It can then share this identifier or 32-character hash output with every other self-driving car it has contact with, or even validate this against a database or some other centralized data store, or perhaps an immutable record on the blockchain.

This gives me the confidence that if the source code for my self-driving car ever gets hacked and makes it unsafe to drive,

I'll know it right away. I'll try to start my self-driving car, which will immediately hash its source code, share that hash output with other self-driving cars or validate it against an authoritative source, and instantly we can see I've got an entirely different hash output letting me know before I've gone anywhere that my self-driving car is not safe, and putting that self-driving car into a limp or shutdown mode, where it simply refuses to go anywhere until the compromised software has been updated and replaced with the right version.

Cryptographic hashes give us a way to link all blocks on the blockchain together in an immutable fashion, such that if any one particular block or the data on any block is changed or altered to any degree, no matter how small, we will know it instantly and we will break the link between that block and every subsequent block.

If you haven't watched the module in this course that covers the in-depth walkthrough of Proof of Work consensus, you might want to check it out now.

We actually show how cryptographic hashing is used to link together all blocks on the blockchain, creating a data store that is immutable, secure, and extremely trustworthy.

## Lab 1: Hashing

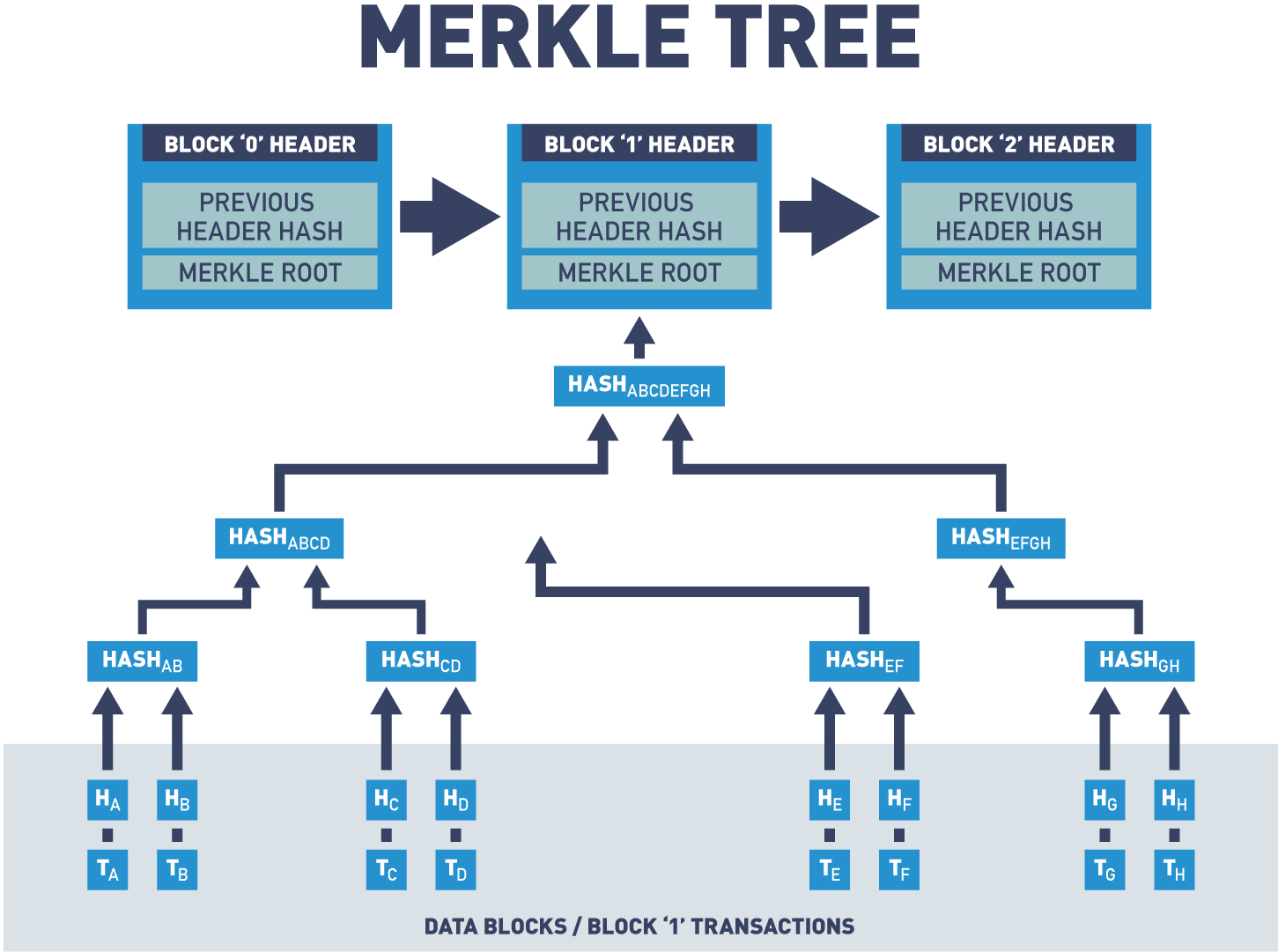
Next, let's engage with an interactive lab. This lab is an actual hands-on demonstration of taking data and creating a hash output. Enjoy!

[Start Lab](https://blockchaintrainingalliance.com/pages/lab-hash)

## Merkle Tree

A special type of data storage structure based on hash functions is called a Merkle tree:

* It is structured as a binary tree; the leaves contain the values to be stored and each internal node is the hash of its two children.
* It provides efficient lookups and protection against forgery since verifying a transaction is included in the tree. Can be accomplished by sending only the transaction, the hash contained in each node between the transaction leaf node and the root, and the hash values used to create each hash sent.
* Looking up a transaction in a Merkle tree with three levels includes sending two transactions (the desired one and the other child of its parent) and three hashes (the transaction’s parent, the root, and the root’s other child).



Merkle trees are a data structure that allows authenticated storage with efficient data retrieval.

## Merkle Tree, Validation of Data

Blockchains use Merkle trees for fast and efficient validation of data.

Merkle trees summarize the entire set of data in a block by creating a root hash of that data.

A root hash is created by repeatedly hashing pairs of child nodes until only one node is left.

Let's take a look at a diagram of a Merkle tree.

This diagram consists of four transactions represented as transaction "A", transaction "B", "C" and "D".

The transaction data is then hashed and the resulting hashes are stored in leaf nodes represented as H of "A", "B", "C" and "D".

Nodes are repeatedly hashed in pairs and the resulting hashes are stored in child nodes until only one node remains: the Merkle root or root hash.

The reason you wouldn't want to hash the entire set of data as a string is because it's not efficient when validating transactions.

In this example, if Alice needed to show Bob that this transaction was valid, let's say transaction "C", Alice would need to send the entire list of data to validate the block.

But when using a Merkle tree, Alice only needs to send the nodes that contain the transaction that she is looking to validate.

Let's say Alice wants to validate transaction "F".

Alice would only need to send the data of transaction "F" and four hash values to Bob.

Bob would then calculate the hash value based on the given information.

And if the root matches the block, the transaction can be assumed to be valid.

Merkle trees allow for validation of a specific transaction without requiring the entire set of data.

## Ethereum vs. Hyperledger Fabric

The use of public keys for identity management is a logical choice since knowledge of a public key is necessary for verification of digital signatures. Both Ethereum and Hyperledger Fabric use digital signatures on transactions and blocks to verify the identity of the creator and that the signed data has not been modified since signing. Public key cryptography is used in the blockchain as a method for managing users’ identities without revealing real world identities.

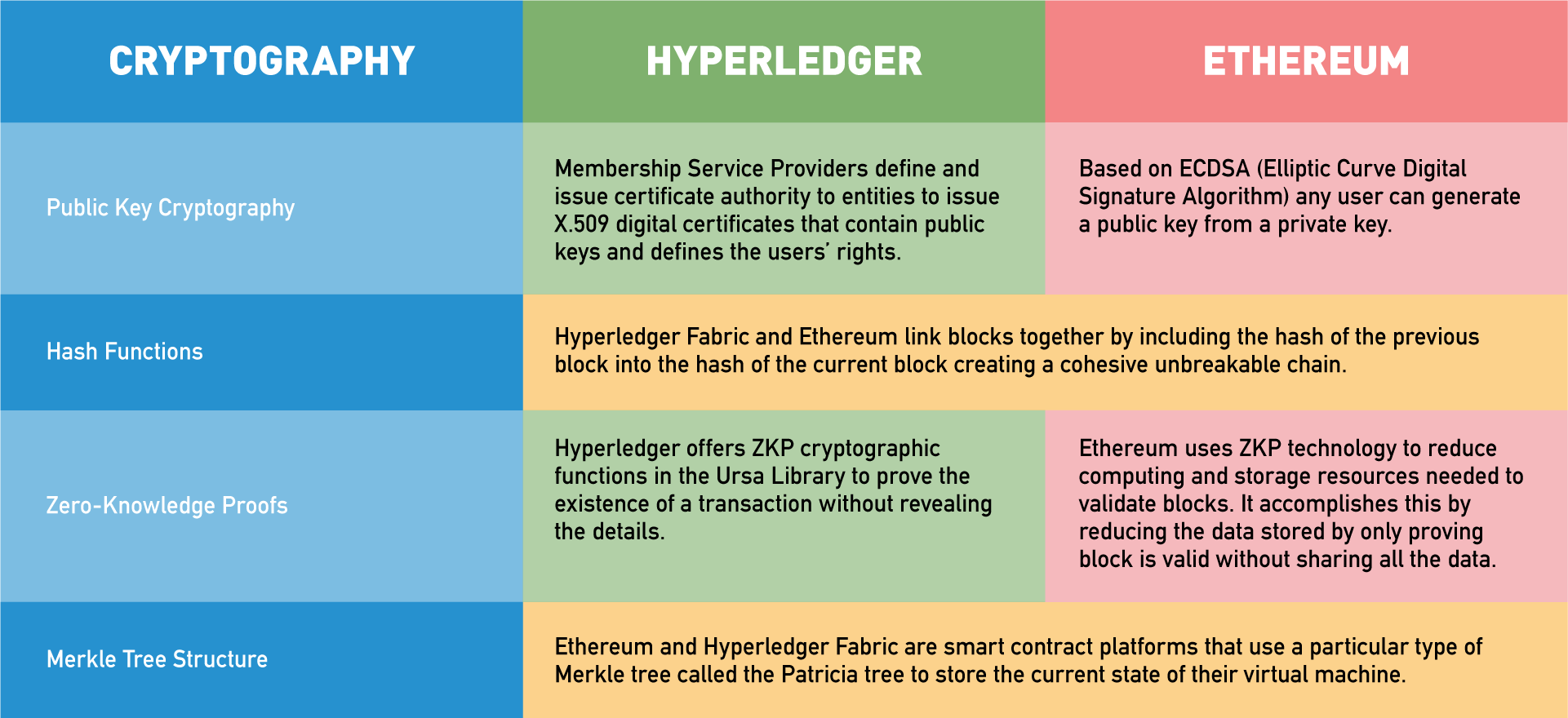
In Ethereum, users are identified by an address that is directly related to the user's public key. This provides identity verification while preserving anonymity.

In Hyperledger Fabric, users are identified via [X.509 certificates](https://www.ssl.com/faqs/what-is-an-x-509-certificate/). These certificates provide several pieces of information about the user, but one of these is also the user's public key.

Hash functions are at the core of all blockchain technology. One of the primary uses for hash functions is chaining blocks together. In both Ethereum and Hyperledger Fabric, blocks include the hash of the previous block to tie the blockchain into a cohesive whole.

Zero-knowledge proofs are to increase the privacy of users. Currently, Ethereum is working on a layer 2 solution, where a second layer blockchain would store large amounts of data and only prove the batch of information is valid to layer 1 (mainnet). Hyperledger Fabric has a pluggable cryptographic library that supports ZKP techniques for enhanced privacy measures.

Merkle trees are a data structure that allows authenticated storage with efficient data retrieval. Both Ethereum and Hyperledger Fabric are smart contract platforms that use a particular type of Merkle tree called the Patricia tree to store the current state of their virtual machine.



## Disintermediation - Trust Through Transparency

Now, that we have an understanding of how collaboration and cryptography work together to create a layer of trust, let's discuss how blockchain has a powerful disintermediation effect.

Nodes on the network are allowed to place data directly onto the database that is shared.

This eliminates the need for an intermediary to do such task.

As we discussed, developers can create a distributed ledger on a blockchain, and use cryptography to give people secure storage space on that ledger.

This creates a very different world than what we have come to know today, because for the first time in the digital world, people are allowed to own their own data.

You may be asking yourself: "How is this different from the current technology?".

Today, organizations use our data, sell our data, store our data, and exchange our data.

Data is an extremely powerful asset and to own your own data is a vast change to the current system.

In a world powered by blockchain, having ownership of your database is truly empowering.

You can now share the information that you choose with any organization that you desire.

The power of blockchain and owning your own data is the ability to transact peer-to-peer.

With the current system of intermediaries, when you go out to eat at a restaurant, and you pay with your credit or debit card, you're not paying the restaurant directly.

Instead, a database record at your bank is being debited and the database record at their bank is being credited.

In this example, the value and data in the database belong to the intermediary, and not the individual.

You are then dependent upon them to secure and validate your transaction, which shifts the power to the intermediary.

But in a blockchain world, the individual has their own ledger record, and the secure key that allows them to access it.

You no longer need an intermediary.

A transaction is simply debited from your record and credited directly to somebody else's record.

Blockchain allows you to have the power to control more than financial transactions.

Later, we'll take a deeper dive into how the healthcare industry may utilize blockchain to allow people to own their own health records.

And with blockchain, you can determine who can access those records.

We talked about how cryptography and collaboration create trust.

Now, let's examine how peer-to-peer transactions with blockchain create transparency which can lead to even another layer of trust.

This layer of trust can aid to curb corruption and even create cost savings.

Currently, the data and records owned at centralized organizations are stored and hidden within a database.

These databases for the most part are inaccessible and do not communicate in an effective manner with other systems.

This also makes it easier for a corrupt individual or persons within the centralized organization to manipulate these records.

Because of the possibility for manipulation and foul play, there are many flawed and expensive safeguards put into place.

These safeguards are done through regulations and legal requirements creating expensive overhead and delays.

Besides the mounting cost to safeguard these internally, there are also many necessary safeguards from external forces, because they are individual points of critical data storage, bad actors have to identify only one point of failure to access.

The combination of one central point of storage and the storage of valuable data make these centralized databases a very enticing target for malicious persons.

With blockchain, these malicious actors would have to identify and target numerous points of failure until they control more than 51% or what's known as consensus.

In most blockchains, it could be up to hundreds of thousands of points of weakness that would have to be exposed to be corrupted.

It's nearly an insurmountable task.

Not only must a centralized organization worry about bad actors, but they must do so, while still allowing access and synchronizing with other centralized organizations.

Having to constantly update and synchronize data across many centralized databases is not efficient.

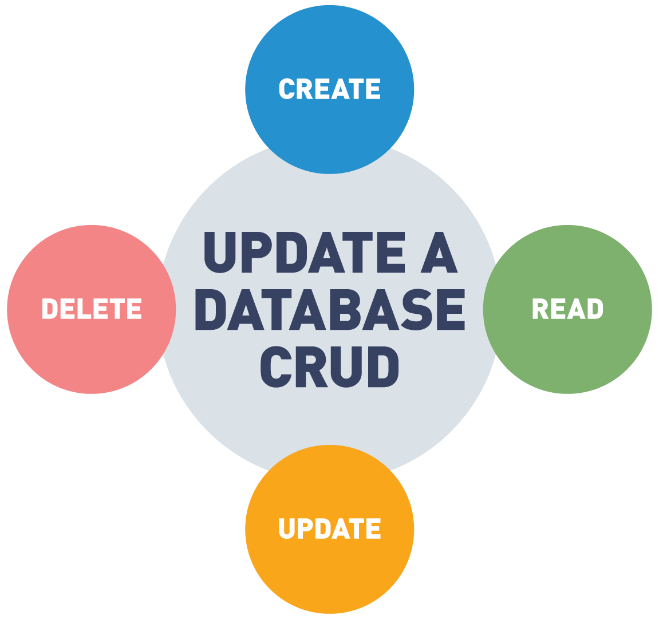
The cost is high and the vulnerability to bad actors is amplified.

All the more reason blockchain solutions are so exciting.

Blockchain offers efficiency. It also creates trust and financial benefit through transparency, security, immutability, and accessibility through ownership.

## Traditional Database Updates

A database is a collection of interrelated data organized so that individual records or groups of records can be retrieved to satisfy various criteria.



Traditional databases use the CRUD method which has four main operations:

* Create - add a new value to the database.
* Read - read a value from the database.
* Update - change an existing value in the database.
* Delete - remove the value from the database.

## Transparency of Traditional Databases

Traditional databases do not retain historical information:

* Only the most recent versions of each value are visible.
* Deleted values are not visible in the database.
* This limits the transparency of data contained in the database.
* Values can be modified or deleted after creation.

The CRUD update model of databases allows data to be changed or removed from the database. This means that the visible data in a database is not an accurate historical record of the database. The existence of an update operation means that each value in the database is only the most recent version of that value and could have had different values in the past. The delete operation means that values can be removed from the database.

This limits the transparency of data in the database since values can be modified or deleted after creation.

## Blockchain Updates

The blockchain is designed to be a data structure that only allows appending:

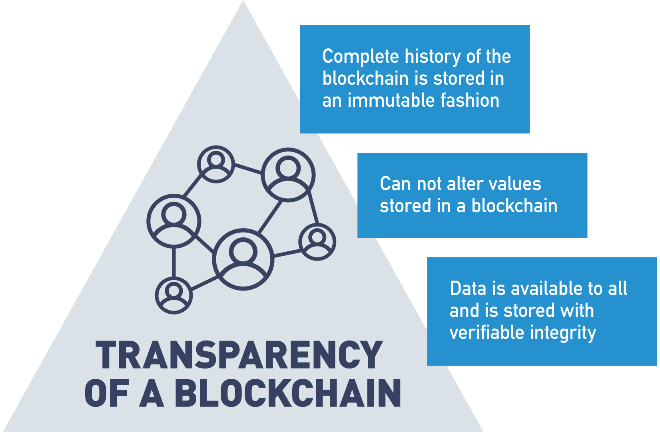
* The past history of the blockchain is visible and immutable.
* Updates to the blockchain can be performed by including them in new blocks added to the blockchain.

The blockchain is designed as a data structure where each block in the chain locks in the value of the previous block and so on, back to the first or *genesis* block. This means that the blockchain is an append-only data structure without support for modification or deletion.

The entire history of the blockchain is publicly visible and stored in a distributed and decentralized fashion. Values in the blockchain can be “updated” by appending a new version of that value in a later block, but the complete history of the value is preserved.

## 2.4 Transparency of a Blockchain

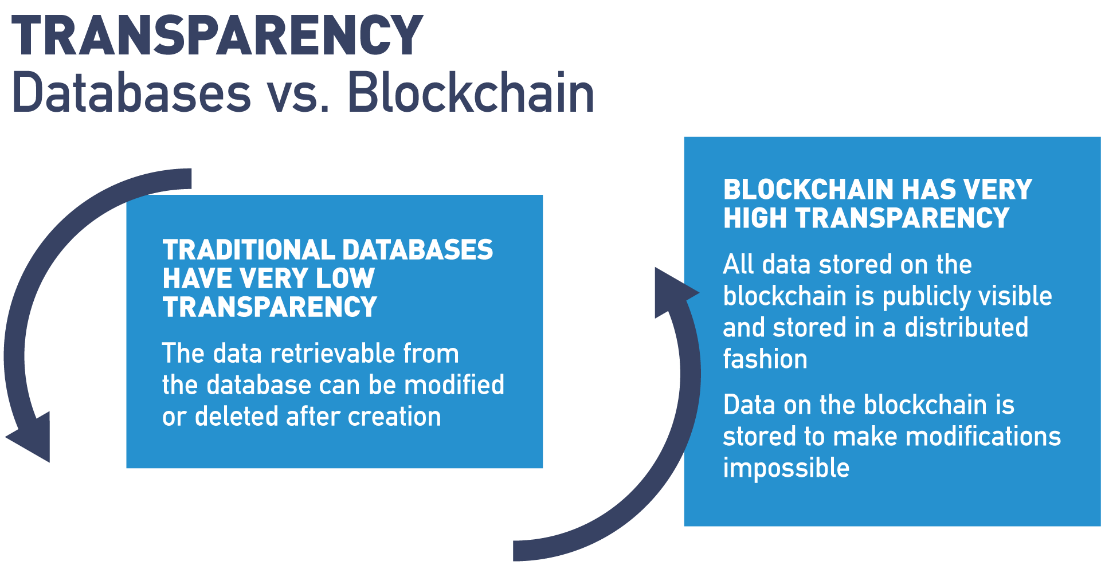
The blockchain is designed so that its entire history is visible and unchangeable. Transactions in the blockchain cannot be modified after creation, and their complete history is publicly visible. This means that the blockchain is a completely transparent data structure with the useful property that the integrity of the blockchain is easily verifiable by any user.



## Transparency: Databases vs. Blockchain

Traditional databases and the blockchain were created for different purposes and have different levels of transparency. Traditional databases have low transparency since values can be modified or deleted; however, this changeability allows them to store data in an efficient manner, with only the most relevant versions of each value retained in storage.

The blockchain is publicly visible and immutable, meaning that it has very high transparency. Its append-only structure and decentralized storage sacrifice storage efficiency for trustworthiness of the stored data.



## Transparency

One of the big benefits we get in any blockchain solution, public or private, is the idea of transparency.

In a public blockchain solution like Bitcoin or Ethereum, because they're anonymous and we have no concept of identity, we have no way of treating users differently.

And so all data on a public blockchain is transparent and visible to all other participants.

And this is really important. It adds a lot of value, when we're talking about exchanging currency or tokens of monetary value, because as long as we can protect the anonymity of the participants, it gives us a great way for anybody to validate the details of any transaction on a ledger that is immutable, permanent, can't be changed and offers a high degree of trust.

This also has a lot of other really interesting potential use cases that we're starting to explore with public blockchain technology, voting and voter registration, tracking election results.

These kinds of things are really, really great use cases for having that level of public transparency.

On public blockchains, there's another kind of transparency, which adds a lot of value as well, and that is full transparency into the smart contracts that execute on that blockchain.

These, oftentimes, are smart contracts which have the potential of working with other people's money, sometimes large amounts of other people's money, and if you're going to entrust your hard-earned money into someone else's smart contract, it's really nice to have the ability to be able to go and review the source code of that smart contract, either yourself or by hiring a developer to audit that smart contract, to make sure it's written fair, that there are no security vulnerabilities, and that it does what it claims to do.

On the private blockchain side, what we have [is] permissioning.

And we can control how open or closed our data is.

We still have a lot of benefits of being able to share data in shared infrastructure that private blockchain creates.

There are a lot of business networks and value chain relationships where the participants would love to be able to share more data and more information with consumers about the business processes and the steps that go into delivering the goods and services we consume.

What has traditionally prevented solutions like this is the lack of any kind of shared infrastructure.

While technically conventional technology may be able to address these concerns, it is oftentimes human beings not being able to come to consensus on questions of who owns the platform, who builds the platform, who maintains the platform.

And, if a participant leaves the ecosystem, do they take all or part of the platform with them.

That have prevented us from using conventional technology in these respects.

Using private blockchain solutions like Hyperledger, can help alleviate many of these concerns and create a truly shared technical infrastructure between organizations.

This allows participants in a supply chain or value chain to track data and to share that data about how goods and services are produced, created, consumed, and distributed into the open market, that we haven't really been able to do practically before.

It's estimated that over 1/3 of the food we produce goes to waste, because we don't have this kind of clarity into our supply chain with food or into the supply chain with other types of products.

Think about if a meat gets recalled because it might be contaminated, how much perfectly good meat gets thrown away just to err on the side of caution.

Where if we just had greater resolution and visibility into where that product originated from and how it went all the way from production to our plate.

Then, we could issue more accurate recalls and reduce the amount of food waste.

Consumers might value your product more, your offering more, if they're able to see where it comes from.

If you're manufacturing and distributing clothing, and you can demonstrate to consumers that all of that clothing was sourced from parts of the world with fair labor practices consumers are going to have more trust and faith in the brand and ultimately willing to pay a higher price for it.

So, these kind of transparency solutions are one of the biggest benefits of blockchain and one of the areas being most explored, because right now there are a lot of consumers who would simply like more visibility into the products and services they purchase.

And blockchain, both public and private, can be a great solution for doing that.

## Immutability in the Blockchain

Blockchain is designed to be an authoritative ledger of the history of the network.



This history may include financial transactions and business agreements where modifications to the ledger may have wide-reaching business impacts. Blockchain is based on an untrusted network, so trust that the blockchain has not been modified needs to arise from the structure of the blockchain itself, rather than from trust in the organization storing a certain copy.

## Immutability

So, one of the big benefits of blockchain is what's known as immutability.

The idea that once a record gets committed to the blockchain or to the ledger, it's there permanently.

In blockchain, it's a little bit different than a database, and we'll talk about this in another module, in a lot more depth, but in a traditional database we're used to being able to edit records and delete records, and that's not the case in a blockchain.

In a blockchain, there are only two possible operations: we can create a new record, and we can go back and we can read existing records.

And this contributes to this idea of immutability - once data is written to the blockchain it can't be edited, it can't be deleted.

All you can do is add another record to the blockchain indicating that something about that data has changed.

This immutability is what makes blockchain such a secure solution, and it's what makes it a trustless solution.

Meaning, I don't have to trust anybody that I'm interacting with and trading with, as long as we both trust in the blockchain and the data on the blockchain.

Then, we can transact back and forth seamlessly.

The way immutability works is blockchain is, by design, a very, very inefficient solution.

We are asking a large number of nodes, all the nodes on a network, to perform exactly the same work as every other node.

Essentially, we are duplicating work over and over and over again.

The reason we do this, is because the only way to potentially change data on a blockchain, is by changing the record on that blockchain for 51% or more of the nodes, or the miners, or the participants trying to come to consensus on the blockchain.

And when you get to very, very large-scale networks, Ethereum with its 16,000 plus nodes, Bitcoin with over 30,000 nodes, this becomes a very, very, very tall order.

Trying to hack or change a record on over 15,000 of those Bitcoin nodes would be quite a bit of work.

So, it's not impossible to change the record on a blockchain, but it is impossible from a practical standpoint.

Now, one thing that should be noted when we talk about immutability is: all that blockchain gives us is an accurate recording of what was posted.

It is still up to whoever is posting that information on the blockchain to make sure it's accurate and true.

In other words, blockchain doesn't do anything to validate that the information on it is correct.

All it validates is that that information hasn't been changed since it was originally written.

Another way to think about that is, I could post a record on blockchain that says: "The sky is orange".

That doesn't make the sky orange.

We all know the sky is blue. All that does is that means I can't ever come back later and claim I didn't say that or I said it was blue, and someone changed the record.

That immutability that blockchain gives us is that that data was captured as it was originally written and hasn't been changed.

Another part of this immutability is cryptographic hashing, and the way that we chain all these blocks together.

If you haven't watched the module on Proof of Work, I would suggest you go watch that now, to see a really in-depth overview, a hands-on demo of how blocks are actually linked together in such a way.

And, if I ever went back and tried to change any information or prior transaction on the blockchain, I would break that chaining in a very obvious way that anyone would immediately spot if they came and querried that data off the blockchain.

When you hear about immutability, just understand that all we're talking about is the virtual impossibility of anyone ever being able to come along and change any data on the blockchain.

And also, along with that, understand that we only have two possible operations on blockchain: we can only read data and we can only add new data.

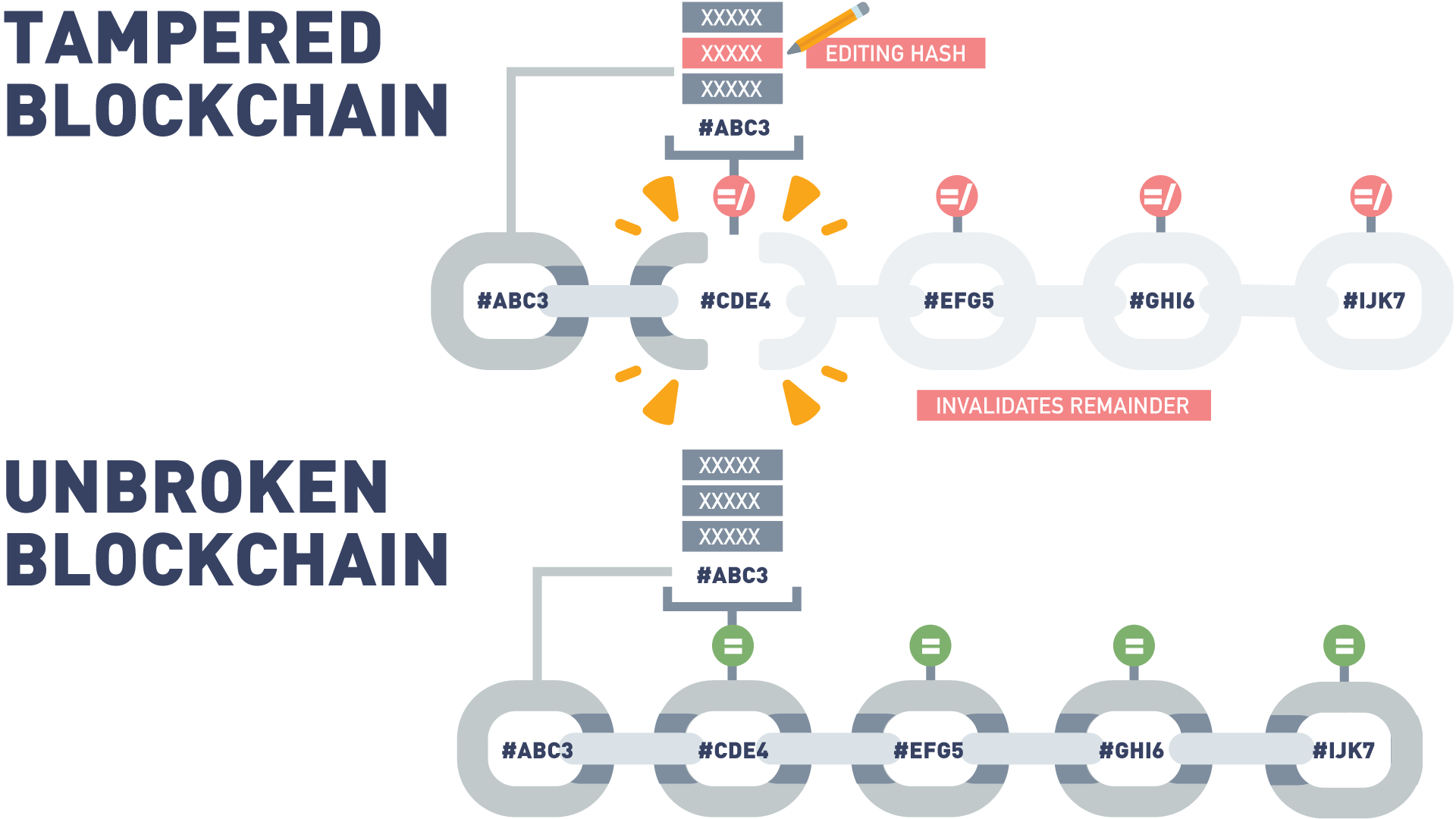
There's no concept of an edit or delete, and this is what we talk about when we talk about immutability on the blockchain.

## Immutability in the Blockchain Is Essential

The blockchain needs to be immutable. If someone can change the blockchain after the fact, then it is no longer a trusted historical ledger. The blockchain is designed so that immutability is cumulative; each piece is linked to every other piece, creating a cohesive whole that is more difficult for an attacker to modify.

* At the bottom level, transactions are digitally signed by their creators. An attacker can’t forge a transaction unless they steal a private key.
* A block structure is predefined. Attackers can’t modify it to suit their purposes.
* The chain part of the blockchain is achieved using hash functions. Each block includes the hash of the previous block, creating a clear link between each block in the blockchain.
* Each block is digitally signed by its creator. The creator is selected through the blockchain’s consensus protocol, making it difficult for an attacker to be a legitimate creator.

All four of these features help to make the blockchain resistant against changes occurring after the fact.



## Why Is the Blockchain Immutable?

Each transaction cannot be forged or modified because it is mathematically infeasible to forge a digital signature. The structure of blocks is publicly defined, and invalid blocks will be publicly rejected.

Each block “locks in” the value of previous blocks by including their hash. Attackers cannot find another block that will produce the same hash.

A block cannot be forged or modified, because it is digitally signed by the creator. The creator of a block is either publicly known (Proof of Stake) or difficult to become (Proof of Work), making masquerading as the real creator difficult or impossible.

Now, let’s take a moment to discuss how each of the features mentioned contribute to the immutability of the blockchain.

At the bottom level, each transaction is digitally signed. This means two things about transactions:

* Existing transactions can’t be changed after the fact, because the signature will no longer match.
* Fake transactions can’t be created since an attacker can’t create a valid digital signature for a transaction between other parties.

Both of these contribute to the immutability of the blockchain since they limit the range of transactions that an attacker has to work with if he wants to create a fake but valid blockchain.

Next, the block structure is publicly defined in the protocol. This limits the types of modifications that an attacker can make to a block when trying to modify the blockchain.

Third, each block contains the hash of the previous block. This is what ties the blocks of the chain together. Remember from earlier that one of the properties of a hash function is that it is extremely difficult to find two inputs to a hash function that create the same output. Since a block contains the hash of the previous block, it’s difficult to find a different version of the ledger’s history that matches the most recent block, as that would require finding two different versions of the previous block that have the same hash.

Finally, each block is digitally signed by its creator. Since the creator of a block is selected via a consensus algorithm, it’s difficult for an attacker to become the legitimate creator of a given block. If an attacker is not the legitimate creator of a block, it’s impossible for them to create a digital signature that others would accept.

## Immutability Mechanisms

Now, let’s look at how different blockchains implement immutability.

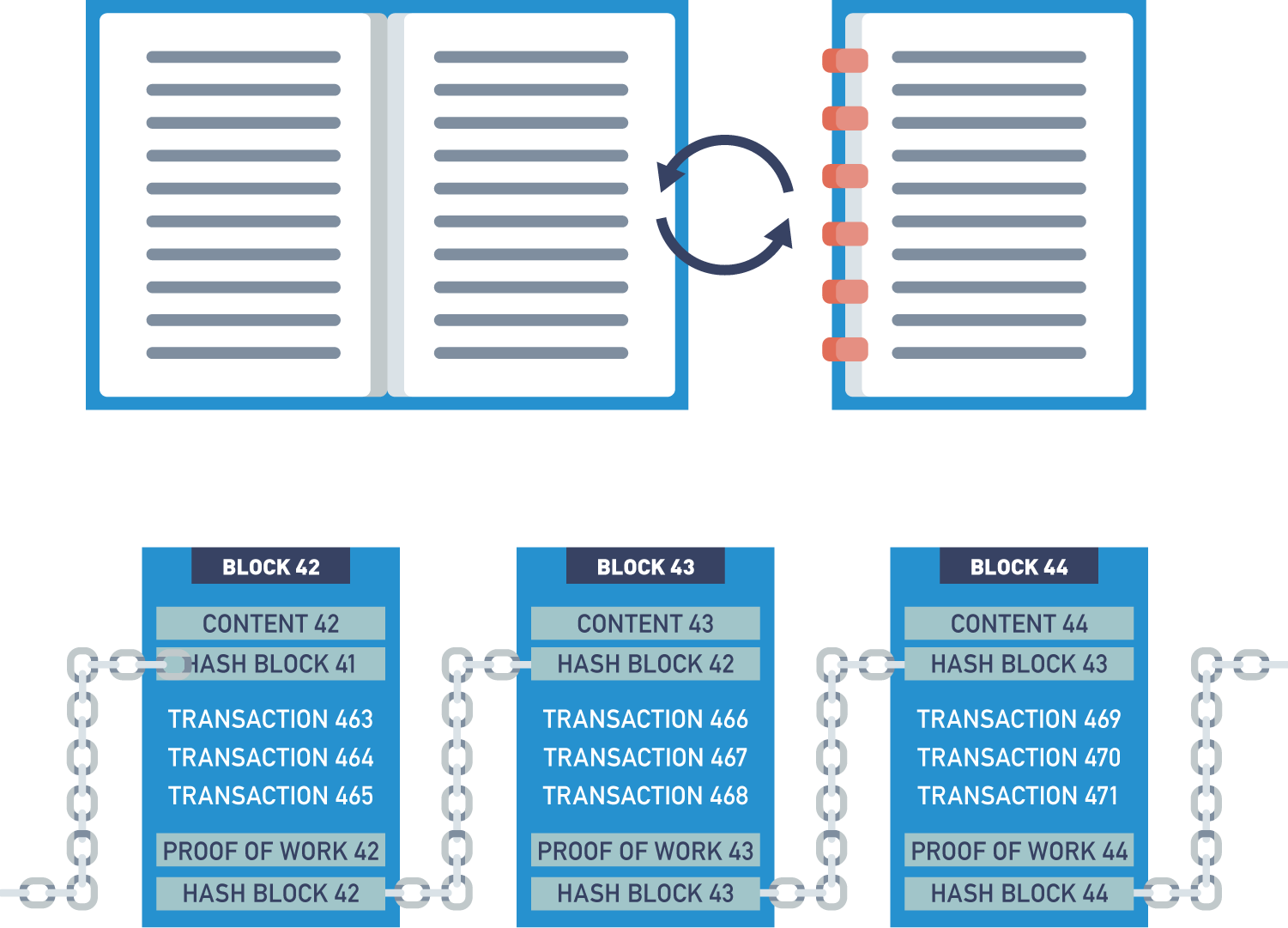
In Ethereum and Hyperledger, the immutability mechanism is the one that we’ve described previously. Each transaction and block is digitally signed and are linked using cryptographic hashes.

[Corda](https://www.corda.net/), a multi-party application development platform, relies on its notary service for immutability. Each Corda network has one or more notary services that verify transactions. Each transaction is considered separately and, if approved, is signed by the notary service. Transactions signed by a notary are finalized and cannot be modified after the fact.

## Hashing and Chaining

It is important to understand the value of locking in the previous block by including its hash in the next block. As explained in the article [*“A Gentle Introduction to Immutability of Blockchains”*](https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/) by Antony Lewis,

* Creating a ledger of transactions with blocks that refer to previous blocks is a much better idea than numbering the blocks sequentially.
* In a book with pages, 1, 2, 3, etc., it would be easy to tear out page 25 and replace it with another page.
* The integrity of the book has been manipulated and altered. However, there is nothing about the new page number that ties it (chains it) to the content of the previous page.
* Instead, in a blockchain, blocks are referenced by their hash and each block explicitly specifies which block (hash) it is building on.



## Hashing and Chaining with Proof of Work

We will cover the Proof of Work in a later module. However, this demo uses the Proof of Work to show how blocks are chained together and how tampering with information in a past block destroys the integrity of the proceeding blocks.

In this video, we're going to talk about Proof of Work consensus, and how Proof of Work consensus is used to create an immutable chain of block data on the blockchain.

Let's take a small example. Let's say we have some block data and, in the interest of simplicity, we will keep this very, very short.

But understand that in real life a block will most likely contain many more than just three transactions.

But on this block, we have a full block consisting of three transactions.

When it's time to validate a full block, all nodes on the network will start to guess a nonce value.

What we're looking for is a nonce value such that when we take our input transaction data and we combine it with a nonce value, we get a hash output that matches the difficulty.

In this case, the difficulty is a hash output that begins with four leading zeros.

Every node on the network will guess a different nonce randomly until they happen to find one that matches the difficulty.

So, our node may start off by guessing "123", and we see that that does not produce a hash output that matches the difficulty of four leading zeros.

Let's try again. Let's try "973321". Once again, that does not give us a hash output that matches the desired difficulty.

[So], rather than guess over and over and over, let's go ahead and ask a computer to do our work for us.

The computer is now guessing different nonce values randomly until it happens to guess "22294", which you see produces a hash that begins with four leading zeros.

Because this hash is the output of input to a hash function consisting not only of the transaction data, but also of the nonce, changing either one will result in a new hash output which does not match the difficulty.

If I change "22294" to "22295", you'll see I get a hash output which no longer meets the difficulty criteria.

However, if I change any of my transaction data, I'm also altering the input to the hash function, and thus generating an output which is completely different from the desired outcome.

In this way, nodes or miners on a network can validate they have the same transaction data.

If we all start randomly guessing nonce values for this set of data and my node guesses "22294" first, all it has to do is simply share this nonce value with every other node on the network.

Each node can then try this value "22294" on their copy of the transaction data.

If any of the data has been altered or changed in any way, no matter how insignificant, or the node in question simply did not record the data correctly, this nonce value will not work for them.

For example, if we change "4.2 bitcoin" to "4.9 bitcoin", you'll see that the proposed nonce does not work.

In this way, all nodes can come to consensus or agreement on what the right set of transaction data should be.

When a node thinks it's guessed the right nonce, it simply shares that value with the rest of the network.

If the majority of the network, 51% or more, agree with this nonce, because they have the same transaction data on their copy of the block, then the miner who guessed this number first, will be rewarded and the network will come to consensus or agree that this is the correct version of the block data.

Any nodes which have different data for the current block will then discard the copy of the current block they have and replace it with a copy that the rest of the network has agreed upon.

This method is used to create blocks of data chained together.

Let's say, that we have some transaction data here on the blockchain.

We're gonna go ahead and mine our first block.

Now, you'll notice what we've added in this demo is the hash of the previous block, which is something we store in the header of every block on the blockchain.

Because this is the first block, I simply get a previous hash value of zero.

Combining zero with the current transaction data on the block and the proposed nonce gives me a hash that meets the output difficulty.

When it's time to validate the second block, the process repeats itself.

I simply take the hash of the previous block stored in the header of the current block, combine it with the transaction data in the current block, and try to guess the correct nonce.

In this case, it's "12314"

As discussed in our video on cryptographic hashing, changing any of the input data, no matter how slight, will result in an entirely different hash.

If I try and change "2.3" to "2.9", I no longer get an output which matches the current difficulty.

This new output is also reflected in the header of the next subsequent block.

If I have a series of blocks that have all been mined and linked together, then you can see that going and changing data on any block will break every subsequent block after it.

So, if I try to alter this record "David pays Charlie 2.3 bitcoin" and I want to change it to "5.3 bitcoin", I change the hash output of the current block.

This is reflected in the current block and also in the next block.

Now, the nonce proposed for the next block does not work when combined with that block's transaction data and with the hash of the previous block.

This means that if I want to alter data on the blockchain, not only do I need to remind the block that I changed the data on, I also need to remind every subsequent block in the blockchain.

This is no trivial task when you consider that major blockchain such as Bitcoin and Ethereum contain millions of blocks.

And this process must be repeated on tens of thousands of nodes worldwide in a very short amount of time.

This ability to link together blocks in an immutable fashion and to cause attackers to have to undertake so much work, repeated so many times is what gives blockchain its security and immutability.

I hope you've learned a little bit more about Proof of Work consensus and how blocks on the blockchain are linked together through watching this video.

## Lab 2: Blocks

Next, let's engage with an interactive lab. This lab will give you the chance to examine blocks on the blockchain. Enjoy!

[Start Lab](https://blockchaintrainingalliance.com/pages/lab-blocks)

## 2.5 Chapter 2 Summary

In this chapter, we discussed:

* Distributed ledger technology (DLT) and how it differs from previous ledger storage techniques.
* Cryptography and how it is used in several different ways in blockchain.
* Hashing functions, zero-knowledge proofs (ZKPs) and Merkle tree data structures and how they are used to secure the blockchain.
* Public-key cryptography and public/private key pairs to support privacy, authenticity and security.
* Ledger immutability and transparency result from combining these technologies for an agreed-upon, append-only distributed ledger system chained together by blocks.

# 3. Blockchain Functions

## 3.1 Chapter Overview

In this chapter, we will examine some blockchain functions. First, we will discuss smart contracts, how blockchains have the ability to store and run computer code (applications) that can execute the terms of an agreement. These digital promises stored and executed on the blockchains remove intermediaries and ambiguity thereby reducing conflict.

We will discuss how blockchains secure their information and how these techniques differ from traditional database security. Next, we will discuss different types of blockchains (public, private and hybrid models) and design considerations that need to be made before blockchains can be developed. We will examine the steps in a basic blockchain transaction from start to finish.

Finally, we will discuss blockchain consensus models and why they are the backbone to the blockchain operations. We will compare Proof of Stake and Proof of Work models and be able to discuss the differences and environmental considerations. Also, we will discuss private blockchain structures and how permissioning mechanisms are the basis for their ConsenSys models.

## Learning Objectives

By the end of this chapter, you should be able to:

* Explain what smart contracts are and how they work.
* Discuss the benefits of using smart contracts.
* Compare blockchain security vs. standard security.
* Indicate the differences between private and public blockchains.
* Understand when to use a public vs. a private blockchain.
* Analyze the flow of a transaction in blockchain.
* Discuss consensus mechanism used in blockchain.
* Explore different methods of achieving consensus (Proof of Work, Proof of Stake, etc.).

## 3.2 What Are Smart Contracts?

When we make a transaction on the blockchain, understand that there are only three types of transactions we can make.

It's what I refer to as the onion model of blockchain.

And we're gonna start off with a very outer layer of that onion.

The thing that most people are familiar with when they get into blockchain.

The thing we do all the time when we trade cryptocurrency back and forth.

That is two or more parties coming together and using the blockchain to record an announcement of the exchange of monetary value.

So, we might use blockchain to record the fact that I paid you three Bitcoin for your used car or I paid you twelve blockchain for your vacation home.

This is the model that many of us start off with in blockchain and again, it's the one that's most familiar and gets talked about the most right now.

But if we peel away that outer layer, and we take away the idea of a monetary transaction or exchange, well, then we're left with two or more parties using blockchain to record an important announcement.

And we see many valid use cases around this. Let's say, that I go to the doctor for my annual physical.

My doctor checks me out and he says: "Hey Kris, I want to put you on a new prescription for XYZ".

Well, maybe we're keeping our medical information on the blockchain, and so my doctor and I both agree that's a pretty good thing to add to my medical record.

In this case, we still need two or more parties, because it's very important that I, as a patient, don't have the ability to go and update my own medical record without a licensed medical professional involved.

And it's also equally important that my doctor is not able to update my medical record without my consent or permission.

And so, that's two or more parties coming together, recording an important announcement or important data point, but nowhere in that example has money or anything of monetary value exchanged hands.

Now, if we peel away the very last layer, you can take away this idea of having to have two or more parties.

And what we're left with is just a single party announcing an important or significant event.

And this is the simplest type of blockchain transaction, and also the most powerful.

If we think about blockchain, perhaps for managing a supply chain scenario, we might have a grower of organic produce announce or commit a record to the blockchain that says they've planted a crop.

And we might have an organic pesticide company come and treat that organic produce.

We still have a single organization or single entity making the announcement of something they did, and this is really the heart of blockchain.

When you understand that it becomes really easy to understand where smart contracts fit in.

And smart contracts are just computer code. They're codified logic that we can use to respond to any kind of event that gets captured on the blockchain.

In that organic produce example, if I want to notify someone when that fresh produce has been treated with organic pesticide, so I can create traceability for the end consumer, well, I might have a smart contract that manages that that defines the rules and the steps that get taken when that particular type of event occurs.

And this is all smart contracts are.

There's oftentimes a misconception when people hear the word contract that they think of a legally binding agreement between two or more parties.

It's not necessarily the case. Smart contracts don't have to be legally binding and they don't have to involve multiple parties.

In fact, if you come from a programming or development background you can think of a smart contract easily enough as a "class".

If you're not a programmer or don't come from a developing background, you can just think of a smart contract as a set of rules that get executed every time a certain type of event happens.

And this is where the real power of blockchain comes in that not only do we have a permanent, unchangeable record of all the different events that have occurred, we can also write computer code, very, very non-subjective computer code, that defines exactly how that process is going to be managed and what steps are going to be taken when that event occurs.

This allows us to ensure process consistency.

It allows us to ensure that processes that are normally fulfilled by intermediaries or middlemen can now be satisfied on their own without the need for human intervention.

And this leads to much more lean and efficient organizations in way of organizing human effort.

So, when you hear smart contract just think about computer code that you write to respond to certain types of significant events.

If you've ever worked with workflow or business process automation or management tools, you can think of smart contract is just being another workflow tool, albeit one that has the power to work with money.

So, don't get too intimidated when you hear smart contracts, and don't get too caught up in the language.

While they sometimes may be legally binding, they're not necessarily legally binding in the same way a true contract is.

They're just a way for us to bake our own logic into block chain solutions to ensure that consistency of execution.

## Smart Contracts Recap

Let’s review some basic information about smart contracts:

* They are computer programs that execute an action based on terms and conditions.
* Can also be known as chain code.
* Smart contracts have terms recorded in a computer language instead of legal language. Smart contracts are not necessarily legally binding and do not need multiple participants.
* Each step of a smart contract can only be implemented after the execution of the immediate former step.
* Smart contracts are written in Solidity, a programming language designed for developing smart contracts that run on the Ethereum Virtual Machine.
* The smart contracts act as a foundation to build decentralized applications (DApps).
* Once executed, the information in the smart contract is stored on a blockchain which cannot be altered.



## What Do Smart Contracts Provide?

These are some of the features that smart contracts provide:

* Accuracy  
  Replacing human intermediaries with executable code ensures the process will always be performed the same.
* Cost savings  
  Replacing intermediaries often provides significant cost reduction.
* Efficiency  
  Removing process intermediaries often results in significant process efficiency gains.
* Backup  
  A blockchain and smart contract deployed to it can provide a permanent record, allowing for auditing, insight, and traceability, even if the creator is no longer in business.
* Autonomy  
  Smart contracts can be developed by anyone, no need for intermediaries such as lawyers, brokers, or auditors.

## Campaign Finance

One area getting a lot of attention in blockchain right now, is campaign finance and campaign donations.

There are some really interesting and compelling use cases, ways that we might be able to use blockchain to do new and innovative things around campaign finance that just aren't practical or feasible today.

Let's say that I'm running for office and you want to support my campaign.

Well, today, you might write me a thousand dollar check and I get all 1,000 of those dollars right away to use for my campaign.

Maybe, we want to use blockchain to empower voters to keep their politicians more accountable to the promises they make on the campaign trail.

Consider the following scenario.

Let's say, that instead of donating a thousand dollars to my campaign, you write a smart contract on the blockchain to manage campaign donations.

You give that smart contract a thousand dollars instead.

That smart contract has been programmed with the terms and conditions under which it is able to release those funds to my campaign.

I might get two hundred and fifty dollars of that thousand initially to use for my election.

If I get elected, the remaining $750 can stay in the smart contract.

Otherwise, it gets refunded to you.

Let's say, I do get elected. Perhaps, I don't get the second 250 of that thousand dollars until a year in office, if I fulfilled three or more of my campaign trail promises.

And then, we might say as a final step, I get the remaining five hundred dollars to use for my reelection, only if I fulfilled 80% or more of my campaign promises during my first four-year term in office.

This would put a lot of power back in the hands of voters and would keep politicians accountable for the promises they make, long after election day.

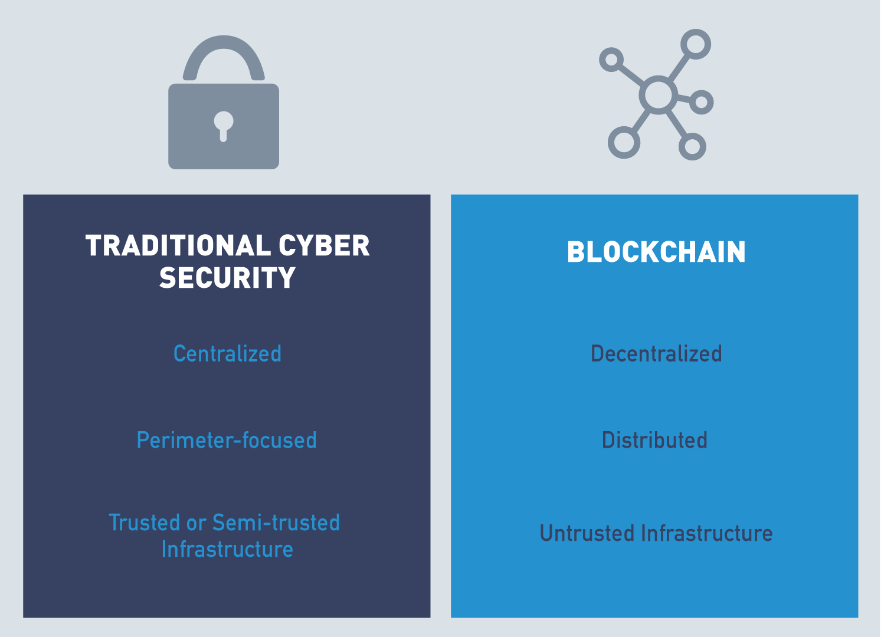
While things like this certainly are possible with conventional technology, they're not very practical or feasible.

Blockchain and smart contracts puts this power back in the hand of voters and has the potential to radically reform campaign finance and campaign donations.

## 3.3 Blockchain Security vs. Standard Cybersecurity

Blockchain is commonly called the future of computing. It takes a very different approach to data storage and processing and requires a very different perspective for security.

In this section, we will discuss some of the ways that security differs in traditional and blockchain environments.



## Introduction to Blockchain Security vs. Standard Cybersecurity

In this section, we're gonna talk a bit about how traditional cybersecurity is different than security concerns on the blockchain.

In traditional cybersecurity that we're all used to, we're very perimeter-focused meaning that we put trusted data and assets behind a very, very strict perimeter.

We assume that anybody we let inside that perimeter is trusted, either partially or fully, to see that data and access those resources.

And the brunt of our focus goes into making sure that we keep the right people from getting beyond that perimeter, that we only let authorized users through, and then we prevent any attackers or strangers from breaching that perimeter and accessing the data and resources we store behind it.

This is very different from blockchain, which runs on a massively decentralized peer-to-peer global network.

Just by its very definition, you can see that there is no perimeter on blockchain, and so our security has to come from somewhere else.

Our security on blockchain comes from the incredible amount of repetition.

The fact that we ask every node to keep the same copy of the ledger and periodically to reach consensus, majority consensus, on what the proper data in that ledger should be.

This makes the amount of work that an attacker would have to do practically impossible, if they wanted to change, hack, or alter the ledger.

Another big difference between traditional cybersecurity and security on the blockchain is with conventional applications and conventional technology.

We either develop all our own code or application parameters in-house or we rely on a single, third-party trusted provider who creates that line of business system for us.

All the code, generally, comes from one place, and if we don't write it ourselves, all we have to have is trust and faith in the third-party organization providing it to us.

In blockchain, things are a little bit different, because oftentimes in blockchain solutions we're writing smart contracts which call code from other smart contracts, which we may or may not write ourselves.

And which may come from a variety of different authors.

So, whereas in the traditional cybersecurity space, we really only need to rely on our own due diligence to write secure code or the due diligence of a third-party application provider.

In blockchain, we have to expend a lot more time and energy, making sure that the code and the contracts we're calling is safe and secure.

In other words, we want to make sure that we're not inheriting any security vulnerabilities from other smart contracts that have been written by unknown and potentially untrusted parties.

And the final big difference between conventional cybersecurity and blockchain is that in conventional line of business systems all of our applications either run directly on trusted hardware that we own as an organization or run on hardware with a high degree of trust provided by a third-party such as Microsoft Azure or Amazon Web Services.

In the blockchain world, all of our code runs on untrusted resources, untrusted hardware that can be owned by anyone, anywhere in the world.

This means that we must ensure that all the trust in a blockchain solution comes from the protocol and the code layer itself, because it's a much more massively distributed network, and we don't have direct control or access into the hardware that supports it.

So, there are a lot of differences between conventional cybersecurity and security in the blockchain space that you're going to want to understand before you deploy your own blockchain solutions.

## Blockchain Security Environment

One of the primary differences between cybersecurity in a traditional computing environment and on the blockchain is the environment itself and what it is and isn't designed to do.

**Standard Cyber Security**

* The traditional computing environment is a company network fully or, at least mostly, under the control of the company's computer security staff.
* While many organizations are making the shift to cloud-based environments, they still have a high degree of control over the security and configuration of their rented systems.
* Traditional networks are highly centralized, and the focus of cybersecurity on these systems is primarily perimeter-focused. All systems and authorized users on the network are trusted or semi-trusted, so the focus is on preventing attackers from entering from outside the network.

**Blockchain Cyber Security**

* Blockchains are designed to be decentralized, distributed systems running on untrusted hardware.
* While security in traditional environments is designed to provide security by putting all data in one place and building walls around it, security in blockchain is based on ensuring that data is protected from modification by copying data to as many locations as possible to make modification of all copies infeasible.
* Traditional infrastructure focuses on confidentiality and integrity, while blockchain is designed to provide integrity and availability.

## Security Attacks

Both traditional computing environments and blockchain have security considerations associated with them. In many cases, the same attack is possible against both paradigms, but the details of how to implement it vary.

Next, we will discuss how a few different attacks can be launched against traditional computing environments and blockchain.

## Security Attacks: Denial-of-Service (DoS)

A denial-of-service (DoS) attack is when an attacker makes it impossible for a system to serve its users as designed. This can be accomplished by exploiting a flaw in the system, but, more commonly, is accomplished by performing legitimate actions at a rate higher than the target can handle. To be effective, denial-of-service attacks typically focus on a system’s weakest link or bottleneck.

* In traditional environments, denial-of-service attacks target a company's web server to prevent customers from accessing the company's services. This can be accomplished by making more connection requests than the server is capable of supporting.
* In blockchain, a denial-of-service attack involves submitting more transactions to the blockchain than it can handle. Since many blockchains have fixed-size blocks created at a fixed rate and are stored in a distributed fashion, they have a maximum capacity that a determined attacker can exceed, rendering the blockchain unusable.

## Security Attacks: Endpoint Security

Traditional infrastructure and blockchain environments also differ with regard to endpoint security. Endpoint security originated to ensure multi-layer prevention against malware, fraud, cyber threats, and attempts to extract private information.

* In traditional cyber, endpoints are under the control of the enterprise and have some level of heterogeneity. Heterogeneity can be dangerous because an attacker has more options for finding a vulnerability to exploit.
* In blockchain, endpoints are the nodes and may be completely homogeneous. While homogeneity means that a flaw in one system is a flaw in all of the systems, blockchains built in trust and data privacy feature guard against such attacks.

## Security Attacks: Code Vulnerabilities

Computer applications are dependent on reliable code. Another way that traditional and blockchain cybersecurity differ is in the level of trust in the code used in a company's applications.

* In traditional cyber, the company writes most of the code, and vulnerabilities can arise only from code that the company controls.
* In blockchain, anyone can write a smart contract, and a flaw in the smart contract or the underlying platform code can have wide-reaching consequences. But since smart contracts can be vetted and reused, such inconsistency can be edited from the code. We will discuss an example of a vulnerability in a platform's code in a later section covering the Ethereum network.

## Security Attacks: Intentional Misuse

Both traditional and blockchain environments are vulnerable to attacks based on intentional misuse of the system.

* In traditional cyber, insider attacks or intentional misuse of the system by clients are possible. In fact, a denial-of-service attack is a specific type of intentional misuse.
* Blockchain systems are set up to incentivize network participants, miners or nodes, to do something that is in their best interest. A weakness is, if more than half of the network's processing power is controlled by a single group, the network is controlled by that group.

## Security Attacks: Data Protection

Finally, traditional infrastructure and blockchain differ in their goals regarding data protection.

* In traditional cyber, data is siloed, and access is strictly controlled by the owners, placing responsibility for confidentiality, integrity, and availability in their hands.
* In blockchain, data is distributed, and the blockchain is relied upon to provide integrity and availability.

## Lab 3: The Blockchain

Next, let's engage with an interactive lab. In this lab, you will be examining a blockchain containing five blocks, each labeled according to position. Enjoy!

[Start Lab](https://blockchaintrainingalliance.com/pages/lab-distributed)

## 3.4 Different Types of Blockchains (Public & Permissioned)

When we try to understand the main difference between a public and private blockchain, it is important to understand the terminology.

* Public Blockchains  
  A public blockchain is open to anyone to join. Public blockchains are decentralized where no one has control over the network. These immutable and censorship resistant networks are ideal for participants who don't trust each other, but still interact in a network and take part in consensus. Bitcoin and Ethereum are examples of public, permissionless blockchains.
* Permissionless Blockchains  
  Public blockchains are permissionless. Anyone effectively can join the blockchain network. No one is prohibited from joining.
* Private Blockchains  
  Private blockchains define a user's rights on the network prior to admittance. Restrictions are placed on activities such as who can write to the ledger and what transaction they can participate in. Hyperledger and Corda blockchains are examples of private permissioned blockchains.
* Permissioned Blockchains  
  In a permissioned blockchain, participation is permissioned by an organization or a consortium of organizations. This empowered entity defines who can participate in certain transactions and consensus on the network.

## Public (Permissionless) Blockchains

When people get into blockchain, there's a natural discussion about what type of blockchain, because blockchain comes in many different types and flavors.

And normally, we hear about public versus private blockchains.

One factor that often gets left out is also the idea of an open versus closed blockchain.

And it's important to consider both parameters, so you know where on a possible solutions quadrant your idea falls.

When we talk about public and private, what we're really talking about is who is able to write data onto that blockchain or onto that immutable ledger.

The open versus closed brings in to consideration who's able to read that data.

And so, we can talk about solutions which are public and open, public and closed, private and open, private and closed.

When we talk about public blockchains, what most folks are really talking about is a public open blockchain.

It's a blockchain where anybody can come write data to the blockchain, anybody else can come read that data.

So, public blockchain platforms like Bitcoin, Ethereum, Litecoin tend to get talked about a lot right now,

and these are what we also refer to as permissionless blockchain platforms meaning that they really strive to, by design, increase and protect the user's anonymity.

And, if we don't know who a user is, if we don't have a way of identifying individuals, and we don't have any way of creating permission or access rules around that user,

and it's what we get, is the system where anybody can commit data to that blockchain and anybody can come along and read data to that blockchain.

There's a perception that public blockchain platforms like Ethereum can't be used to build permission scenarios or to control access to data.

The truth is they can, they just don't give you the built-in tools that a private or permission blockchain platform will.

You can always use these open public platforms to build a permission solution, but just understand that it's upon you, your architects, and your developers to create that permissioning model, and that all starts with some kind of identity management system.

When you think of public blockchains, you think about blockchain platforms like Ethereum, understand, by default, by the very nature and design, they're designed to protect anonymity.

And, if we don't know who a user is, then we really have no way of creating permissions, role-based access and controlling what data they can read or write.

In a lot of situations, this is desirable, this is why we see cryptocurrencies based on public blockchain platforms, because having that anonymity is important.

And, if a user has a currency, something of value, they should be able to exchange it and spend it, and do what they want with it, just like anybody else.

We don't want to treat any class of users differently than any others in those scenarios.

That's a public blockchain, and that's a very different animal from the private permission blockchain.

## Public Blockchain Benefits

In the [*"Public vs. Private Blockchain In a Nutshell"*](https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f) article by Demiro Massessi, public and private blockchains have different features. The benefits of public blockchain are:

* Ledger is distributed  
  The database is not centralized like in a client-server approach, and all nodes in the blockchain participate in the transaction validation.
* Immutable  
  When something is written to the blockchain, it cannot be changed.
* Open Consensus Model  
  No restriction placed on who can operate a node in the network.
* Open read and write  
  Anyone can participate by submitting transactions to the blockchain, such as Ethereum or Bitcoin; transactions can be viewed on the blockchain explorer.
* Low barrier to entry  
  Transactions on a public network can be accomplished with an Internet connection and a cell phone.
* Secure due to mining (51% rule)  
  With Bitcoin, obtaining a majority of network power could potentially enable massive double spending, and the ability to prevent transaction confirmations, among other potentially nefarious acts. This has never been accomplished as the computing power needed to stage such an attack would be too costly.

## Private (Permissioned) Blockchains

The counterpart to a public blockchain is naturally a private blockchain.

These are platforms like Hyperledger or Hashgraph.

And private blockchains are more specifically known as permissioned blockchains.

When we talk about private blockchain or when you hear folks talking about private blockchain solutions, they tend to be talking about things on the private and closed end of the spectrum.

We want to control who can write data to this blockchain, and we want to control who can read data from this blockchain.

And in order to do that, the first step is identity.

If we don't know who a user is, it becomes difficult, if not impossible, to define rules about what data they can commit to the ledger and what data they can consume from the ledger.

When we talk about private blockchain, just think about permission blockchain, the blockchain which right from the beginning is an idea of who you are.

And this is very different from a public platform like Ethereum, in which the platform tries to protect and maximize anonymity.

And we, by design, don't know who a user is, unless we build in that kind of identity management scheme.

Private blockchains tend to come with identity management tools or a modular architecture, where you can plug in your own identity management solution.

This can be anything from an Active Directory deployment to an OAuth solution using Google, Facebook, LinkedIn, etc.

Just understand the idea behind the private blockchain.

All begins with understanding who a user is, because once we understand who a user is, we can determine what role they're in, and we can use that role to determine what information should they and should they not have access to.

This also changes the incentive for good behavior a little bit in a public blockchain, because we don't know who a user is.

We rely on economics and game theory incentives to ensure that everybody in the system behaves honestly and according to the rules.

We set up situations through group consensus, which we discuss in other sections in this course, through which honest participants are economically rewarded, where dishonest ones only incur work or cost, with no possibility of ever recouping that cost.

In a private permission blockchain, we rely on the fact that we know who a user is.

In a corporate scenario, blockchain for the business, blockchain for supply value chains, because we know who an individual is, what organization they're associated with and what their role is, we also assume that they're going to behave fairly aboveboard, because if not, we know exactly who's misbehaving and they know that they're gonna suffer the consequences for that.

Public and private blockchains, two very, very different offerings.

A lot of people make the impression, get the impression that they compete with one another, when really they don't.

They just serve to provide different types of solutions and enable different kinds of products and offerings to be built on top of them.

## Private Blockchain Benefits

The following benefits of a private blockchain have been described in the [*"Public vs. Private Blockchain In a Nutshell"*](https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f) article by Demiro Massessi:

* Ledger is distributed/immutable  
  The database is not centralized like in a client-server approach, and all nodes in the blockchain participate in the transaction validation. When something is written to the blockchain, it cannot be changed.
* Compliance support  
  As an enterprise, you likely would have compliance requirements to adhere to, and having control of your infrastructure would enable this requirement more seamlessly.
* Faster transactions  
  When you distribute the nodes locally, but also have much less nodes to participate in the ledger, the performance is faster.
* Consensus more efficient/more options  
  More options for consensus models. Enterprise or private blockchains have less nodes and usually have a different consensus algorithm, such as BFT vs. POW, which we will discuss in a later section.
* Better scalability  
  Being able to add nodes and services on demand can provide a great advantage to the enterprise.
* Enterprise permissioned  
  The enterprise controls the resources and access to the blockchain, hence private and/or permissioned.

## Security: Public vs. Private Blockchains

As discussed in [*"The Difference Between Public and Private Blockchain"*](https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/) article by Praveen Jayachandran, both public and private blockchains share many similarities:

* Both are decentralized peer-to-peer networks, each maintaining a shared append-only ledger of digitally-signed transactions.
* Both maintain transaction replicas in-sync through a protocol referred to as consensus.
* Both provide certain guarantees on the immutability of the ledger.

On the other hand, as described in [Investopedia](https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/#:~:text=The%20primary%20distinction%20between%20the,and%20maintain%20the%20shared%20ledger), the main difference between a public and private blockchain is related to who is allowed to participate in the network, execute the consensus protocol, and maintain the shared ledger:

* A public blockchain network is completely open and anyone can join and participate in the network.
* A private blockchain network requires an invitation, and must be validated by either the network starter or by a set of rules. Private blockchains are usually set up as permissioned networks, placing restrictions on who is allowed to participate in the network, and only in certain transactions.

## Public and Private Comparison

Now that we've talked about public and private blockchains, what those terms mean and again, you can think of that as permission versus permissionless blockchains,

We can talk about some of the differences and what each different type of platform aims to provide.

Public blockchains are really good for scenarios where protecting the anonymity of users is important or adds value to the solution and they're really great platforms for solutions where all users should be treated equally and we can see this because most public blockchains right now are used to support crypto currencies and this is a real great use case with a crypto currency like Bitcoin, Litecoin, ether etc.

We don't want to have any permissioning or role based access.

Anybody should be able to own some Bitcoin.

Anybody should be able to trade it with anybody else and it's not necessarily important that we know who the participants in any transaction are.

That leads to an open permissionless model with full transparency.

This is very different in the corporate world where we see private blockchains being adopted at scale because the concerns are the opposite in a corporate scenario.

In a business scenario, anonymity is a bad thing.

I want to know exactly who all the participants are and I need to know who they are because I don't want full transparency.

I don't want to share all my business data with all the participants in my business network or the general public at large.

I want to control who sees what type of information, under what circumstances and I also want to control who is able to contribute that information onto the blockchain.

I might use a private blockchain solution to manage supplier vendor relationships where only myself and my suppliers can see the price that I'm paying for a certain item.

Only a particular supplier gets to see the details of the contract that I have and not the details of a contract I have with any other suppliers and I may wish to share some of this high-level macro data with consumers so that they can see the origins of the products they're buying.

But, of course, I'd want to hide the financials behind all that so when we look at how these two solution types differ, we see the public blockchains tend to focus more on b2c or business to consumer scenarios.

Whereas private blockchain offerings like hash graph, hyper ledger really lends themselves well to be to be scenarios supply chain value chain relationships or creating any kind of shared infrastructure between enterprises.

Just to understand that well there's a big misconception that these are competing offerings.

They're really not and many real-world use cases use components of both.

It's important to understand the difference between them and it really all starts with Identity Management.

When you're thinking in your head about public versus private blockchain.

To understand that it all begins with Identity Management and in a private blockchain I know who all the participants are right from the beginning.

In the public blockchain, again, I don't know who those participants are and that's not to say that I can't build a permission solution on a public platform.

But, myself, my architects, and my developers are gonna have to develop the logic and the mechanisms behind identity management so that's public and private blockchain, two very different animals, they serve vastly different purposes.

As you start to dig into a lot of real-world use cases, what you're going to find is many use cases make use of both types of blockchain, integrated seamlessly to you.

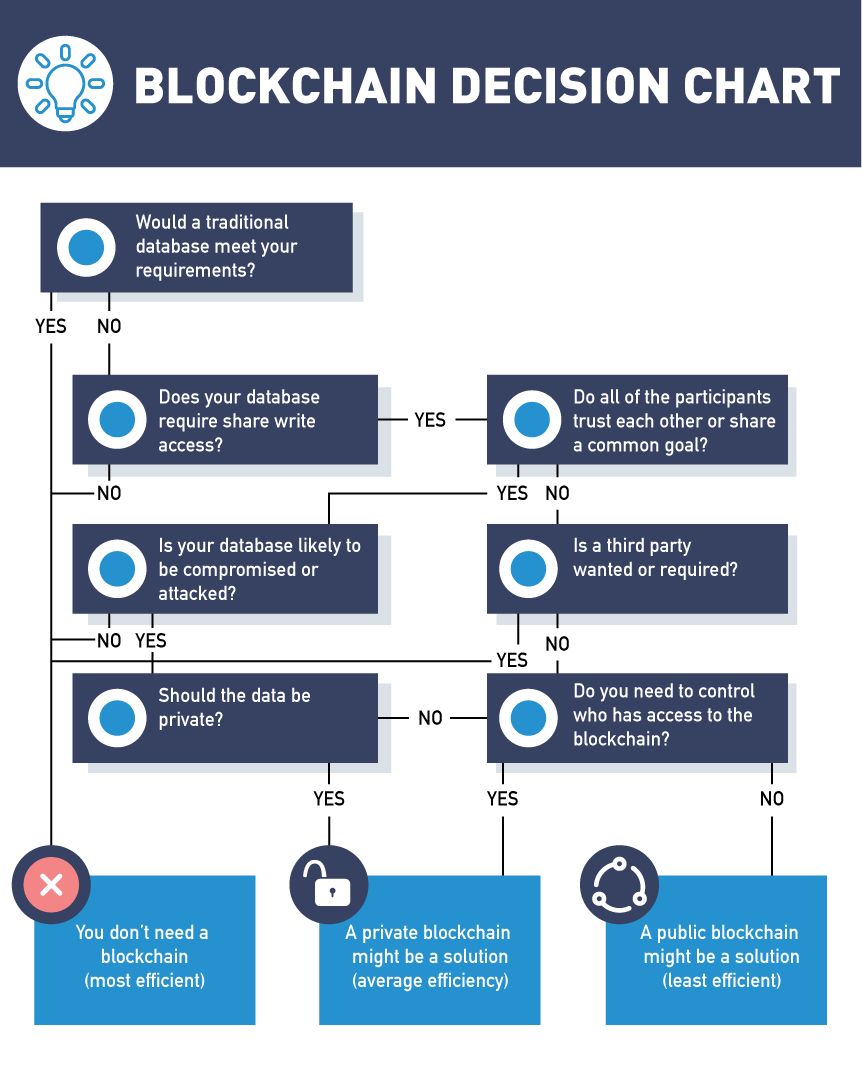
## Is Blockchain Right for You?

Consider the following aspects before deciding if blockchain is for you:

* Blockchain decisions  
  When it comes to decision making around which blockchain model to use, it's important to determine which platform and structure is right for your business.
* Intermediaries  
  Blockchain implementations can eliminate middlemen from work processes.
* Central authority  
  Some organizations rely on one person having control, with blockchain decentralized work flows without a single point of failure are emerging.
* Multi-party interaction  
  Blockchain provides a trust layer that opens up new opportunities for participation.
* Visibility  
  Blockchain transparency reduces dispute over what is in the ledger since agreement occurs before transactions are committed and everyone can have access to the ledger.
* Write access  
  Public permissionless blockchains do not prohibit who can add blocks to the chain, where private permissioned can restrict access.
* Value transfer  
  Blockchains can differ in the ways participants transfer value.

## Blockchain Decision Chart

Let's take a look at the blockchain decision chart:



## Questions to Ask When Deciding on Blockchain

Discussion on these topics need to be addressed when making the decision to adopt a blockchain strategy for your company:



## Blockchain Is Like Hot Sauce

One important thing to keep in mind as you're evaluating blockchain, is it's like hot sauce.

And I want to give credit where credit is due for this analogy.

This was inspired by a friend of mine, Samson Williams, a thought leader in the blockchain space.

But Samson loves to talk about blockchain being a lot like hot sauce.

Hot sauce is surprising because you can put it on a number of things and it really tastes good.

But there are some things hot sauce just doesn't belong on.

You'd never put hot sauce on an ice cream.

Understand that blockchain is like hot sauce - there are a lot of areas you can add a little splash of blockchain to, and end up making a much better and more compelling solution.

But there are some areas that you can't add blockchain to without making things a lot worse.

And just like hot sauce, there is a big misconception that blockchain is an all-or-nothing proposition, that if we're going to architect and develop a solution on blockchain, we either have to build something that exists entirely on blockchain, or we need to build something that exists entirely on conventional technology.

The truth is that like hot sauce, blockchain is really best when it's combined with something.

If you were hungry and poured yourself a big bowl of hot sauce, not only would you be unsatisfied and unhappy, but you wouldn't want to repeat the process again.

That's the same way with blockchain.

If you are looking at building a solution completely and entirely on the blockchain, without exploring some of the amazing potential that you get by combining blockchain with conventional technology, then you probably got a bad recipe.

So, when you're thinking about blockchain, and how to add it to your personal and professional life, understand that it's not a meal all by itself.

It's just a little splash of hot sauce you put on something that already works pretty well.

## Blockchain Considerations

Companies must consider many factors when deciding how blockchain will fit into the business model. There is not a “one size fits all” blockchain but rather a well-thought-out approach that considers many options.

* Governance  
  Governance of blockchains deals with a system for managing and implementing changes to blockchains. Chapter 4, “Blockchains and Governance”, covers how blockchain is managed and how changes are implemented.
* Smart contract functionality  
  Each organization has unique needs when deciding on smart contract functionality. Such decisions as to the design, implementation and testing of these digital promises need to be determined. Can smart contracts replace or accentuate current work flows? Can a previously written smart contact fit in the current business model?
* Consensus algorithms  
  Consensus models change depending on the type of blockchain environment you are creating. In order for a blockchain to work, the participants must come to an agreement as to the transactions in the ledger or the state of the ledger. This agreement is called consensus. Public blockchains have miners that are incentivized to reach consensus whereas private blockchain set up enterprise nodes that agree to the state of the ledger. We will discuss consensus models later in this chapter.
* Integration  
  Consideration for current work flows and how to bridge blockchain platforms with existing systems are a vital conversation. How can blockchain add value to your current organization while leveraging your existing systems?
* Cryptocurrency requirements  
  As mentioned previously, a cryptocurrency is a medium of exchange digitally enabled by blockchain. Cryptocurrencies secure and keep track of assets on a public blockchain. Enterprise blockchains generally do not use the cryptocurrency feature. Decisions on if and how your blockchain will exchange value among participants are important discussions that need to occur during the design phase.
* Cost modeling  
  New questions arise around consortium type blockchains, one consideration is how to split the technology cost among the participants in a fair and equitable manner.

Overall, blockchain decisions will be made by actors in the blockchain system:

* System Architects design and build blockchain networks. This includes decisions on node types and membership rights.
* System Developers design the smart contracts for the community to use.
* System Operators interact with the software, permissioning and onboarding participants. This includes storing the ledger, creating wallets and managing credentials.
* Blockchain Users join a blockchain by setting up a wallet and/or receiving permission to engage in a particular function.

## Blockchain Transaction Flow

In this section, we'll discuss the blockchain transaction flow.

Regardless of the blockchain technology, the flow of data through a blockchain will remain relatively the same, at least at a high level.

It will all start with a blockchain user performing an operation that should be stored on the chain.

The operation will trigger a smart contract, or it will trigger chaincode.

In either case, the code will be executed on the actual blockchain itself.

The output of this code will result in a transaction, and that transaction is what we intend to be stored on the blockchain.

Next, the blockchain operators using protocols that will be specific to the specific blockchain that's running on will spread that transaction throughout the blockchain network.

The block creators will collect all of the transactions and it will create a new block.

In most blockchains, this is the job of the miner and is the output of the mining process.

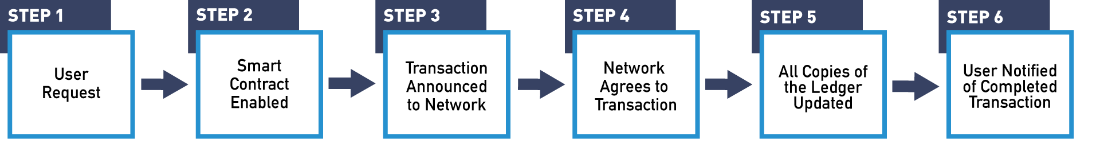
The block operators will spread the block through the peer network to update the ledger copies once consensus has been achieved.

And this results in the block operators again executing code included in transactions within the block to update their own copy of the internal state of the blockchain.

The users will be notified of an event from a blockchain creation via an event.

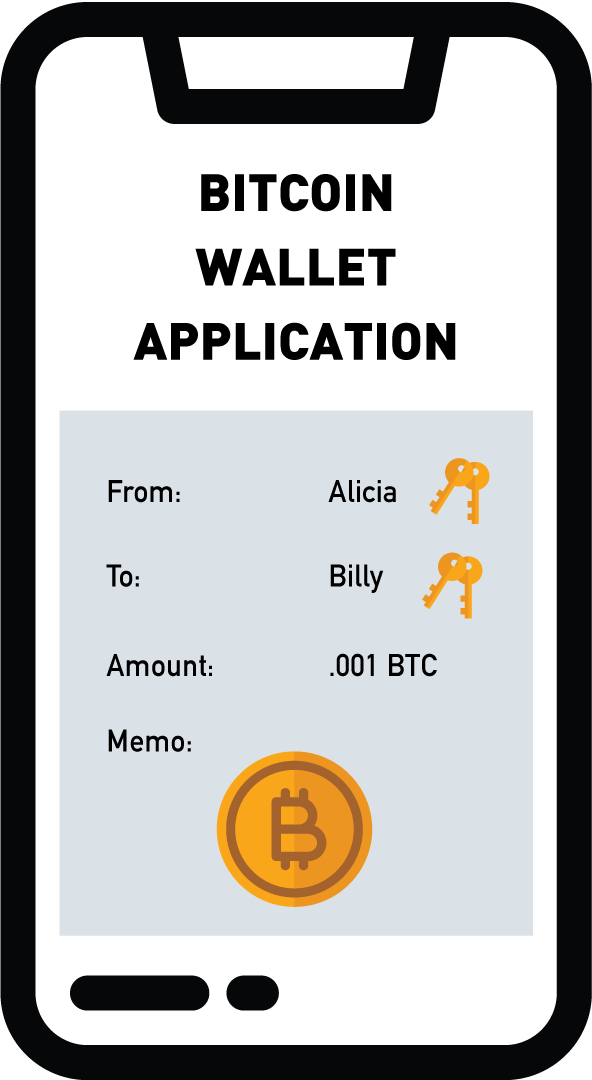
## 3.5 The Blockchain Transactions

Although blockchains can differ in form and function, all follow a basic transaction flow.



**Step 1: Operation Initiated**

Let's follow the step with a basic Bitcoin transaction. If Alicia wants to send Billy some bitcoin, she would go to a Bitcoin wallet application either on her phone or computer where she has some Bitcoin stored. Wallet applications are usually free downloads that create a digital wallet to purchase and/or store your cryptocurrency.



It is worth mentioning here that cryptocurrencies are a function of a particular blockchain, the Bitcoin blockchain only transacts bitcoin and the Ethereum blockchain can only exchange Ether. To initiate the transaction, Alicia would make a request of the system to send Bitcoin to Billy’s wallet by specifying the amount and Billy’s Bitcoin address.

**Step 2: Smart Contract Triggered**

When Alicia sends her transaction to the network, it triggers a smart contract that checks with the nodes on the network to make sure Alicia has the currency to spend, and that she hasn't already spent it. Once checked, the transaction is added to a proposed block.

**Step 3: Operators Spread Transaction**

Proposed block is communicated to the network through the peer-to-peer protocols.

**Step 4: Consensus**

In order for the Bitcoin network to validate a block, nodes or miners must validate the correctness of a block by completing a math problem first. The node that completes the Proof of Work equation first is rewarded with some newly minted Bitcoin. Once a solution for the equation is reached, the other nodes can easily check its accuracy, thereby accepting the new block onto the blockchain.

**Step 5: Spread the New Block**

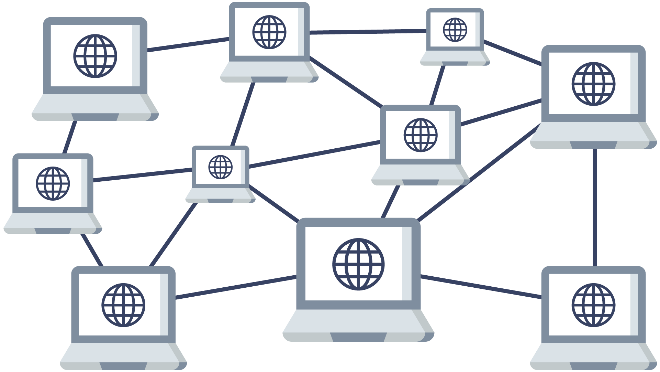
This block is spread throughout the network through the same peer-to-peer communications we used for the transaction. When block operators receive a copy of the new block, they add it to their copy of the distributed ledger. This guarantees that all members of the peer network agree on the current state of the blockchain’s distributed ledger.

**Step 6: Transaction Completed**

The user’s wallet monitors for the creation of new blocks that include transactions associated with the user. When a block containing the completed code from the user’s operation is received, an event is created to notify the user that the operation is complete. When the block containing Alicia’s Bitcoin transfer to Billy is added to the blockchain, an alert will be sent to the affected wallets that the transaction was accepted and completed.

## 3.6 Consensus in Blockchain

Consensus in blockchain is moving away from a centralized system where one entity keeps track of the ledger towards a decentralized system where trust does not rest with one entity but all entities and what they decide together. The blockchain is a distributed and decentralized system, which means that it needs to have a way of tracking the official current state of the system. Since the blockchain can include financial transactions and business agreements, it is important that all parties involved are in sync regarding the terms of the agreement.



In this section, we will discuss the details of how a blockchain network comes to agreement on the contents of the blockchain.

## Consensus

One of the most important components to blockchain is this idea of group consensus.

As we talked about in an earlier module, blockchain is inherently a very inefficient system.

We're asking multiple nodes, sometimes tens of thousands of computer nodes, to all repeat the same work: they're all keeping a copy of the same data.

And the reason we agree to this tremendous inefficiency is because if we can get all or most of those nodes to agree on what the truth is.

We can have a lot of trust that that's actually the truth, that that record hasn't been tampered or altered or changed in any way.

Consensus is one of the underpinnings of blockchain.

There are several different methods we use right now to have all these nodes reach consensus.

Essentially, when we talk about consensus, you can think of every block in a blockchain as being like a sheet of paper.

It's got a fixed amount of space. We write a transaction on every line, and when that sheet of paper is full, it's important that we all, as a group, come together and compare our different sheets and select the sheet or the version of paper that the majority agree with.

And so, there are several different methods that we use to come to consensus on a block.

The oldest and most widespread method is what's called Proof of Work.

And you'll see in another module, we actually dive into Proof of Work hands-on, and show you live what Proof of Work looks like and how it actually works.

Proof of Work has served us well for the past nine, almost ten years, got its start in Bitcoin, and it's used in every major public and most private blockchain offerings.

But we're also starting to see some of the limitations of Proof of Work.

One of the big limitations behind Proof of Work right now is how big and how fast it can scale.

Currently on Proof of Work blockchains, we're able to process somewhere between 50 and 20 transactions worldwide per second, which may sound like a lot until you realize that modern payment processing networks like Visa can scale up to over 70,000 transactions a second.

So, in order to compete with conventional technology, blockchain really needs to add a few more orders of magnitude to that transaction rate.

There are many proposed alternative consensus methods for how we might be able to reach that kind of scale.

There are things in production right now like Tangle which use a blockless solution, and they're also new and emerging consensus methods like Proof of Stake, or Proof of Activity that we're currently examining to take the work out of Proof of Work.

We also have another module in this course where we talk about Proof of Stake, and then another one where we compare Proof of Work versus Proof of Stake.

If you're curious about any of the details of how these consensus mechanisms are actually implemented, be sure to check out those modules.

But the takeaway point to understand is that, it's this consensus, it is this idea of asking all of these nodes, potentially tens of thousands of nodes, to all repeat the same work and then periodically come together and agree on whatever the majority select the right version of the truth to be.

That gives blockchain that high level of trust and that makes it such a secure record store.

## Introduction to Consensus in the Blockchain

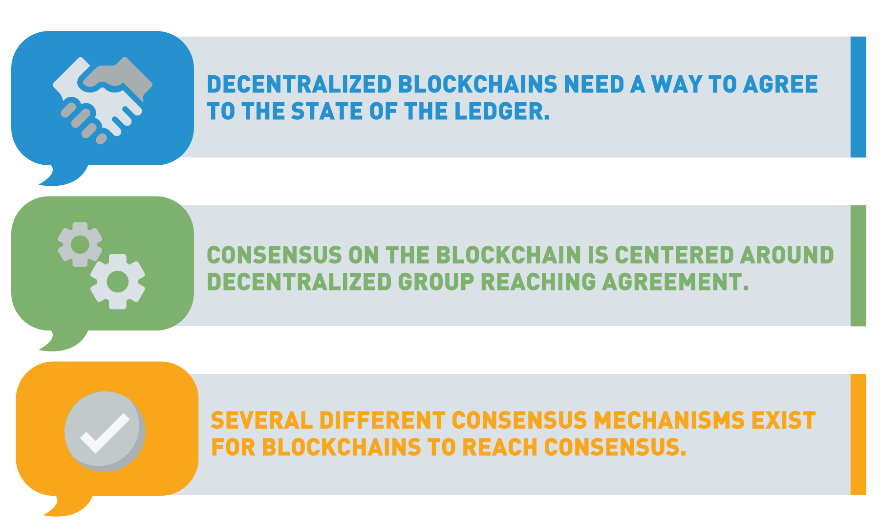
As discussed in the [*"Blockchain Consensus and Fault Tolerance In a Nutshell"*](https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03) article by Demiro Massessi,

"The blockchain is designed to be a shared, synchronized historical ledger, meaning that there needs to be a final decision at some point on what should and shouldn’t be included in the official record. Since blockchain is decentralized, there is no "higher authority" that can rubber-stamp and finalize the contents of a blockchain block.

The method that [*Satoshi Nakamoto*](https://en.wikipedia.org/wiki/Satoshi_Nakamoto), creator of the Bitcoin network, invented to achieve consensus is based on scarcity. In one way or another, blockchain consensus algorithms boil down to some kind of vote where the number of votes that a user has is tied to the amount of a limited resource that is under the user’s control. Based on the economic law of supply and demand, collecting enough of an asset to have a controlling share will drive up the price of the asset enough to make achieving that level of control unfeasibly expensive".

## Consensus Mechanisms

In order to ensure no one spent the same Bitcoin twice, Satoshi Nakamoto created the consensus algorithm called Proof of Work for the Bitcoin network. Since then, several other consensus algorithms have been invented to fit different use cases. These include Proof of Stake, Delegated Proof of Stake, Practical Byzantine Fault Tolerance, and Proof of Elapsed Time. The most commonly used consensus algorithms are Proof of Work and Proof of Stake.



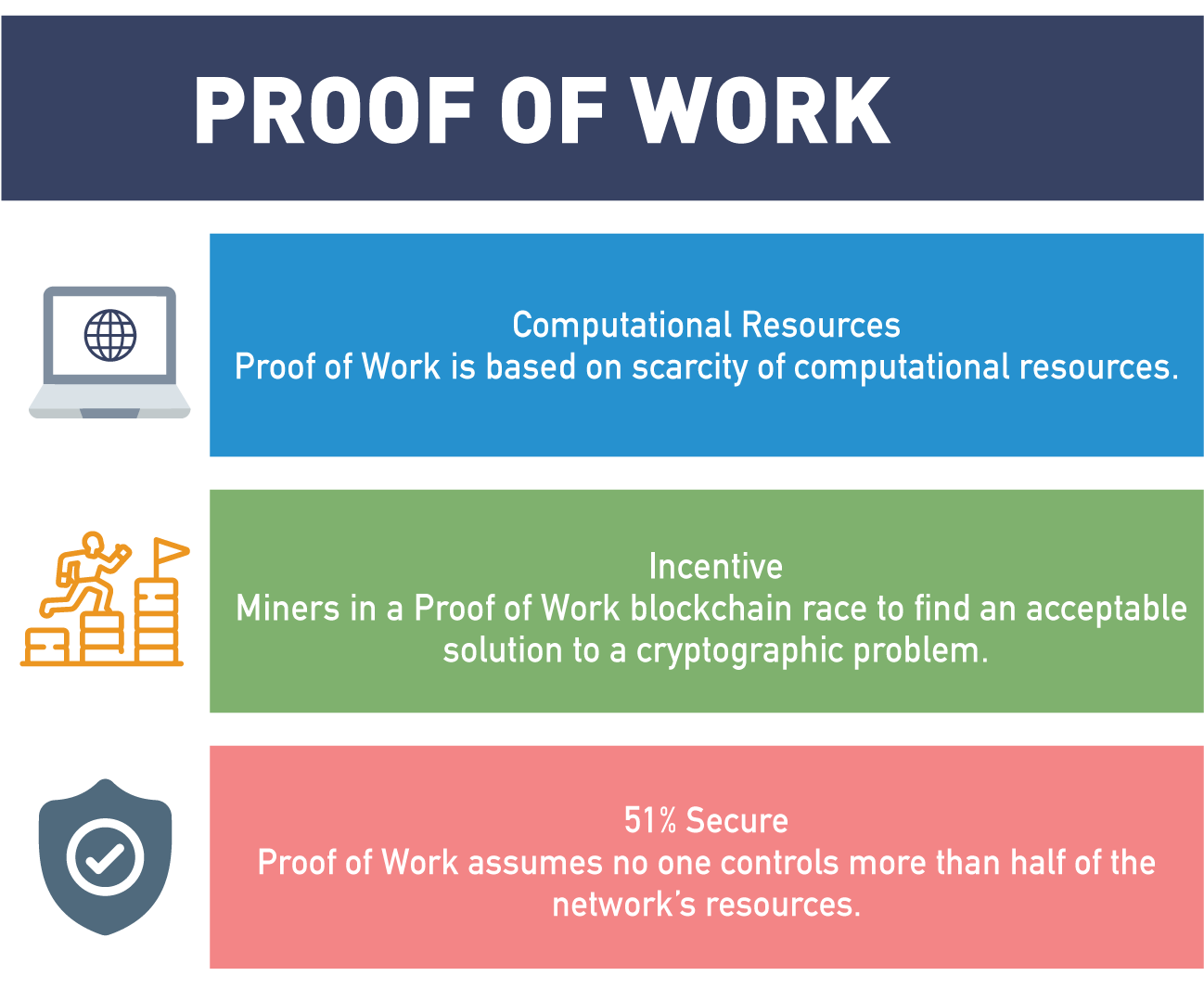
## Proof of Work

As explained in the [*"Blockchain Consensus and Fault Tolerance In a Nutshell"*](https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03) article by Demiro Massessi,

"In Proof of Work, users in the blockchain network who want to create the next block (and win the associated reward) are called miners. To win the right to mine a block, miners race to find an acceptable solution to a “hard” cryptographic problem. (...), “hard” mathematical problems can only be solved by random guessing. When a miner finds an acceptable solution, they create a block and broadcast it to the network, finalizing that block.

Proof of Work exploits the scarcity of computational resources by choosing a problem that can only be solved by guessing. There is no limit on the number of guesses that a miner can make at once. Proof of Work, therefore, incentivizes miners to run as many mining machines as possible to maximize the probability that they are the first to find a solution to the problem. Since mining computers take money to purchase and money to run, the amount of control that a user can exert over the blockchain is limited by the amount of money they have available to invest in mining equipment".

Also, the process of mining requires computing power that runs on electricity. Some argue the Bitcoin network is not sustainable because of its increasing need for electricity. The argument against this assumes Bitcoin miners are out to make a profit and by using renewable energy sources to power the mining operations they will be more profitable. As a result of seeking out carbon-friendly energy sources, mining companies will bring new renewable energy solutions to the power grids.



The security of the Proof of Work consensus is based on the assumption that no one controls more than half of the computational resources of a blockchain’s mining network. If one entity controls 51% of the mining effort, they control consensus. To take control would require a huge investment in equipment and energy, more than would be gained by defrauding the system.

## Proof of Stake

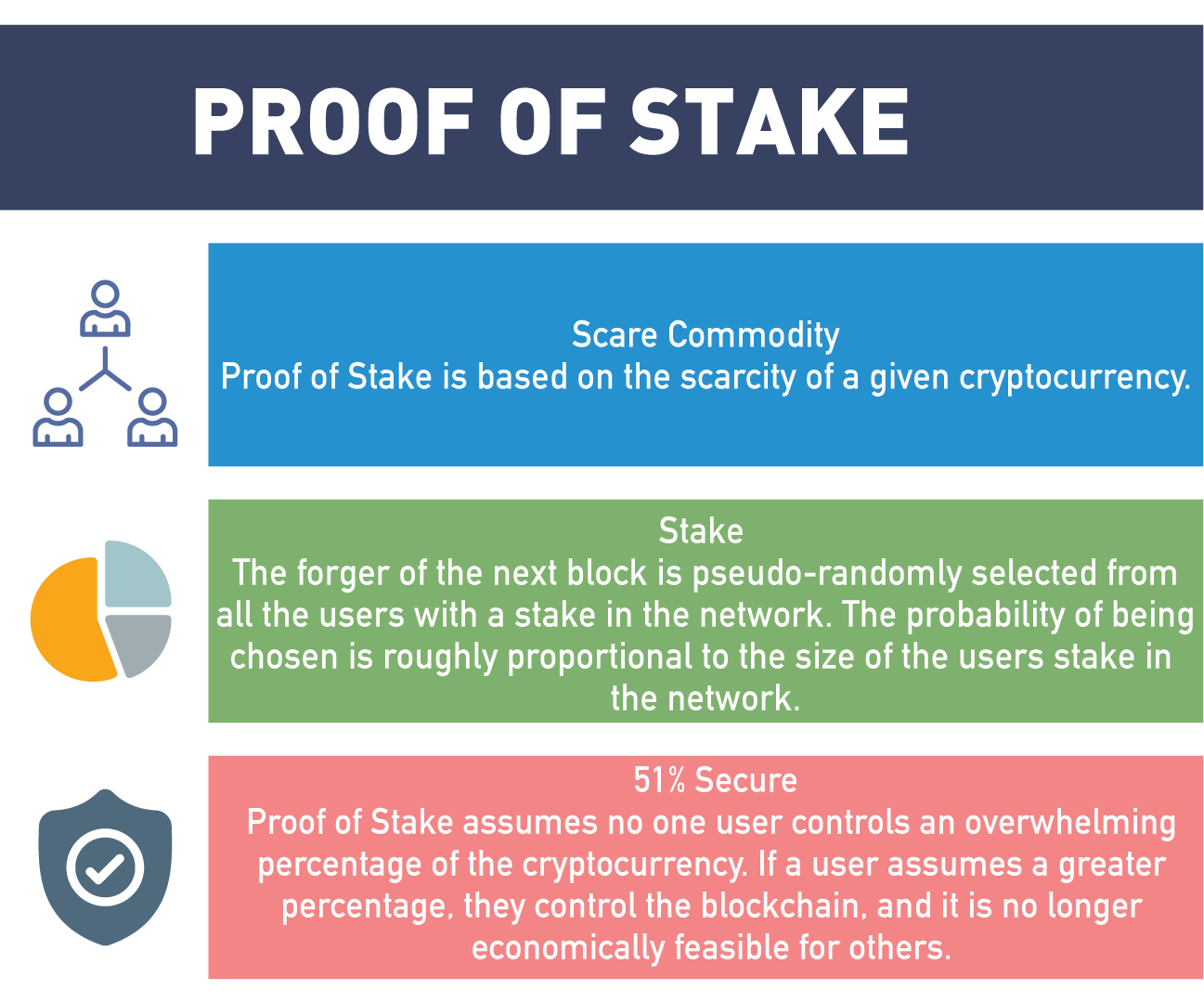
Proof of Stake comes with a number of improvements to Proof of Work systems, it requires less energy and has a lower barrier to entry since no specialized hardware is required to create blocks.

In the same [article](https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03) that we mentioned on a previous page, the author explains,

"Users in a Proof of Stake blockchain can "stake" or promise not to use the tokens they own. This gives them the opportunity to be selected as the next user to create or "forge" a new block and earn the reward. A block forger is pseudo-randomly selected from all of the users who have staked some of their assets, and the selection process is biased based on the size of the stake.

For example, imagine that a wheel is divided into sections where the size of a section is proportional to the size of a user’s stake. The next block creator would be chosen by spinning the wheel and seeing whose section comes out on top. In Proof of Stake, each user has a copy of the wheel and they are all synchronized so that each person can independently determine the selection and get the same result. This is why Proof of Stake uses a pseudo-random instead of a random selection process".

In Proof of Stake, an attacker needs to control enough of the staked currency to guarantee they will be selected to create every block. Since cryptocurrency is a limited asset, buying up enough of it to do this is expensive, making attacks on Proof of Stake systems economically infeasible.

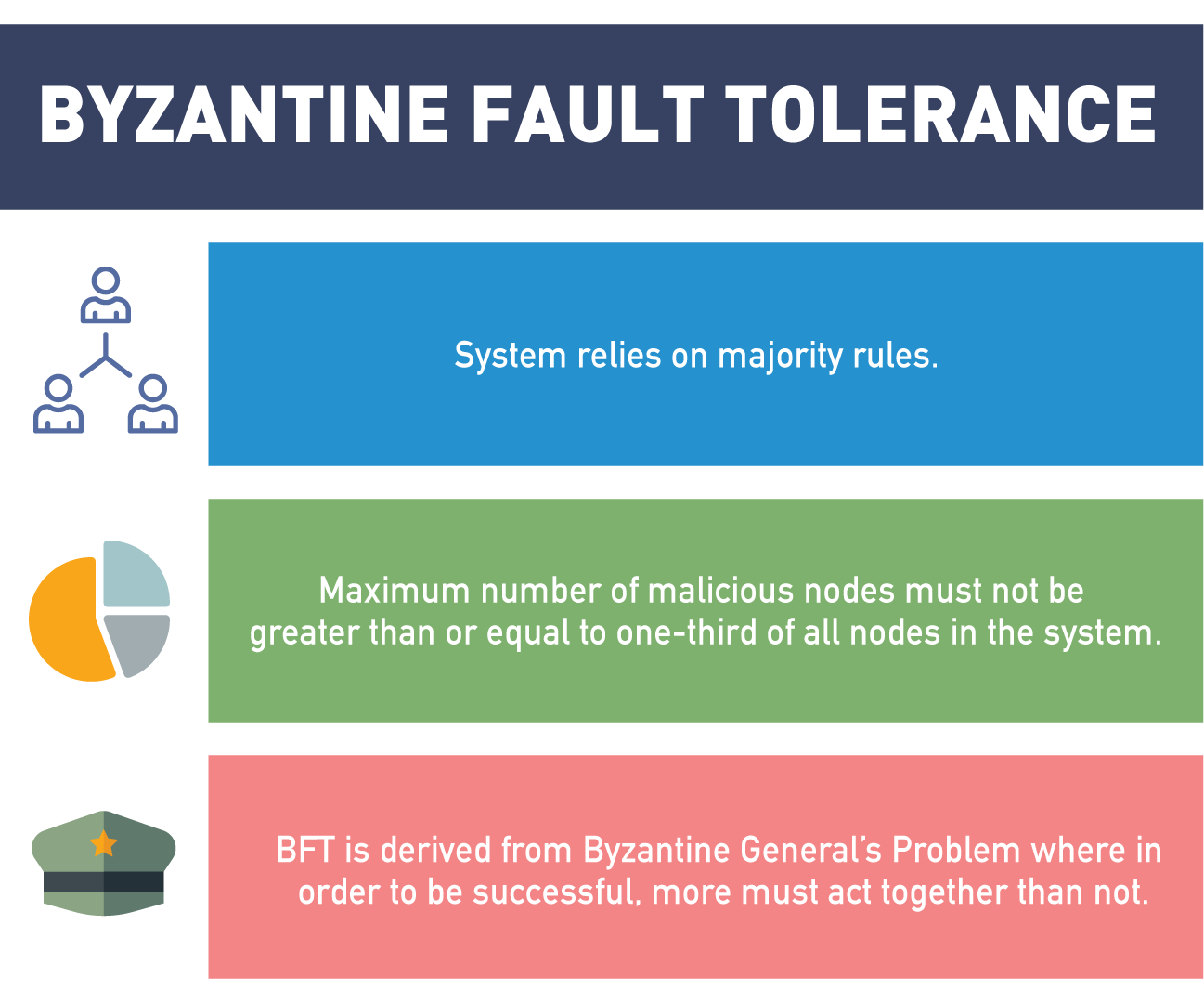


## Fault Tolerance in the Blockchain

In blockchain, it is essential all participants agree to the state of the ledger. Shared decentralized ledgers arrive at network agreement or the state of the ledger by consensus algorithms. But what happens if all participants in the network don’t agree? Let's discuss the concept of Fault tolerance and why it is an important blockchain concept.

As described by [Demiro Massessi](https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03),

"Blockchain is a distributed, decentralized system that maintains a shared state. While consensus algorithms are designed to make it possible for the network to agree on the state, there is the possibility that agreement does not occur. Fault tolerance is an important aspect of blockchain technology".



## Fault Tolerance

One of the things we've talked about extensively in this series is how inefficient and redundant blockchain is and that is by design.

That's what gives us immutability.

And another thing it gives us is an extreme level of fault tolerance.

At its heart, blockchain runs on a peer-to-peer network architecture in which every node is considered equal to every other node.

And unlike traditional client-server models, every node acts as both a client and a server.

And so, we continue this redundancy down at the network level, where we're asking all these nodes to perform the same work as all these other nodes.

Like any peer-to-peer system, we have an extremely high degree of fault tolerance.

In fact, if we have two or more nodes online in a blockchain system, we still have a working blockchain.

And when you think about that amazing fact given the scale of major public blockchains, you can see the inbuilt fault tolerance.

Let's look at Bitcoin for an example.

That's a blockchain that consists of over 30 thousand nodes coming to consensus on every block.

As long as we have two or more of those nodes online and able to communicate, we still have a working solution.

That gives us a tremendous margin for error, for nodes coming and going offline, for network transport issues, and it makes blockchain really, really a great platform to use in environments with less than ideal networks and power infrastructure, because we can have nodes come offline, go back online and when a node comes online after being offline for a while, all it has to do is sync up, and get all the data that it missed while it's been offline from all of its peers, and then it's right back online participating like all the rest.

This is very different from the centralized systems that blockchain aims to replace.

In a traditional client-server model, if that server is offline, those clients have no way of getting the data that they requested or performing the operations they'd like to perform.

This is not the case in blockchain.

And if we look back historically at other peer-to-peer solutions, solutions like Bittorrent or Napster, we've seen the tremendous difficulty that authorities have had taking some of these networks offline.

That is due to the fault tolerance you get from a peer-to-peer architecture.

In fact, we saw this recently during the Arab Spring, when the Egyptian government decided one night to shut down Internet access for the entire country.

Well, within 24 hours Egypt was back online and connected to the Internet through a network-sharing mechanism known as mesh networking, which at its heart is just a peer-to-peer method for sharing Internet connectivity.

We know that peer-to-peer has a long history of providing extremely high fault tolerance and reliability, and that's why we've chosen to build a platform like blockchain on top of it.

If you're looking for a solution platform that offers you that kind of incredible fault tolerance, if you're looking to deploy a solution into areas with less than ideal infrastructure or under conditions where nodes may come online and go offline frequently, then blockchain may be a really good platform to look at.

## The Byzantine Generals' Problem

The Byzantine Generals' Problem has been thoroughly explained in the [Medium article](https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03) by Demiro Massessi,

"The Byzantine Generals' Problem is a scenario designed to demonstrate the difficulty of multiple parties coming to an agreement when communication can only be accomplished on a one-to-one basis and is untrusted. In the story, several Byzantine Generals are besieging a city with their separate armies. If they all attack together or all retreat together, they will be ok, but if some attack while others retreat, they will be destroyed.

The generals can only communicate by messengers, who could be intercepted and forced to carry fake messages, and one or more generals may be a traitor. The goal is to find a way to achieve a consensus on strategy despite the possibility of traitors and false messages. Presumably, all generals will abide by what they believe is the majority consensus. The Byzantine Generals' Problem is solvable as long as two-thirds of the generals are honest.

Blockchain is designed to be Byzantine Fault Tolerant, meaning that the network will come to a consensus on the official state of the blockchain, despite the fact that some members may misbehave. The solution to the Byzantine Generals' Problem is inefficient, so the blockchain needs some way of being confident of consensus without going through a full solution".

## Proof of Work vs. Proof of Stake

We've talked a lot in this course about Proof of Work versus Proof of Stake.

Proof of Work is the oldest and the original consensus protocol. It's coming up on its tenth anniversary; first one into production with Bitcoin back in 2009.

And as a consensus protocol, it served us very, very well.

There have been a number of hacks and exploits that have been committed against various smart contracts and solutions written on top of the blockchain.

But for almost a 10-year history with over half a trillion dollar market cap, no one's been able to successfully exploit Proof of Work itself, which really shows the security and the reliability of the protocol.

However, there are some shortcomings and criticisms to Proof of Work that are now leading us to look at alternative consensus mechanisms, like Proof of Stake.

One of those is our transaction processing capability.

On a good day, Proof of Work is capable of processing anywhere between 10 and 20 transactions per second worldwide.

This may sound like a lot, but it still leaves us a wide gap to conventional processing powers, that something like Visa's payment processing network which can scale up to over 70,000 transactions per second.

So, in order for blockchain to continue to be a successful solutions platform, we know that we're going to need to find other consensus mechanisms, which allow us to scale up that transaction processing speed into a range where we start to compete with conventional technology.

There are also some other criticisms behind Proof of Work that are leading us to alternative methods, like Proof of Stake.

One of those is the idea of centralization.

As you know from this course, one of the key tenants of blockchain is the idea of decentralization, that no one central authority, intermediary or participant, should ever have too much power or control in a blockchain network.

What we're seeing right now with Proof of Work is an arm's race, where folks are competing with very various specialized pieces of equipment, specialized hardware, specialized mining rigs, in order to mine most efficiently.

And this can be done most efficiently in large data centers where electricity is cheap.

Right now, almost 80% of the processing power behind the Bitcoin network resides in six major data centers in mainland China.

A lot of advocates and blockchain purists think that this is far too much centralization in one geopolitical region of the world.

One way we aim to change that is through Proof of Stake, where we remove the work component of group consensus and we replace it with a very specialized form of gambling or wagering.

The idea of being that if we no longer require specialized hardware in order to come to consensus, we can allow anybody with any kind of device to participate in consensus.

That may be you at home with an old laptop, or a friend with a smartphone, or a tablet, or an iPad, that sits on your nightstand most days and doesn't get used.

This allows for a much wider and more decentralized range of devices and potentially a much larger network size to participate in consensus.

Speed and the idea of decentralization are big drivers behind the move to Proof of Stake.

And we're gonna see how well that works out.

We'll see Proof of Stake finally go live in Ethereum later this year (2018), certainly with more blockchains to follow if it becomes a successful consensus mechanism.

When you hear the debate these days about Proof of Work versus Proof of Stake, and you're trying to understand what do they mean and why are we looking at transitioning from one to the other, understand that we're just trying to overcome some of those big limitations behind Proof of Work, the consensus mechanism that has served us so well to date.

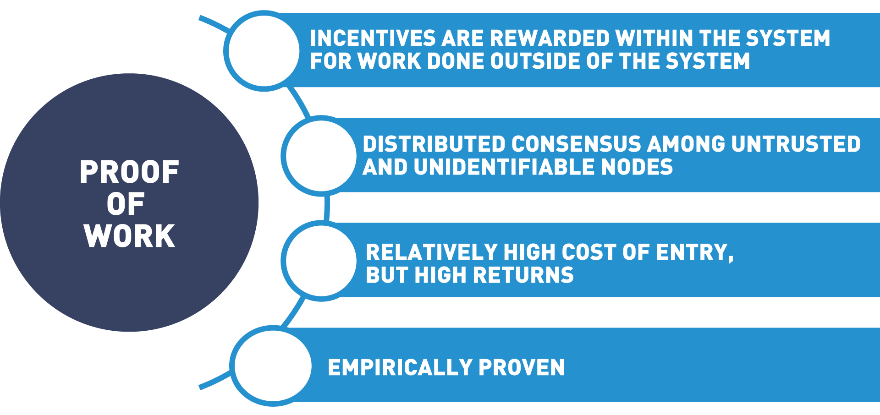
We're trying to find consensus mechanisms that most importantly allow us to scale up, to get our transaction processing power on par with conventional technology, and we're also trying to remove some of the centralized aspects that we've seen form around Proof ofWork.

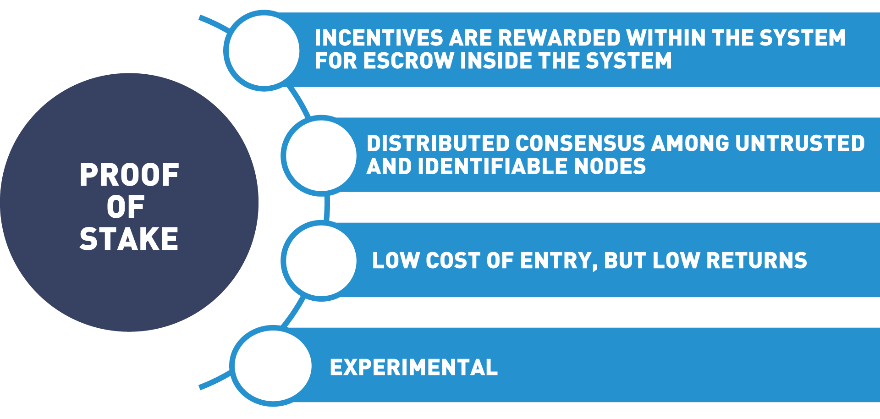
We talk about Proof of Work and Proof of Stake in much greater depth in other modules in this course.

If you're curious about the difference between them, how they work and what the actual implementation differences are, be sure to check out those other modules.

## Proof of Work vs. Proof of Stake

Let's recap differences between Proof of Work and Proof of Stake:





## Bitcoin Consensus Model

Bitcoin, the first blockchain to appear, uses Proof of Work which requires miners to solve a complex cryptographic mathematical puzzle for which they get rewarded. Block rewards are newly minted Bitcoin granted to the miners that solve the puzzle first. Built into the Bitcoin blockchain protocol, is an event called halving. [Bitcoin halving](https://www.investopedia.com/bitcoin-halving-4843769) happens every four years and Bitcoin’s block reward gets cut in half. The halving occurs when the block height reaches a certain point (210,000 blocks) which is programmed into the protocol. The first halving occurred in November 2012 and the block reward was cut from 50 BTC to 25 BTC. The second occurred July 9, 2016 and the reward was reduced to 12.5 BTC. The third occurred on May 11th 2020, cutting the block reward to 6.25. The next halving is estimated in the year 2024 and the reward will be reduced to 3.125 BTC. The Bitcoin network is programmed to produce only 21 million bitcoin and the halving is what keeps inflation in check by slowing down the distribution. About ⅔ of the 21 million BTC have been mined so far.

## Ethereum Consensus Model

Ethereum currently uses Proof of Work for a consensus model. Ethereum was introduced in a white paper by [Vitaly Dmitriyevich "Vitalik" Buterin](https://en.wikipedia.org/wiki/Vitalik_Buterin), a Russian-Canadian entrepreneur and programmer from Toronto. He envisioned the second-largest cryptocurrency when he “forked” or copied the Bitcoin code, made improvements and created the Ethereum blockchain. This new blockchain was not only a currency exchange system but along with the [Ethereum Virtual Machine](https://ethereum.org/en/developers/docs/evm/), an interconnect, turing complete computer, open to programmers to develop. It creates a platform that smart contracts can be executed and applications can be built upon. Ethereum has always planned to move away from a Proof of Work consensus mechanism to a Proof of Stake. Plans for Ethereum to adopt Proof of Stake will occur when [Ethereum 2.0](https://ethereum.org/en/eth2/) is incorporated, this improvement is expected sometime in the second half of 2021.

## Hyperledger Fabric Consensus Model

Hyperledger Fabric is a private permissioned blockchain platform that breaks consensus into components, allowing users to pick a consensus algorithm for their particular situation. Instead of a predetermined consensus model, Hyperledger has an ordering service that performs consensus related events, this ordering component can pick the consensus model that best suits the blockchains needs. By approaching consensus in this modular fashion, Hyperledger DLT’s can change consensus models without huge overhauls to the code base.

As explained by [Demiro Massessi](https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03),

"Hyperledger Fabric deliberately avoided hard-coding a consensus mechanism into the protocol by defining an “orderer component” that performs all of the consensus-related operations. This allows users of Hyperledger Fabric to select a consensus algorithm that fits their use case without being forced to make large-scale code edits".

## Corda Consensus Model

[Corda](https://www.corda.net/) is a private permissioned blockchain. Each Corda network has a notary service made up of independent parties that approve blocks using any applicable consensus algorithms.

As mentioned in [Jamiel Sheikh](https://jamiel.io/#about-me)'s book “Mastering Corda: Blockchain for Java Developers”, R3 provides a set of Corda applications called The Corda Business Network Toolkit to manage one or more Corda networks. Corda does not follow the standard blockchain model of transactions being bundled into blocks and then being finalized by the network as a whole. Instead, a Corda network contains one or more notaries consisting of several independent parties. Transactions in Corda are finalized by a notary with a multiparty digital signature using an algorithm like Raft.

## 3.7 Summary

In this chapter, we discussed:

* Smart contracts and benefits from using smart contracts.
* Differences between blockchain security vs. standard security.
* Differences between private and public blockchains.
* Factors in deciding on blockchain.
* Transaction flow in blockchain.
* Consensus mechanisms used in blockchain.

# 4: Blockchains and Governance

## 4.1 Chapter Overview

In this section, we will cover blockchain governance. We will start by discussing the cooperative way blockchain companies share the computer code for this technology. We will also explore how this open source environment is fostering new innovations. And then we will examine who really is in charge of blockchains and how the network effect determines the direction a blockchain will take.

Next, we will take a look at how these trustless systems with open interactions are more secure than past systems. Finally, we will dive into the idea of collaboration among parties who don't trust each other and how blockchain technology is changing how the global community can interact. This new form of world wide collaboration can be the key to solving the world's toughest problems.

## Learning Objectives

By the end of this chapter, you should be able to:

* Discuss open source communities and blockchain source code.
* Discuss the different types of governance models and what types of governance are used in public and private blockchains.
* Analyze governance types in a blockchain and determine which are used for the more popular blockchains.
* Analyze examples of Decentralized Autonomous Organizations (DAOs).
* Summarize the advantages and disadvantages of a consortium blockchain.

## 4.2 What Is Open Source?

Blockchain technology and the developers who work with it reinforce the basic tenet of decentralization in many ways. Not only by decision making consensus models, but also the way in which it distributes the software code.

* Proprietary/closed source code  
  Software controlled by the person, team or organization who created it and maintains exclusive rights over it. Only the original authors can legally copy, inspect, and alter the software. Most users of proprietary software sign an agreement giving permission to use the software but not alter it. Microsoft Office is an example of proprietary software.
* Open source code  
  Computer code that describes a specific approach to creating software. When describing tools for distributing open source code Discipline Tools states, Open source initiatives embrace and celebrate principles of open exchange, collaborative participation, rapid prototyping, transparency and community-oriented development. Open source software is code that anyone can inspect, modify and enhance. Much of the Internet was built on open source technologies. Users of the computer software never interact with the source code, rather it's manipulated by programmers who improve and fix it. As with proprietary software, users must accept the terms of the license, but they are dramatically different structurally. Linux and Kubernetes are examples of open source software.

Open source software fosters collaboration by sharing code and encouraging modifications and improvements. Instead of charging for the software program, software developers find it more lucrative to charge for service around developing and maintaining these open source projects.

## Benefits from Open Source Software

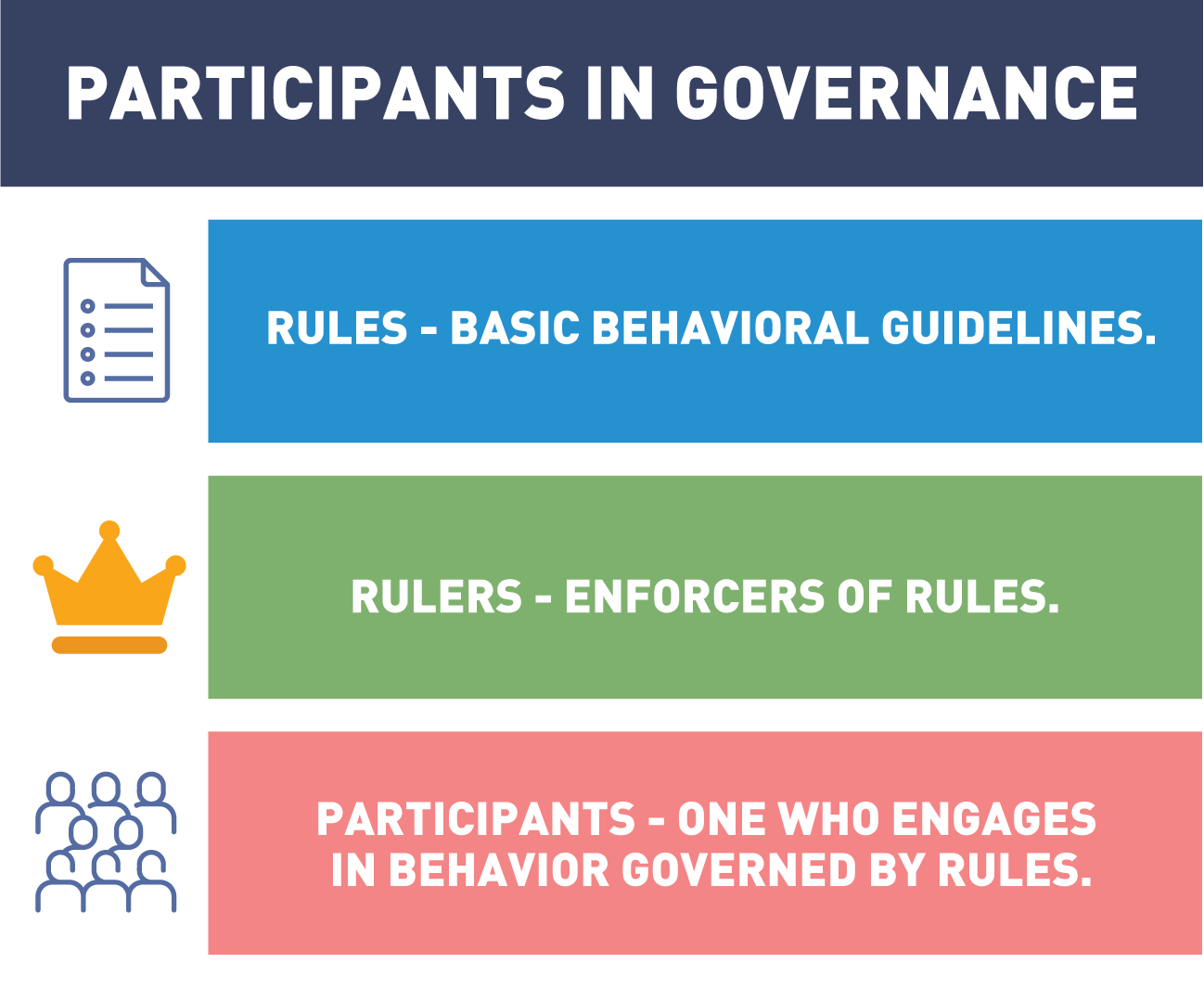
Developing software in an open source environment means a willingness to share and collaborate in a transparent way.

* Control  
  To a developer's open source means an individual can contribute to the direction the code takes. This open participation means coders who participate the most have more influence over the direction of the code.
* Training  
  The ability to copy code and make your own changes in test environments act as invaluable hands-on training. This also fosters innovation as programmers can devise previously unthought-of functionality and code direction.
* Security  
  In open source, software programs are considered more secure because they are open to peer review where errors can be spotted. Coders are encouraged to test code, find errors and develop fixes to bugs as long as they follow the process the network has in place.
* Stability  
  Open source projects have a certain amount of code stability due to the openness for public review. A publicly distributed source code is openly reviewed and can expose situations that may not have otherwise been tested.
* Community  
  Open source inspires the community to get involved. When contributing to an open source project, you join a community of people that ultimately affects the software you are interested in.

The programming code for Bitcoin, Ethereum, Hyperledger and other blockchains is open source.

## 4.3 Introduction to Governance

Humans are tribal by nature, we tend to attract each other and build tribes, villages, towns, cities, states and countries. With these interactions comes a need to direct the behavior of the group. These directions become the social norms among those who are living with or near each other. These norms become the rules by which the behavior of the group is governed. It doesn’t matter if the governance is the real world or the digital world, there are shared underlying principles within both. Let's take a look at who is involved.



Governance can be undertaken by a government, market, network, organization, social system or family.

For a governance process to work effectively, the above three principles will need to agree to the rules that govern the behavior. The rules should be aligned with the overall participants' goals, and the leaders should have the ability to enforce positive and negative actions.

Now that we have a simple understanding of governance, let’s analyze how this is taking place in both the standard world and the blockchain world.

## Governance Explained

Every business wants to make sure it's getting the best out of technology spending.

IT governance is a formal framework that provides a structure for organizations to ensure that technology investments support business objectives.

Now we all know that, despite our best efforts, things occasionally do go wrong.

A large part of modern governance efforts includes planning for disasters in a way that ensures business continuity - the ability to remain available to customers no matter what.

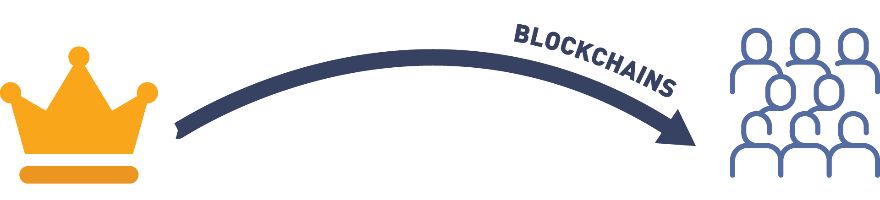
Modern decentralized solutions are most often created in a cooperative or consortium format - a shared joint effort business organizations.

In these initiatives, it is important not only for clear and comprehensive governance to be in place, but for that governance to be consistent across participating organizations.

These type of cross-organizational governance efforts represent an entirely new type of project initiative, and will require business analysts, solution architects, product and program managers, and executive leaders who understand the incredible potential and massive disruption that decentralized solution architectures bring to focus.

## Governance Models

A basic description of governance can be defined as a system by which behavior is directed. This direction is guided by a set of norms or rules and a way to enforce or keep order. The mechanism to enforce these policies can take many forms from a dictator who has complete control to a democratic governance model where the voice of the majority is recognized.



Blockchain governance models reflect a more democratic flavor due to the open source environment. Blockchains are composed of a community of users who work together to strengthen the system. The degree in which the majority rules can vary.

* Representative democracy  
  This type of governance has a few individuals, empowered by the group, to suggest new rules and guide future direction. The amount of authority the representative has is granted by the majority. The representatives selected reflect the views of the majority and are given authority to guide the community. The control comes from the community and representatives are presumed to act in the best interest of the governed. This type of governance is more efficient as only a few debate the issue and decide on policy. Issues can occur when the majority opinion unevenly reflects the community, causing minority groups to be underserved. Also the assumption is that the representatives are acting on the best behalf of the group and not in their own best interests.
* Direct democracy  
  All decisions regarding the governance of the group are voted on by the entire community. In this form of governance model every vote counts and people have more control over the quality of policies. In this model it is best to have an educated community where everyone is willing to participate for the good of the whole.

## How Does Blockchain Fit Into Governance?

Each and every blockchain ecosystem that has or is being created will need some kind of governance mechanism in place. As discussed in the [*“Bitcoin and Blockchain Governance: What It Is and Why It Matters”*](https://www.bitcoinmarketjournal.com/bitcoin-and-blockchain-governance/) article by Evan Karnoupakis, traditional systems and laws are made and then enforced. When participants (miners, developers, and users) in the network are interacting, ideally they are acting in a way that’s best for the overall group. Being able to build a governance structure in a decentralized (sometimes anonymous, as well) world has proven to be extremely difficult, but this is a problem that many DLT companies are in the midst of solving.

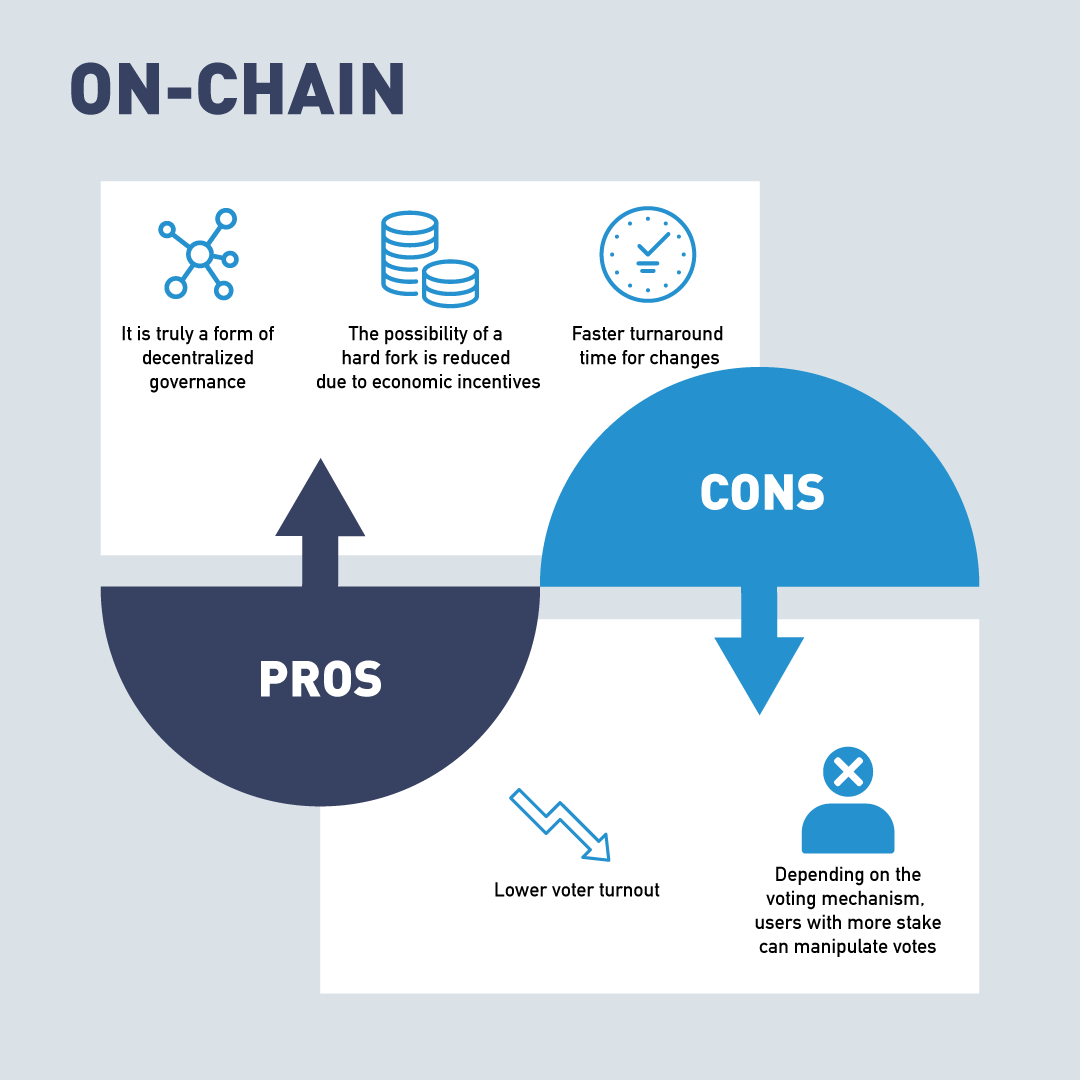
Most governance structures in the blockchain ecosystem are looking to achieve similar goals, such as:

* Protocol changes and technical upgrades.
* Critical bug and vulnerability fixes.
* Using pooled funds for research and development.

## On-Chain vs. Off-Chain Governance

These goals can be achieved through many different methods of governance. When designing a blockchain, choices between on-chain and off-chain governance must be balanced.

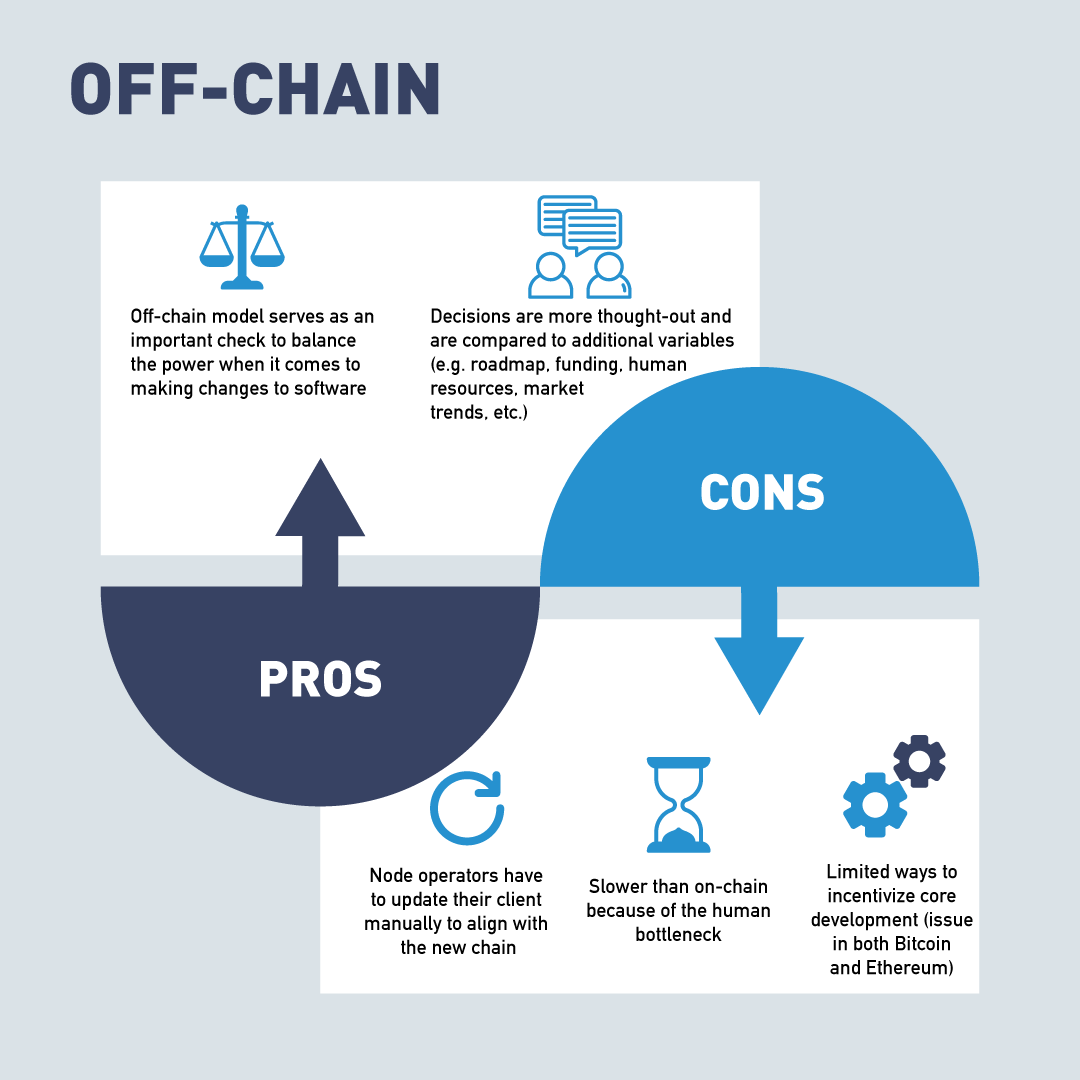
In the on-chain governance, rules for instituting changes are encoded into the blockchain protocol. This means that any decision being made is automatically being translated into code (e.g. decisions concerning block size). Developers propose changes through code updates and each node votes on whether to accept or reject the proposed change.



On the other hand, as discussed in the Medium article [*"Revisiting the On-chain Governance vs. Off-chain Governance Discussion"*](https://medium.com/@poolofstake/revisiting-the-on-chain-governance-vs-off-chain-governance-discussion-f68d8c5c606),

"Off-chain governance can be seen as decision-making that first takes place on a social level and is later actively encoded into the protocol by the developers. For instance, Bitcoin developers share their improvement proposals (BIPs) through a mailing list, whereas Ethereum collects improvement protocols (EIPs) on GitHub.

Fred Ehrsam (Coinbase co-founder) argues that the Bitcoin governance system resembles the checks and balances system of the US government. Just like the Senate, developers submit a pull request to the community, the miners take the role of the judiciary who decides whether or not proposals are adopted in practice. Lastly, the users are just like citizens in a nation or state and can revolt and switch protocols or sell their tokens".



## What Is Blockchain Governance?

In the previous chapter, we discussed the decentralized characteristics of blockchains. But if blockchains are decentralized, how are decisions made and by who? Open source software organizations and open source software development projects need a way to manage projects. Most organizations are centralized and have a set leadership team. Before getting into the details of how governance works on the blockchain, it’s important to have a clear definition of what blockchain governance is.

In order for a blockchain to survive, it must adapt to the needs of its users and advances in technology. The way the changes are debated and decided upon is important for these decisions to be implemented. A decentralized ecosystem is designed not to be under the control of a single source, there is no CEO to take responsibility for issues. This means blockchains need a new strategy for governing the policy it wants to adopt.

Strategies must include incentives so the members want to be good actors in the system. The efforts of the group must be coordinated to be productive. Both of these elements are necessary in blockchain governance models.

## Blockchain Governance Strategies

Several different blockchain governance strategies have been proposed and implemented for different blockchains. Let's review some blockchain governance strategies sorted from the fewest to the most members directly involved in the decision, as discussed in the [*"Blockchain Governance In A Nutshell"*](https://medium.com/coinmonks/blockchain-governance-in-a-nutshell-67903c0d2ea8) article by Demiro Massessi:

* "Benevolent dictator for life  
  The original creator or lead developer of a cryptocurrency has the final say on all decisions. The simplest governance strategy is nicknamed benevolent dictator for life. In this strategy, the creator of the blockchain is the final authority on all decisions regarding the blockchain (...).
* Core development team  
  A team of the most active developers decides what functionality should or shouldn’t be included. The next step up places control of the blockchain roadmap in the hands of a core development team. This is a strategy commonly used in open source programming projects, where users are able to offer or request features, but developers have the final say on what is or is not included in the official release.
* Open governance  
  The team making governance decisions for the blockchain is chosen by the users of the blockchain. Some blockchains use the open governance method of handling governance of the blockchain. In this system, the team that makes the final technical decisions for a system is selected by the system’s users.
* On-chain governance  
  The rules for how the blockchain operates are stored on-chain in smart contracts with built-in capability and procedures for modifications. A blockchain-specific governance strategy is on-chain governance. In this form of blockchain governance, the rules describing how the blockchain should operate are stored on the blockchain itself. These regulations typically are implemented as smart contracts on the blockchain with built-in methods for users to modify the rules based upon their needs and the needs of the blockchain".

## Consortium Governance

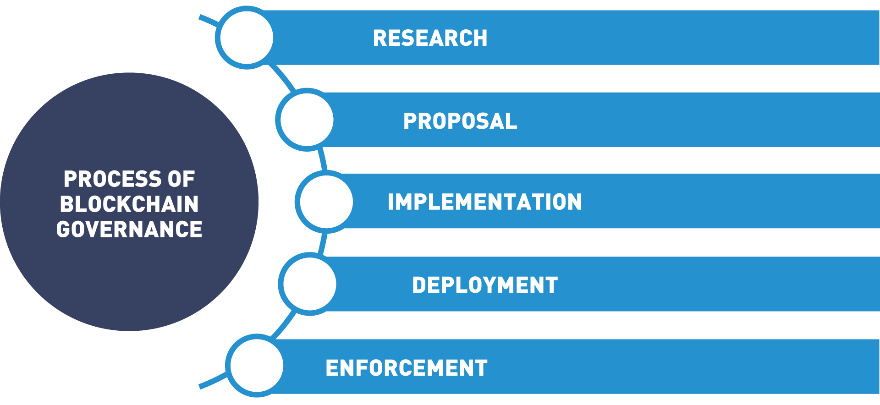
Due to blockchains built in trust and collaboration mechanisms, new pathways are opening up for enterprises to work together. A new form of collaboration fostered by blockchain is consortiums. Consortium, as defined by [Webster's dictionary](https://www.merriam-webster.com/dictionary/consortium), is

"an agreement, combination, or group (as of companies) formed to undertake an enterprise beyond the resources of any one member".

Most enterprise blockchain solutions will be implemented by a "consortium" of enterprises, building one or more applications on top of a "blockchain platform". These consortiums are already forming in many industries to deal with the particular problems of those industries. Alliances in Trade Finance, Carbon Emissions Accounting, Social Impact and Healthcare have working blockchain consortiums solutions.

## Who Really Governs the Blockchain?

Blockchain governance comes down to the users. For a blockchain community to thrive it needs a robust community. Changes to the operation of the blockchain must be accepted by the majority of its users or they will create a new blockchain that does. The process by which changes are made follow these five steps discussed by Pierre Rochard in his article [*"Bitcoin Governance"*](https://nakamotoinstitute.org/mempool/bitcoin-governance/):



The changes to a blockchain starts with research. Before the problem or situation can be addressed it must be understood. A proposal consists of a problem definition and a proposed solution. Implementation requires a little bit more work as the nodes and user must agree to the change or it can not be enforced.

As explained in the [*"Blockchain Governance In A Nutshell"*](https://medium.com/coinmonks/blockchain-governance-in-a-nutshell-67903c0d2ea8) article by Demiro Massessi:

"Major changes to a blockchain require a hard fork. A hard fork is a change to the blockchain protocol that makes it incompatible with old clients.

For a hard fork to be successful, users need to agree to follow it. Users can refuse to follow a hard fork, creating a divergent blockchain. The DAO Hard Fork on Ethereum created Ethereum Classic.

Despite the official story of who governs the blockchain, in the end, the users are the ones who really make the final decisions of what will or will not be included in the blockchain. With the huge number of potential options, users can abandon a blockchain that makes changes that they disagree with.

Any major change to a blockchain requires a "hard fork". All this means is that the blockchain protocol has changes that are not backward compatible, so blockchain clients that do not make the switch will not be able to operate on the main blockchain. A soft fork is a change that invalidates previous valid blocks by accepting new blocks, soft forks are backwards compatible. For a hard fork to be successful, users of the blockchain need to make the decision to update their software protocols to incorporate the new changes.

If not all users decide to make the switch after a hard fork, a divergent blockchain can be created. Since the blockchain is a distributed network, the decision to implement a hard fork doesn’t cause the old version of the blockchain to become non-functional. Users who choose not to follow the fork can decide to maintain the old blockchain, fragmenting the blockchain network".

## Bitcoin Network and Governance

As we mentioned in previous sections, Bitcoin uses a Proof of Work model to encourage miners to add blocks to the network. This governs the operations of the blockchain. But what happens when changes need to be made? How do they get implemented? The Bitcoin community consists of three main players: developers, miners, and users. None of these participants have the ability to make emergency decisions when unexpected situations occur. Bitcoin uses an off-chain governance model where decisions are balanced by the developers, miners and users. In blockchain, developers must write the code to change the blockchain. Without the consent of the miners and users, the developers have no way of enforcing the change. Miners and users must choose to adopt the new software changes.

## Bitcoin Improvement Protocols (BIP)

When a change to the Bitcoin protocol is needed, developers will share the proposed change with other protocol developers. This improvement sharing could be in the form of an email to the bitcoin-dev mailing list, a formal white paper, and/or a Bitcoin Improvement Proposal (BIP). Code is written and tested that will enact the change. If developers in the community approve the proposals and resulting code, the proposal is put to a vote on chain and the miners decide if the proposal is implemented. This occurs through a hard or soft fork.

This system is not without faults, as can be seen with the SegWit improvement protocol which alters block size. The vision surrounding blockchains deals with decentralization. By implementing the SegWit changes, a change in how the Bitcoin blockchain protocol operates, a central authority was responsible for enacting the change. To many in the community this decision went against the fundamental tenets of blockchains decentralized philosophy.

As a result, the Bitcoin community was torn and the Bitcoin Network split into two different chains Bitcoin (BTC) and Bitcoin Classic (BCH). [The Bitcoin Foundation](https://bitcoinfoundation.org/) is set up to educate and promote the Bitcoin Blockchain.

## Governance in Ethereum

Vitalik Buterin first described the concept of Ethereum through a [Whitepaper](https://ethereum.org/en/whitepaper/) introduced at the Bitcoin Convention in Miami 2014. It was based on the code for Bitcoin, but included a logic engine that could execute smart contracts. By connecting computers using the Ethereum blockchain, computing power is aggregated creating the Ethereum Virtual Machine. Ethereum is not only a functioning blockchain with smart contract capabilities, but a platform for new blockchains to be built upon. The EVM computing does not come free, a GAS price is charged for the GAS needed to perform the transaction’s computations. This GAS fee can change dramatically depending on network conditions as the current price of Ether is part of the calculation.

## Ethereum Improvement Proposals EIP’s

Like Bitcoin, Ethereum's three main players (developer, miners and users) must update code to improve on functionality. [Ethereum Improvement Proposals (EIPs)](https://ethereum.org/en/eips/) are standards specifying potential new features or processes for Ethereum. EIPs contain technical specifications for the proposed changes and act as the “source of truth” for the community. A note worth EIP was the code for issuing a token. The [Ethereum Request for Comment, ERC-20](https://ethereum.org/en/developers/docs/standards/tokens/erc-20/) introduced the standards for issuing utility tokens on blockchain based on Ethereum protocols. The [Beacon Chain](https://ethereum.org/en/eth2/beacon-chain/) introduced the Proof of Stake consensus model and the concept of sharding. Sharding is the concept of running parallel side chains to alleviate congestion of the network. The [Berlin Hard](https://www.coindesk.com/berlin-hard-fork-is-now-live-on-ethereum) fork and the [London Fork](https://eips.ethereum.org/EIPS/eip-1559) are improvements to stabilize fees paid to the miners so these fees do not fluctuate with the price of Ether.

Ultimately, Ethereum uses the benevolent dictator for life mode of blockchain governance. While user input and input from the development team is welcome for Ethereum, Vitalik Buterin is the final authority on decisions regarding the Ethereum roadmap.

## DAO Hard Fork on Ethereum

One famous example of this type of fragmentation is the DAO hack on the Ethereum network. The DAO was an Ethereum smart contract that completed a record-breaking crowdfunding campaign on the Ethereum network, with all of this value stored within the DAO smart contract. A flaw in the smart contract’s code allowed an attacker to create another version of the smart contract under their control and siphon off a portion of the DAO contract’s funds, worth roughly 72 million dollars at the time. After much debate, the Ethereum network decided to implement a hard fork that allowed investors of the DAO to reclaim their stolen Ether.

This was a very contentious decision, because the historical ledger in the blockchain is supposed to be immutable and all transactions are final. Smart contracts are supposed to be their own final authority, so any action that could be performed with a smart contract, including exploiting a programming flaw to drain value from it, is considered fair game. The Ethereum network’s decision to reverse the DAO hack went against the principles of blockchain’s immutability and the supposed self-regulation of smart contracts.

Some of the Ethereum network refused to follow the DAO hard fork, resulting in a divergent blockchain where the DAO hack was successful. This created the Ethereum Classic cryptocurrency, which shares the same history as Ethereum up to the DAO hack, but is completely independent after that point.

## Governance in Hyperledger Frameworks

[Hyperledger](https://www.hyperledger.org/) was introduced as an open source blockchain project sanctioned by the Linux Foundation. Spearheaded by [Brian Behlendorf](https://en.wikipedia.org/wiki/Brian_Behlendorf), its mission is to provide the community with the tools and education to foster distributed ledger technology on an enterprise level. Hyperledger frameworks use an Open Governance model to make technical decisions regarding the Hyperledger environment. The Hyperledger [Technical Steering Committee (TSC)](https://www.hyperledger.org/about/leadership) is the final authority for technical decisions in Hyperledger. Each year, the Hyperledger Technical Steering Committee is selected from the Hyperledger environment’s active contributors and maintainers. Contributors and maintainers can submit themselves as potential candidates for the fifteen slots, and the slots are filled based on voting by the same group of contributors and maintainers. This model is designed to allow those with an active role in the Hyperledger development community to have a say in how that community is governed.

## Governance in Corda

[Corda](https://www.corda.net/) is an open source blockchain project designed for business. Developed by R3, an enterprise blockchain software firm, in collaboration with over 200 technology and industry partners. The Corda platform was launched in September of 2017. Corda also uses an Open Governance model to make technical decisions regarding the future of the blockchain. The Corda Network Governing Body is selected to represent the interests of all users in the Corda network.

## Working Groups and Special Interest Groups

Working Groups and Special Interest Groups are consortium-based discussion sessions to complete a task or develop a whitepaper, prototype, platform or project. These collaborations are aimed at developing open source standards and projects to accelerate the acceptance of blockchain.

[Enterprise Ethereum Alliance Working Groups](https://entethalliance.org/participate/working_groups/)

There are two types of the EEA working groups:

Technical which tackles developing standard and resolving specific problems.

Core Specific Working Groups which ensures quality interoperable implementations.

Some examples of the EEA’s working Groups include: Client Interoperability Testing, Core Specifications and Cross-Chain Interoperability.

[Interest Groups (IGs)](https://entethalliance.org/participate/interest_groups/)

IG’s are designed to foster information exchange across vertical, industry-centric groups where EEA members in specific industry segments can exchange information.

Some examples of the EEAs Interest Groups are: A.I. and Blockchain, Ethereum Mainnet, Supply Chain, Financial Services and Tokenization.

[Hyperledger Wiki](https://wiki.hyperledger.org/)

It is a Linux sponsor environment for projects, Working Groups and Special Interest Groups to exchange ideas and develop projects.

Working Groups in Hyperledger are developed for specific purposes. For example, the [Learning Materials Working Group](https://wiki.hyperledger.org/display/LMDWG) focus is on supplying templates, assisting the project in developing documentation and collecting and categorizing resources created by the vast Hyperledger community. The LMDWG wiki home page also provides a list of weekly events in and out of the Hyperledger community. Each working group has a wiki home page and a [“Join This Group”](https://lists.hyperledger.org/g/learning-materials-development-wg) button.

Some example the Hyperledger’s Working Groups: [Identity](https://wiki.hyperledger.org/display/IWG), [Diversity and Inclusion](https://wiki.hyperledger.org/display/DCI/), [Performance and Scale](https://wiki.hyperledger.org/display/PSWG), and [Technical Working Group China](https://wiki.hyperledger.org/display/TWGC).

Special Interest Groups at Hyperledger are designed to tackle cross industry issues by supplying an open environment for information exchange. The [Climate Action and Accounting SIG](https://wiki.hyperledger.org/display/CASIG/) is developing a carbon calculator spearheaded by Si Chen for global consideration. The ["Resources](https://wiki.hyperledger.org/display/CASIG/Resources)" section on the wiki page has current information about the global emergency. Please consider [joining this conversation as it affects all humans](https://lists.hyperledger.org/g/climate-sig).

Some examples of other Special Interest Groups: [Capital Markets](https://wiki.hyperledger.org/display/CMSIG/), [Healthcare](https://wiki.hyperledger.org/display/HCSIG), [Public Sector](https://wiki.hyperledger.org/display/PSSIG), [Social Impact](https://wiki.hyperledger.org/display/SISIG), [Supply Chain](https://wiki.hyperledger.org/display/SCSIG), [Media and Entertainment](https://wiki.hyperledger.org/display/MESIG/Media+and+Entertainment+SIG), [Telecom](https://wiki.hyperledger.org/display/TCSIG), and [Trade Finance](https://wiki.hyperledger.org/display/TFSIG).

[Government Blockchain Association (GBA)](https://www.gbaglobal.org/)

The GBA promotes blockchain technology by empowering individuals and organizations to connect, communicate, and collaborate to solve public sector challenges around the world.

The GBA hosts international events like the [Government Blockchain Week](https://www.gbaglobal.org/events/category/type/gba-conference/event-at-the-u-s-capitol/money-governance-the-law/list) at the US Capital where they recognize new blockchain emerging projects with an [award ceremony](https://www.gbaglobal.org/gba-annual-achievement-awards-2021/). Spearheaded by a tireless Gerard Dache, the GBA cultivates professional work flows between technologists, public policy makers, application specialists, and those who want to learn about the new and emerging digital currencies. Furthermore, GBA acts as a catalyst in creating a public dialogue around the creative, profitable, and positive leveraging of blockchain technology.

You can find examples of the GBA Working Groups [here](https://www.gbaglobal.org/working-groups/).

As previously mentioned, blockchain is about community. Become part of a growing community by joining a special interest group or working group and become part of the conversation.

## Governance With Autonomy - Driverless Cars

Let's discuss governance with autonomy.

Let's jump 20 to 25 years into the future and see where we've gotten with AI and autonomous drive.

Driverless cars have now evolved to the point where a company can own a fleet of autonomous vehicles all driving in a variety of directions, moving items as well as people.

But it's more than just that. Each car is pre-programmed with a set of guiding principles.

For example, don't hurt humans, reach X percentage of profits within the month, maintain a set percentage of holistic health, etc.

Consider the following scenario: A vehicle arrives to pick up a passenger for transport within a set time frame to take them to their scheduled meeting.

The passenger is running late and therefore decides to take advantage of the option to pay an extra fee for an expedited route.

Conceivable solutions to provide this options could include designating a lane on the highway for users paying the premium or sending micropayments to other vehicles in exchange for adjusting their travels to create a clear path for the expedited vehicle.

Once the passenger has been delivered to the appropriate destination, the vehicle recognizes the need for maintenance after running an internal diagnostic.

After repairs are completed, the vehicle heads off to a charging station and then moves on to the next customer.

This can eventually be applied to blockchain governance.

More specifically, decentralized autonomous organizations.

This is a concept that quickly manifested itself after the Bitcoin white paper spread and people began to run through thought exercises.

## Decentralized Autonomous Organization (DAO)

An organization whose operating rules are encoded into a computer program controlled by its members. It is composed of a complex stack of smart contracts that form a decentralized application (Dapp).

In simple terms, a DAO is an organization that runs on a stack of computer programs (called smart contracts in the blockchain world) that are all interconnected to maintain a set of pre-programmed rules that have been previously voted upon by a community. When thinking about regular corporations stripped all the way down to their bare bones, they are basically different groups following rules, responsibilities, and duties given from those sitting at the top of the organization. The bigger they are, the more complex these pieces become. At the moment, a DAO's goal is to automate this complex system piece by piece.

Within each DAO, there is a kind of pooling process for humans to contribute new rules into the system. These rules are then presented to the community and voted upon, based on the DAOs previously created rules. These new rule commitments will need majority agreement (may be different for each DAO) from the community to make this rule real. If this new computer-coded rule is accepted by the community, then it will be placed into the stack of other computer coded rules to improve the overall autonomous organization.

## Decentralized Autonomous Organization (DAO)

As our technology advances, the world around us becomes more and more automated.

Take securities trading, for example.

In the 1950s, experts began designing the algorithm and rules that an automated trading system should follow.

In the 1980s, technology began catching up and those algorithms could finally start to be implemented.

Systems improved in the 1990s.

And in 2008, the world's first fully automated trading system, Betterment, went live.

Just six short years later, more than 75% of shares traded on US exchanges were made by fully automated systems.

As we continue to use technology to automate more and more of our business processes, the concept of a DAO, or a Decentralized Autonomous Organization, has emerged.

The basic idea behind a DAO is simple.

Most business processes are governed by a set of well-defined rules and procedures.

These rules and procedures can be codified as smart contracts on a decentralized network, thus, automating business process.

This decentralized nature of Web 3.0 technologies like blockchain makes it much more fault-tolerant, as well as providing a built-in layer of redundancy, backup and error correction.

Consider the following example set sometime in the near future, when fully autonomous vehicles and consumer grade artificial narrow intelligence are common.

An entrepreneur notices a lack of ride-sharing services available in her town and decides to enter the market.

She saves enough capital to purchase a fully automated vehicle, as well as an AI Deep Learning system to analyze traffic and demand patterns and design optimal routes for the vehicle to cover.

Now, over time, this single vehicle earns enough to fund the purchase of a second automated vehicle.

The business is able to manage its own operations, forecasting and modeling, and grow with little to no human intervention.

This is the conceptually ideal model of a DAO.

## Governance for Enterprise

We’re focusing on governance in the consortium space, not governance within an enterprise company. So what is a "consortium"? A consortium is just a grouping of institutions (possibly individuals) getting together to achieve a mutual goal.

This goal can be setting some standards for their industry (Department of Justice), selling products (Airbus), sharing resources (Universities), etc. In a consortium, the only real obligation you have to others who are taking part would be providing resources for specific tasks and sticking to the rules laid out prior to you joining. Within blockchain, there are many different industries creating their own consortiums, such as financial services, life science and health care, energy, media and telcos, and the public sector.

Governance becomes much easier when it’s in a controlled environment, with each member agreeing upon set rules prior to jumping in with everyone else. Governance structures vary by industry and profit vs. non-profit, so there will be no set governance model everyone uses, but there are two we’ve come across in the blockchain space:

* One is including the formation of smaller subgroups to work on specific issues.
* The second is providing several levels of potential engagement, ranging from participation in monthly calls to active technology development.

The point we would like to get across here is that a consortium governance model is currently more efficient than most decentralized blockchains.

## Governance for Enterprise: Consortiums

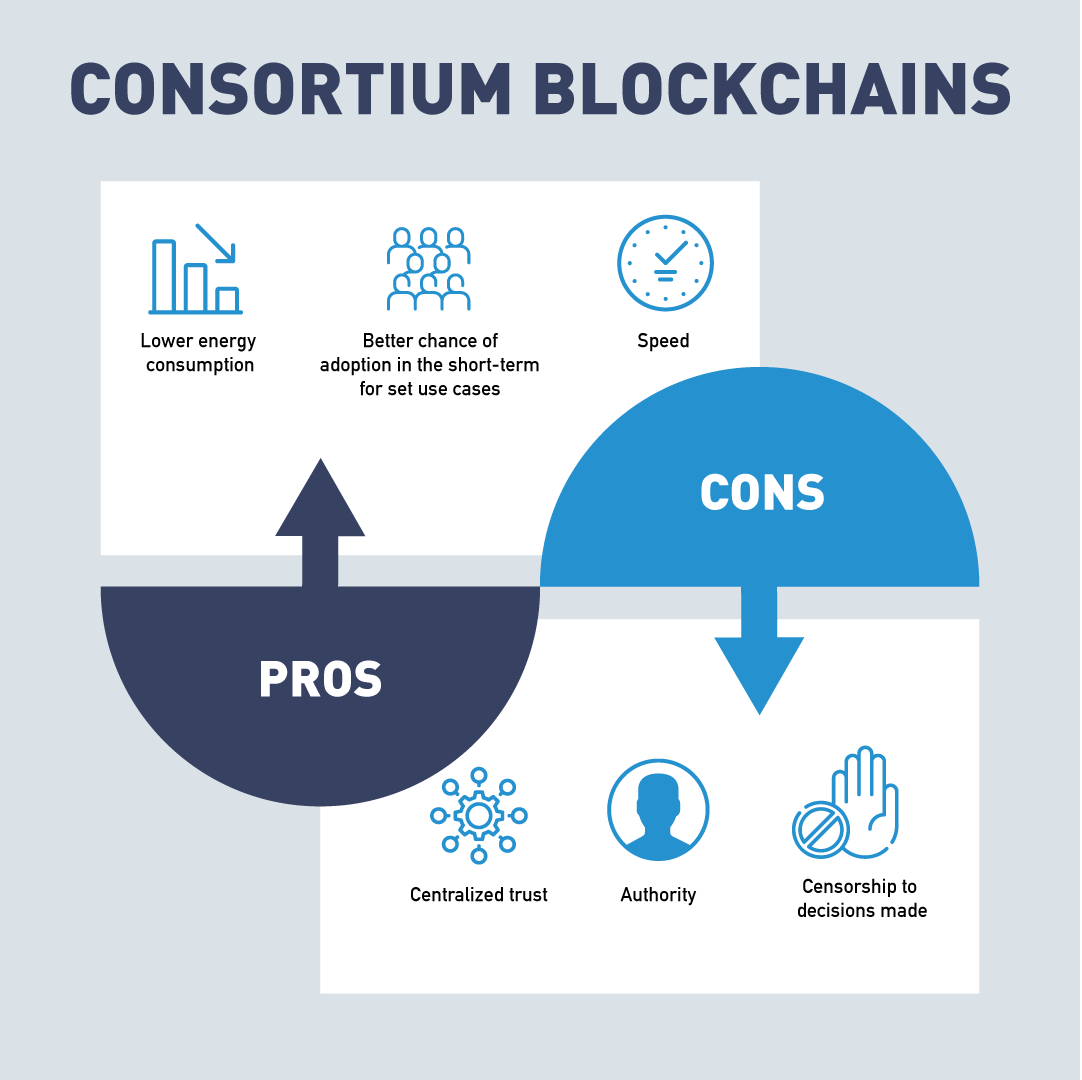
Almost all consortiums up to this point have been permissioned and not decentralized permissionless blockchains, which is an opportunity cost most companies make when joining. At a high level, a permissioned blockchain is just that, a chain in which others must have permission to operate on. So, all the nodes operating on a permissioned chain have been verified by the central institution that is the authority of the network and the transactions that are confirmed don’t necessarily have to go through all the nodes.

These consortium blockchains have historically taken two approaches:

* Business-focused consortia  
  They aim to build and operate blockchain-based business platforms to solve a specific business problem (e.g. Digital Trade Chain – focused on cross-border payments).
* Technology-focused consortia  
  They seek to develop reusable blockchain platforms based on technical standards (e.g. Hyperledger).

## Consortiums: Pros and Cons

Let's see what are some pros and cons of consortiums:



## 4.4 Identity on the Blockchain

In this section, we're going to discuss identity on the blockchain.

Let's start by understanding why we even need to have an identity on the blockchain.

Centralized systems can be coerced by other forms of authority to shut down their network.

Let's take Napster for example.

Napster had a decentralized network architecture, but they maintained the centralized authority.

Therefore, the central authority could be attacked and, by taking out the central authority, could effectively control Napster.

This is because Napster relied on that mix of centralized control over a decentralized network.

This impacted identity because you need an identity to control.

Torrents on the other hand, they do not operate in the same fashion.

Torrents provide a decentralized network with decentralized authority.

This allows the nodes to manage identity differently.

It's also the reason why torrents are still being used today, in spite of the entertainment industry's best efforts to stop it.

Torrents remove the central authority.

So, this begs the question "Why didn't point-to-point networks like torrents attain the same level of acclaim as blockchain?"

Because there's no guarantee that the nodes would do the right thing.

Nobody could guarantee that the nodes would cooperate with each other.

This leads to an extremely important question.

How do you incentivize the nodes on the network to follow the rules?

In a torrent system, anyone can download and share a file, but there's not a real incentive to be a good actor on the network.

What happens when people do something dishonorable on a torrent for instance, and stop seeding the files that ate up bandwidth or occupied space on their computers?

Instead of music going to the network or other files, what if it were money going through a point-to-point network, through a bank network, let's say?

Your transactions would never be processed reliably.

You couldn't trust that the processing was not messed up, either deliberately or accidentally.

Further, because of anonymity and the way that identity works in the blockchain, you wouldn't have a way to punish or reward the actors.

Blockchain solved this problem.

It perfectly incentivized how to create a decentralized self-contained network using crypto economics.

This differed from earlier point-to-point networks because it offered economic incentives to the nodes that followed the rules.

Nodes are given money for following the rules.

This money is in the form of cryptocurrency.

The nodes were punished for tampering with the system or with past transactions, or submitting a bad transaction.

This is why all public blockchains can operate without an authority.

It is also the reason why cryptocurrency is mandatory for a public blockchain, and not needed for a private blockchain.

Because you need a way to incentivize the actors on the network.

Consider how these rewards and these punishments work and how a system without a central authority can determine what is valid and what is invalid.

On the blockchain, identity is important.

You have to be able to prove that your assets actually belong to you.

Different blockchains they use different systems for tracking identity and identity information, but most are based on the principles of public key cryptography.

Before we get into the details of how identity works on the blockchain, we need to discuss the basics of public key cryptography.

The security of a public key cryptography it's based on let's call them hard math problems.

So, by that, I mean a hard math problem is one where it's easy for someone to calculate it, but it's hard for someone to reverse that calculation.

Take multiplication, for example.

All things considered, multiplication is easy.

If you have a little bit of time, something to write with, you can pretty much multiply any two numbers and get the right answer.

A computer can do can do that even more quickly.

Factoring on the other hand, it's hard.

The best way to factor a large number is to try every possible factor until you find the right one.

Well, this approach works well if the number to be factored is small.

It quickly becomes virtually impossible with a sufficiently large factor.

Some public key cryptography algorithms are designed so that breaking the algorithm requires factoring very large, usually prime numbers.

Another hard math problem used in public key cryptography is based on exponents and logarithms.

Exponents are easy, since it's essentially multiplication, and logarithms are hard, since you're essentially factoring.

Most public key algorithms that use exponents use a type called modular exponents.

All this means is that when they're done calculating the exponent, they divide the result by a publicly-known value called the modulus, and they keep only the remainder.

RSA is a commonly known public key cryptography algorithm.

It's based on exponents and logarithms.

RSA uses the power law of exponents.

What this means is that, if you take a number, you raise that number to a power, and then raise the result to another power, that you'll get the same result as if you simply multiply the two exponents together and then raise the base to the result.

An RSA user chooses two exponents so that any number raised to the product of the two exponents in a given modulus produces the original number.

One of these is called the public key and that public key is distributed freely, while the other is the private key, which is intended to be kept secret.

If someone wants to send a private message to the user, they convert it to an integer using a publicly-known method.

They raise it to the power of the user's public exponent and they send the result to the user.

The user raises the received value to their private exponent producing the original message.

RSA is secure because an attacker must be able to calculate a logarithm to determine the secret message.

Since this takes guessing every possible value until the correct one is found,

RSA is designed to make the number of potential values so large that finding the right one is pretty close to impossible.

Another public key algorithm uses different math behind the scenes, but the basics are effectively the same.

A user creates a public key and the private key that can be used together for either encryption or signing, which we'll talk about later.

The algorithms are designed so that an authorized user only has to do the, quote, "easy calculations", while an attacker has to perform the hard calculations, and the algorithm is designed to make attacking so that the hard algorithms are close to impossible.

Public key cryptography is how identity is handled on the blockchain.

A user's address on the blockchain it's their public key.

This has several useful properties.

Users do not need to reveal their identity on the blockchain, but they can positively identify themselves, since determining their private keys requires solving a quote, "hard problem".

Anyone can send a user an encrypted message, since they have easy access to their public key.

Users can verify the validity of their transactions using digital signatures.

You can think of a digital signature as the opposite of an encrypted message.

In RSA, anyone can send an encrypted message to a user by converting it to a number, raising it to their public exponent, and sending the result to them.

The user's public and private keys are designed so that the users can retrieve the original message by raising the received message to their private exponent.

RSA digital signatures involve the opposite process.

A user writes a message and raises a condensed form of the message to the power of their private exponent to create a signature, then they publish that signature.

Their public key and their message are both published together.

Anyone can verify the signature using a simple three-step process, condense the attached message using the same method as the message writer, the message originator, raising that attached signature to the user's public key, then verifying that the results of the previous two steps are identical.

Digital signatures work for the same reason that encryption works in RSA.

An attacker needs to know the user's private key to perform either operation, and the algorithm is designed to make that process difficult or very close to impossible.

This means that identity on the blockchain boils down to the possession of a user's private key.

So, it is absolutely important that that private key be kept safe.

In Ethereum, a user's identity is managed using a public key or address, and the user can use the corresponding private key to sign transactions and read encrypted messages that are sent to them.

In Hyperledger (Fabric) and Corda, identity is encoded in x.509 certificates, which include the user's public key.

In Corda, specifically, certificates can either be public, which means that they are published to the blockchain, or confidential, meaning that they are only shared with the parties that the owner performs transactions with.

## Identity

Self-sovereign identity and blockchain solutions introduce identity management in a way that can improve a system considered broken. This topic will be examined in the next chapter. In this section, we will cover identity as seen through transactions and how and if you want your identity tied to a transaction.

## Anonymity in the Blockchain

In this section, we'll discuss anonymity on the blockchain.

Privacy and anonymity on the blockchain are a crucial part of its success in some applications.

If individuals or organizations are performing transactions on the blockchain, they may not wish this to be public knowledge.

Different blockchains have different levels of anonymity and privacy built into the protocol.

As discussed earlier, public key cryptography is at the center of maintaining identity on the blockchain.

It uses a pair of public and private keys to make encryption and digital signatures possible.

At this point, we need to take a look a bit more into the relationship between a user's keys and a user's actual identity.

The first thing to consider is that there is nothing about a public key that ties it to its corresponding private key.

We've said that a digital signature verifies that an owner of the corresponding private key created the signature, but that is all that it says.

Since private keys are secret, obviously it can't be possible for someone to determine a private key from a public key, at least it shouldn't.

If you know a user's private key, you can calculate the public one, but the reverse is not true.

The other thing to keep in mind is that private keys are just numbers, and can't be tied to a person's actual identity, their real-world identity.

Identity on the blockchain is just possession of the relevant private key, and even if someone guesses or steals that private key, they can't learn its owner's actual identity from it directly.

The original blockchains did not have much in the way of privacy and anonymity protection.

You can't tie public keys to private keys or private keys to real-world identities, which means that blockchain users have a limited amount of built-in privacy.

However, every transaction on the blockchain is public and stored there forever.

This means that a lot of information about the users' identity could be learned through sifting through the data stored on the blockchain to obtain the metadata.

Based on the repeated transactions to places like a coffee shop or a market, someone could get an idea of where an individual lives and their habits.

For businesses, repeated transactions may indicate business relationships that may lead to a loss of a competitive advantage if leaked.

On basic blockchains, anonymity only goes so far.

The limited level of anonymity and privacy protections available on the original blockchain has inspired development of enhancements that increase privacy, while still allowing transactions to be verified and validated publicly on the blockchain.

This is an incomplete list of some of the mechanisms developed and implemented in various blockchains.

We'll start with zero knowledge proofs.

They use cryptography and cryptographic algorithms to allow a user to prove knowledge of a secret without revealing the actual secret.

A common example of this type of proof includes a colorblind person and two objects identical except for the color.

The colorblind person shows one object to the prover, conceals both objects, and then shows one to the prover again.

The prover then says whether or not they are the same object.

Since the only way of determining this reliably is that the objects are different colors, the prover can prove the difference in colors without revealing the color of either object.

Another approach is stealth addresses.

Stealth addresses involve using one-time addresses to perform transactions on the blockchain.

A stealth address is just a one-time address that makes it impossible to link a transaction to a known account.

What this does is prevents the data mining attacks on privacy that we discussed earlier.

We mentioned previously that transactions are digitally signed .

With ring signatures, all that can be determined from a transaction is that a member of a group signed it, but not the particular member.

The ability to see who is performing transactions with whom is dangerous to user privacy and anonymity.

Protocols like CoinJoin mix several transactions together, so that it is difficult to pair senders with recipients.

Confidential transactions take advantage of homomorphic encryption, which makes it possible to perform mathematical operations on encrypted data.

This means that the data contained in a transaction can be hidden from the public, while still allowing the network to verify that the transaction is valid.

Now, let's discuss how different blockchains implement the various privacy and anonymity mechanisms available.

We start with the Ethereum.

Ethereum does not currently implement many real advanced options for privacy or and/or anonymity.

In the current version, user anonymity is limited to the fact that no one can tie a public key to a real-world identity.

This is intended to change in the future though, and the Ethereum roadmap currently includes laying the groundwork for implementing zero knowledge proof.

Hyperledger (Fabric) provides several options for privacy and anonymity.

At the lowest levels, users can achieve increased anonymity through channels which can further encrypt the data that's stored on the channel using keys only available to members of the channel.

At the next level, Hyperledger Fabric also allows users to perform private transactions.

In a private transaction, data is stored on the cloud, but the hash of the data is stored on the blockchain.

This allows users to use the blockchain to ensure data authenticity without storing the actual data publicly on the blockchain.

Finally, Hyperledger supports zero knowledge proof, where a prover can demonstrate possession of some data without revealing the data itself.

These different levels of privacy and anonymity protection gives users a higher degree of configurability on the Hyperledger Fabric blockchain.

Finally, Corda allows users to perform transactions either as a party or an anonymous party on their blockchain.

An anonymous party has the same level of anonymity protection as a basic blockchain, relying on the fact that public keys cannot be tied directly to real-world identities.

A party on the Corda blockchain reveals the real-world identity of the user which intentionally sacrifices anonymity for identity validation.

## Advanced Blockchain Anonymity Techniques

The following are only some of the mechanisms developed and implemented in various blockchains:

* Zero-knowledge proofs  
  Zero-knowledge proofs use cryptographic algorithms to allow a user to prove knowledge of a secret without revealing the secret. A prover proves knowledge of a secret without revealing it. New technology referred to as SNARK (Succinct Non-interactive - ARgument of Knowledge) are fine tuning privacy issues on blockchains.
* Stealth addresses  
  Stealth addresses involve using one-time addresses to perform transactions on a blockchain. A stealth address is just a one-time address that makes it impossible to link a transaction to a known account. This prevents the data mining attacks on privacy that we discussed earlier.
* Ring signatures  
  We mentioned previously that transactions are digitally signed. With ring signatures, all that can be determined from a transaction is that a member of a group signed it, but not the particular member.
* CoinJoin  
  The ability to see who is performing transactions with whom is dangerous to user privacy and anonymity. Protocols like CoinJoin mix several transactions together so that it is difficult to pair senders with recipients.
* Confidential transactions  
  Confidential transactions take advantage of homomorphic encryption, which makes it possible to perform mathematical operations on encrypted data. This means that the data contained in a transaction can be hidden from the public, while still allowing the network to verify that the transaction is valid.

## Specific Anonymity Implementations

* Ethereum  
  Ethereum is working on improving the zero-knowledge proofs, mixing and DAPPS (applications developed to improve anonymity) to strengthen privacy. Also ConsenSys, the Enterprise Solutions builder for Ethereum introduced QUORUM, a fork of the Ethereum blockchain which enables users to benefit from the public Ethereum blockchain while enjoying features from a private network. Developed by JPMorgan, it is a permissioned implementation.
* Hyperledger  
  - Channels: Subsections of the blockchain that make transactions visible only to members.  
  - Private transactions: Hashes of private data are stored to publicly verify it on the blockchain.  
  - Zero-knowledge technology: One can demonstrate knowledge of a secret without revealing the secret itself.
* Hyperledger Besu  
  Besu is an Ethereum client that runs on the Ethereum public network, private networks, and test networks such as Rinkeby, Ropsten, and Görli. Hyperledger Besu includes several consensus algorithms including PoW, PoA, and IBFT, and has comprehensive permissioning schemes designed specifically for uses in a consortium environment.
* Corda  
  Parties on the Corda Network can be represented in one of two ways:  
  - Party: A public key and name.  
  - Anonymous party: Only a public key.

## Trust in Blockchains

Just as there are benefits with blockchain technology, there are also some challenges. Blockchain is a culmination of technologies that have been blended to provide a trustless platform. Expect some challenges and use case justifications taking the old line of business apps to the blockchain.

Let's recap the features of a blockchain that establishes trust:

* Blockchain technology is about storing some kind of data (which are transactions in regards to the Bitcoin blockchain).
* Blockchain is essentially transferring trust from an intermediary to technology.
* Storing data in the blockchain is through cryptographic functions.
* Private key/public key.
* Collaboration through consensus.

## Establishing Trust in Blockchains

All transaction data on a chained block is assumed to be trustworthy.

The users base this trust on the fact that:

* This data has not been tampered with.
* The blockchain is immutable.

## What Do Blockchains Really Do?

Blockchains minimize the amount of trust required from any single actor in the system. They do this by distributing trust among different actors in the blockchain as defined by the consensus protocols.

Blockchains have a shared ledger that gives us the absolute truth of the state of the system. It uses mathematics, economics, and game theory to incentivize all parties in the system to reach a “consensus” (i.e. coming to an agreement on a single state of the ledger).

* Consensus algorithms  
  The blockchain is based on a consensus algorithm where all nodes agree that the transaction is valid.
* Financial transparency  
  Financial transparency can reduce the need for intermediaries.
* Smart contracts  
  Smart contracts reduce the need for accountants, lawyers, bankers, etc., as computer code can replace some basic functions. Trust shifts to technology.
* Trust in technology  
  Trustless blockchains is a transfer of trust to technology from organizations, governments and corporations.
* Confidential transactions  
  Privacy techniques mask details of transactions while still proving they occurred.
* Decentralized ledger  
  The ledger acts as a trust broker when two parties who don’t trust each other want to interact.
* Transparent code  
  Most blockchains are built on open-source software that is transparent, community-driven code that is open for comment.

## 4.5 Summary

In this chapter, we discussed:

* Open source communities and blockchain source code.
* Governance models for blockchain and who is really in charge.
* How a blockchain is “trustless”.
* Why a trustless system is more secure than a system that requires trust.
* Why anonymity is required in public blockchains.
* How private/public key cryptography provides anonymity.

# 5 Blockchain Problem Solving and Future Trends

Now that we understand the basics of how blockchain works, Chapter 5 will discuss the problems blockchain can solve. We will discuss the concept of immutability and how the append only blockchain brings new trust in shared information. Next, we will take what we learned about smart contracts to see how they are bringing autonomy to systems that previously required human interaction. We will discuss the double-spend issue and how blockchain can solve for it. We will also discuss some popular cryptocurrencies.

Next, we will discuss the new business trends blockchain makes possible. First, we will discuss the way we manage our identity and information on the Internet and how decentralized identity solutions rooted on a blockchain are fixing what is broken. Next, we will discuss how blockchain is revolutionizing the financial markets by autonomous market solutions that remove middlemen and open markets up to previously excluded clients. We will also join in the conversation around Central Bank Digital currencies and how enacting blockchain solutions can streamline the government's monetary policies.

Finally, we will discuss the energized world of NFT’s (non-fungible tokens) and how owning unique rights to everything from music, sports collectables and even “captured moments” is turning the collectable world upside down. We end the chapter with a brief discussion on interoperability. In order for this new technology to take hold, blockchains need to be able to communicate and transfer value amongst themselves.

## 5.1 Learning Objectives

By the end of this chapter, you should be able to:

* Discuss immutability in blockchains.
* Explain what transparency is and review advantages and disadvantages of append-only ledgers.
* Explain how blockchain is looking to be autonomous through smart contracts.
* Discuss how blockchain removes third party intermediaries.
* Discuss how blockchain solves the problem of double spending.
* Distinguish between traditional database vs. blockchain immutability.
* Discuss central bank digital currencies and how they operate.
* Explain identity management on a blockchain.
* Discuss decentralized finance and the implications for the financial industry.
* Examine Central Bank Digital Currencies (CBDC).
* Discuss non-fungible tokens and how they will impact society.
* Examine the importance of interoperability for blockchains.

## Immutability Defined

Immutability is when something is unable to be changed.



## Immutability

"Immutable" simply refers to the permanence of data.

Anything we call "immutable" we understand to be permanent and unchanging.

Your local weather forecast - that's mutable, it changes all the time; the stars in the sky, those are immutable, they seem permanent from our perspective.

One of the benefits of blockchain and many other Web 3.0 technologies is the promise of immutability.

The data recorded on a blockchain system can never be altered, edited, changed, or deleted once it has been recorded.

As this data is stored in many different locations, changing or removing a copy of the data in one single place, or in a limited number of places poses no threat.

Blockchain goes further than this though.

In addition to recording facts or data points, blockchain also has the capacity to record who endorses or agrees with those recorded facts.

Think of the difference between a piece of paper, and a contract.

A piece of paper can contain any data, true or not.

A signed contract becomes more than a piece of paper because those signatures represent who agreed with the facts recorded on the paper at the time of signing.

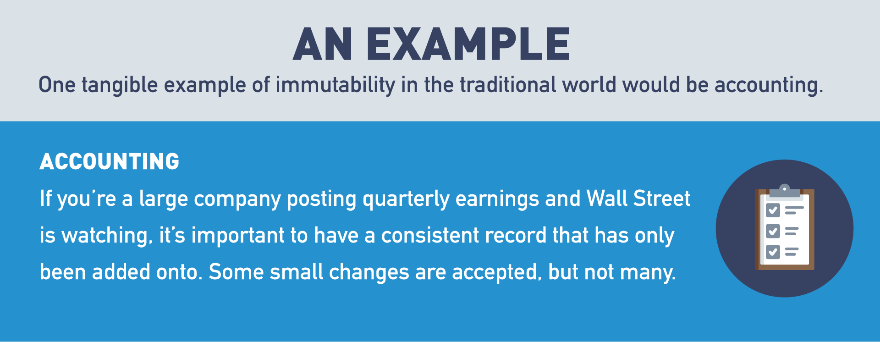
Blockchain provides a digital implementation of this process, and can be an immeasurably valuable tool when you need to capture not only what happened, but who was involved as well.

Imagine the new opportunities that arise when organizations can safely and securely share their most critical data with one another, with the trust that the data they're seeing hasn't been compromised or altered.

## Traditional Database Immutability Concept

The very nature of centrally-operated databases can’t be completely immutable, but that’s the case for blockchain as well. A centrally-run database can embed things into it with features that mention immutability (unchangeable). But if there is a central authority, they have all the ability in the world to override that feature.

Another point to keep in mind is that immutability has been around for many years, just like the majority of the tech used via blockchain; it is the combination of these that makes it unique.



## Blockchain Immutability Concept

Let's review the aspects of the public blockchain that improve the chances of it being immutable.

There are many different variables, but the main one is consensus. In a blockchain, it refers to the logs of transactions which are created by consensus among the chain’s participants. The basic notion is that once a blockchain transaction has received a sufficient level of validation and posted on the chain, it can almost never be replaced, reversed or edited.

If all the nodes within the network (Bitcoin specifically) are working to solve a really hard math problem by running many computers simultaneously, the chances of anyone overriding that are slim to zero.

But, if someone wanted to undermine the immutability of the Bitcoin blockchain, here’s how they would do it:

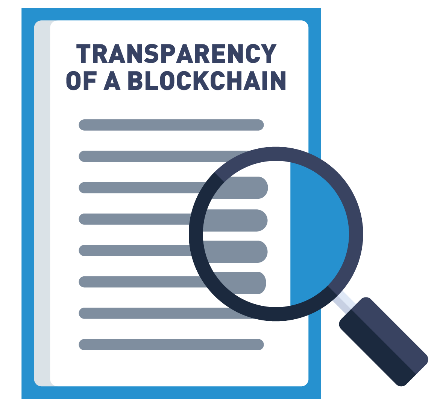
* First, they would install more mining capacity than the rest of the network put together, creating a so-called “51% attack”.
* Second, instead of openly participating in the mining process, they would mine their own “secret branch", containing whichever transactions they approve and censoring the rest.
* Finally, when the desired amount of time has passed, they would anonymously broadcast their secret branch to the network.

Since the attacker has more mining power than the rest of the network, their branch will contain more Proof of Work than the public one. Every Bitcoin node will therefore switch over since the rules of Bitcoin state that the more difficult branch wins. Any previously confirmed transactions not in the secret branch will be reversed and the Bitcoin they spent could be sent elsewhere. The computing power required to achieve this is enormous and probably only theoretical, but it’s important to consider.

One other less technical and malicious example would be from the Ethereum hard fork that directly happened after the DAO hack. In this example, the majority of the Ethereum nodes in the network decided to update the software preventing those hackers from withdrawing the cryptocurrency “earned” (stolen). This update could not be enforced, since every Ethereum user controls their own computer. Nonetheless, it was publicly supported by Vitalik Buterin, Ethereum’s founder, as well as many other community leaders. As a result, most users complied, and the blockchain with the new rules kept the name "Ethereum". A minority disagreed with the change and continued the blockchain according to its original rules, earning the title "Ethereum Classic".

## Transparency Defined

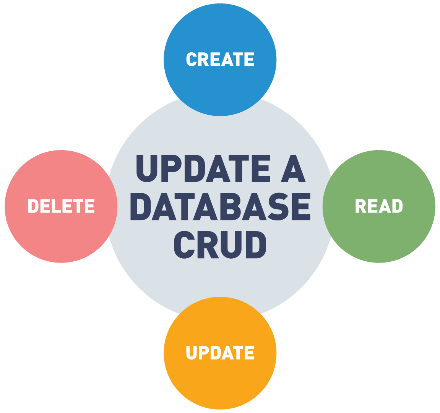
Anything that is see-through, where there is very little fog or obstruction in the way. Just like immutability, transparency comes on a spectrum. Certain things are more transparent than others. In the context of business/technology, this can be seen as a way of operating that is easy for others to see what actions are being performed.



For example, open source projects where all the source code is available for the masses.

## Traditional CRUD Explanation

Before we jump into how blockchain technology can be seen as transparent in certain aspects, let’s review the traditional CRUD method used by most databases.



In a traditional database, a client can perform four functions on data: *create*, *read*, *update*, *delete*. In a traditional database, there is usually an administrator, the authority giver who allows certain known participants in the database to do more than read/create; it allows them to update (change) and/or delete.

Due to the fact that the administrator is controlling who has access and who doesn’t, it’s easier to track these changes and prevent actors from tampering. In the public blockchain world, this isn’t necessarily the case.

## Blockchain Append-Only

Within the public blockchain world, every full node on the network is its own administrator, where it can create (e.g. add) and read; this is also known as read/write access (e.g. append-only). These nodes only add more data over time in the form of blocks, but all previous data is permanently stored and cannot be altered.

Read: query (e.g. search) and retrieve data from the blockchain.

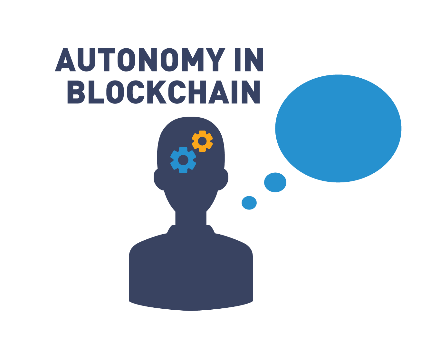
Write: add more data onto the blockchain.

As explained in the [*"Blockchains vs. Traditional Databases"*](https://towardsdatascience.com/blockchains-versus-traditional-databases-e496d8584dc) article by Shaan Ray,

"(...) if the blockchain has recorded that my Bitcoin wallet has 1 million BTC, that figure is permanently stored in the blockchain. When I spend 200,000 BTC, that transaction is recorded onto the blockchain, bringing my balance to 800,000 BTC. However, since the blockchain can only be appended, my pre-transaction balance of 1 million BTC also remains on the blockchain permanently, for those who care to look. This is why the blockchain is often referred to as an immutable and distributed ledger".

# Autonomy Defined

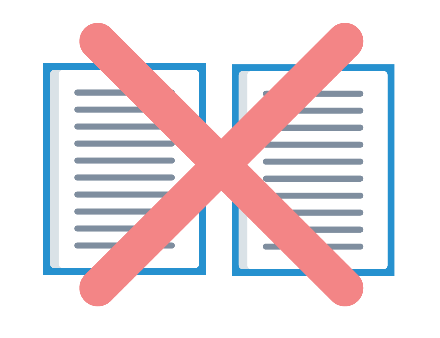
Independence or freedom, the ability to make your own decisions without being controlled by anyone else. This sense of freedom can be at the macro level of a country or at the micro level of a person.



As children and adults, we all want a little autonomy in our lives, careers, or relationships, but it’s just a matter of how much autonomy one truly wants and can handle.

## Autonomy: Human Process-Driven Complexity

The blockchain world is looking to solve all of this complexity with autonomy from intermediaries via automated smart contracts. In the traditional world of doing any kind of transaction with another party, there tends to be a lot of administrative paperwork, with third parties intervening every step of the way. Some of this is needed, but most of it becomes wasted time and effort which could be spent elsewhere.



Depending on how complex a transaction is between two parties, designated specialists can make the process more efficient. Many players are involved in the process, from contract drafters, signatories, and regulators. If a dispute over the contract occurs, many parties can be involved, including the courts.

This complexity can be seen within many areas of life. Take a moment to dissect the backend of certain services or products you use and this concept will become exposed very quickly.

## Autonomy with Smart Contracts

Autonomy in the blockchain world can be seen from many different angles. We are going to focus solely on smart contracts in this section, due to the amount of autonomy they provide everyone involved. The concept of smart contracts has been around for a long time and was first proposed by Nick Szabo, who coined the term in 1994.

The most simplified explanation is:

*"IF THEN ELSE" statement, which means IF X happens, THEN do Y, ELSE do Z.*

Take this concept and apply it to two or more parties, all interacting on a mutually agreed upon contract that executes based on their actions (or non-actions). An example of a smart contract could be,

*"if this happens before the end of the year, then you pay me, else I pay you".*

These "smart" contracts aren’t very smart, at least for now. That’s due to the simple explanation above because these contracts are "if, then, else" statements, which can vary in complexity based on how they’re stacked.

At the present moment, they can't make decisions without human intervention, or AI, which is a highly debated topic at the moment by many neuroscientists/philosophers. Companies are emerging as reliable Oracles that filter in real world facts to the blockchain. An Oracle is defined as a reliable source of information and blockchain makes that information immutable.

Anyone is able to create their own smart contracts without a central authority giving the right to do so. These contracts are executed without too much human intervention, and they’re stored on blockchain technology which provides a sense of permanence. These are three of the main attributes that can bring more autonomy to exchanging information between parties. Setting up a pre-agreed upon contract that’s coded into a blockchain and executes automatically when certain actions are taken is one step in the direction of not only improving our autonomy as individuals or companies, but shifting wasted resources (middle men/women) toward more impactful work.

## Smart Contracts

The first generation of blockchain platforms, collectively known as the "Blockchain 1.0" networks, were capable of capturing and recording data, but not acting upon it.

Bitcoin, the world's first mass-scale blockchain, was designed to capture and record the transfer of Bitcoin from one owner to the next.

At the time, nobody was envisioning blockchain as a platform on top of which applications and solutions could be built.

The release of Ethereum in 2015 changed this model. "Blockchain 2.0" was born, and now blockchain networks could not only capture data, they could act upon it as well.

All of this was made possible by the introduction of a technology called "Smart Contracts".

Put quite simply, a Smart Contract is some computer code deployed to a blockchain network.

Users can transact with the Smart Contract just as they would another user, except when transacting with a Smart Contract, the rules defined in the code are used to process the transaction.

This advancement now allows blockchain solutions to manage and automate processes, and record their results on a permanent, immutable, secure ledger shared with all relevant parties.

Consider the sale of a used car. Alice lists her car for sale, and offers a guarantee to any buyer that the car will be trouble-free for 1,000 miles. Bob looks at Alice's car and makes her an offer of $5,000.

Alice and Bob agree that Alice will take half the purchase price now ($2,500), and the other half if the car has had no major issues in the first 1,000 miles of Bob's ownership.

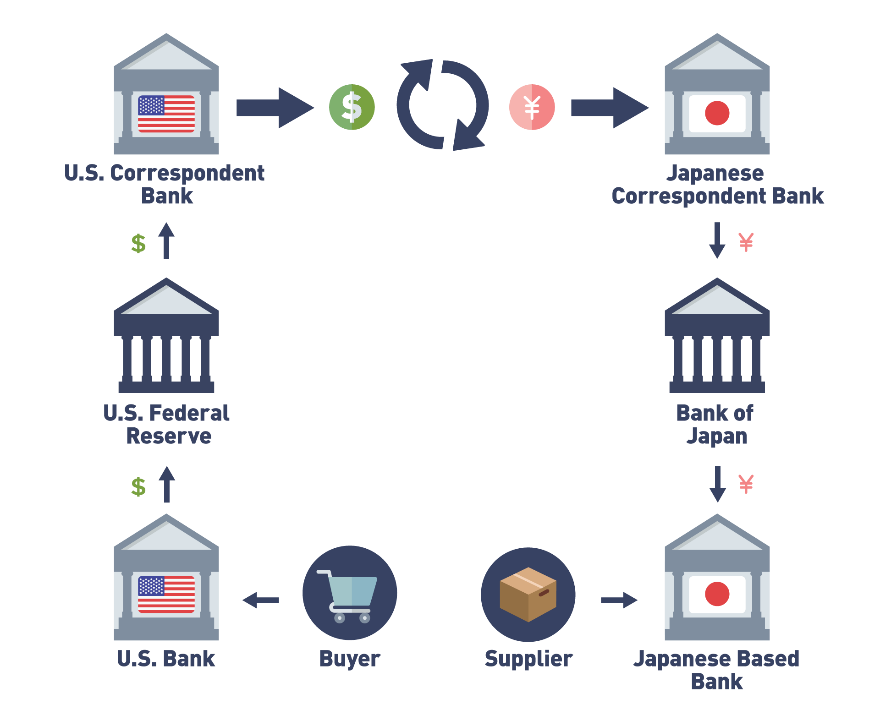
A Smart Contract could be created between Alice and Bob.

The Smart Contract would hold the remaining $2,500 in escrow, and if Bob had an issue with the car, he would report it to the Smart Contract. After 1,000 miles the Smart Contract will determine how much of the remaining funds are due to Alice and how much should be returned to Bob using the rules Alice and Bob initially agreed upon.

All details about the transaction would be recorded on a permanent, decentralized ledger which could be used at any point in the future to answer any questions about the transaction between Alice and Bob.

## Multi-Party Transactions

In our current world of transactions, there’s always a third party to assist with connecting the sender and receiver. This has always been the most efficient way to move something from Point A to Point B. But with a third party making the connection comes the need to trust that they’ll get whatever is being sent in an efficient, economical, and effective way. This trust is open to human and process error. But we’ve discovered through experimentation that certain use cases could be automated via smart contracts.



One example is cross-border payments. Sending money from one country (border) to another country (different border). The major issue with how this is traditionally done today (e.g. correspondent banking) is that certain transactions end up stopping off at 7–10 different checkpoint banks. This constant stopping is making the money movement more expensive (each bank takes a fee), slower, and less reliable (sometimes it might never make it). This type of transaction is heavily reliant upon third parties to facilitate the movement of information and money.

## Blockchain Multi-Party Sync (Removing Middlemen)

Blockchain technology has been shown to provide many benefits, but one of the most prominent and immediate benefits is removing middlemen (third parties) from a variety of processes. There is a long list of examples for middlemen currently being removed, such as:

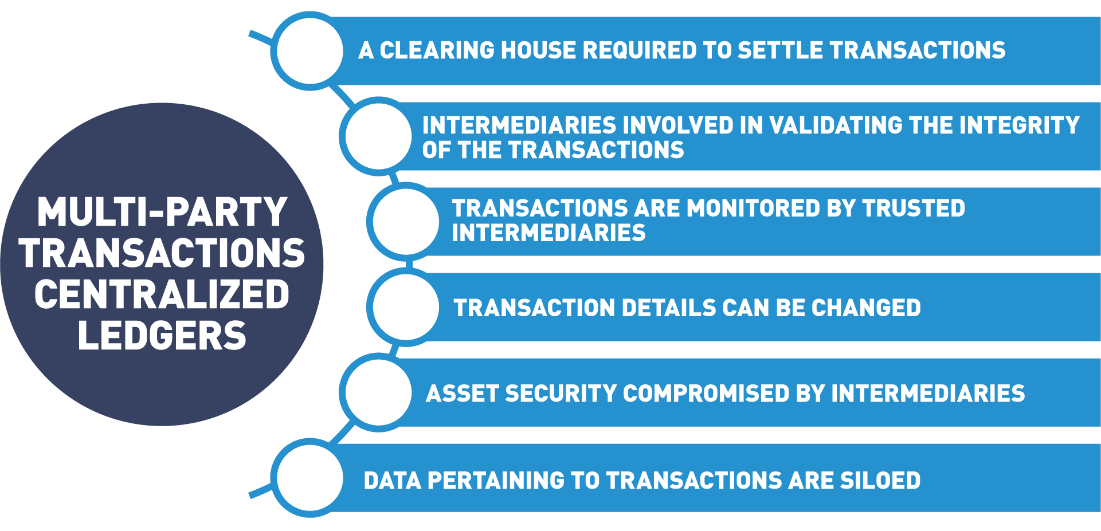
* Energy distributors
* Payment networks (Visa and Mastercard)
* Content distributors (YouTube, Facebook, Medium, etc.)
* Central exchanges (NASDAQ, London Stock Exchange, NYSE, etc.)
* Cloud database providers (AWS, Azure, etc.).

How is the blockchain world removing this middleman? The answer is all around trust. Within the public blockchain world, where everyone is theoretically anonymous, there needs to be trust so we’re able to exchange valuable things without the concern of bad actors. Trust is built into the consensus mechanism that we’ve mentioned multiple times throughout this course. This incentivizes all the participants to help secure and validate good actions throughout the network. With that built-in "trustless" trust, we’re able to remove those middlemen that provide no additional value, plus it could potentially increase the efficiency based on which public blockchain is being used.

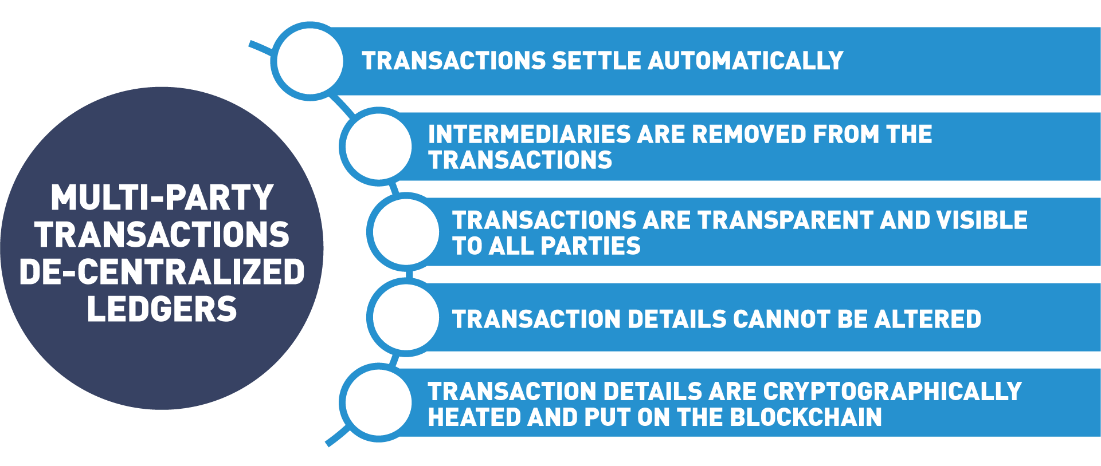


## Cross Border Payments and Ledgers

Traditional centralized ledger systems have weaknesses. Accuracy is dependent on intermediaries who can change details of the centralized ledger. Data derived from the ledger is siloed and misused.



Distributed decentralized ledgers are not dependent on intermediaries who can manipulate the data. Data is secure and tamper resistant.



## 5.2 Double Spend

Bitcoin, the world's first blockchain, was created as part of an attempt to create the world's first truly viable digital currency.

Bitcoin was not the first attempt to create a digital currency, but it was the first which was able to successfully solve a long-standing problem - the "Double Spend" problem.

The Double Spend problem is quite simple.

Let's say Alice owes a debt of $5 to both Bob and Carol.

Alice's total debt is $10, but let's assume she only has $5 currently.

If Alice's transactions were recorded on two separate ledgers, it is possible that one ledger would show she paid $5 to Bob, while the second ledger may show she paid $5 to Carol.

It would be impossible to tell who actually got paid.

This is the double spend problem - any financial ledger MUST prevent Alice from spending her $5 more than once.

Digital assets are particularly vulnerable to the double spend problem as we generally design them to be easy to copy and distribute.

If you've got a great picture you took with your phone, it's easy to post one copy to

Facebook, another copy to Instagram, then you might text a copy to your spouse, and email a copy to your parents.

We live in a world where digital assets are easy to copy and distribute, by design.

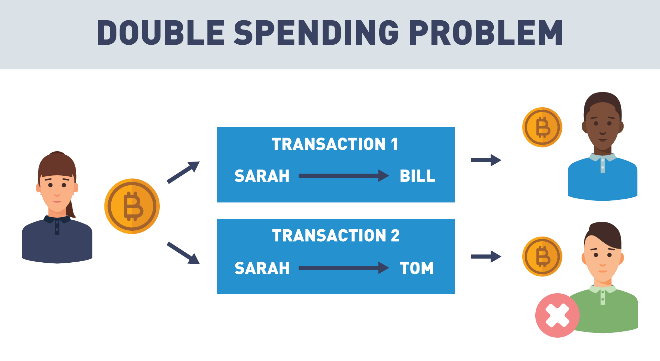
A digital currency should NOT be easy to copy and distribute though.

It was overcoming this technical challenge that lead to so many failed attempts at digital currency before Bitcoin, and the innovations that the solution to this problem has delivered are now being leveraged to track and manage many different types of assets and data that we never could easily manage before.

It is this possibility of building tools and solutions that were never before thought possible that has so many people excited about the blockchain revolution!

## Blockchain Solves The Double Spend Problem

Back in the early 1990’s, developers, cryptographers, and different groups of people were trying to solve the double-spend problem as it related to digital cash, previously known also as electronic cash. Double spending within Bitcoin is the act of using the same bitcoins (digital money files) more than once.



If I buy an apple for $1, I cannot spend that same $1 to buy an orange. If I could, money would be worthless since everyone would have unlimited amounts and the scarcity that gives the currency value would disappear. The network protects against double-spending by verifying each recorded transaction within the blockchain utilizing a consensus mechanism (explained in the previous section).

Bitcoin was the first decentralized protocol to solve this problem and now more protocols are following, such as: Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Directed Acyclic Graphs (DAG) structures, Proof of Authority (PoA), etc.

## 5.3 Digital Currency Difficulties

Today, when someone mentions digital currency, usually Bitcoin or crypto is the first thing that comes to mind, but digital currency had a long history before Bitcoin popularized it. This history goes all the way back to 1983, when [David Chaum](https://en.wikipedia.org/wiki/David_Chaum) introduced the idea of digital cash in a research paper. Then, in 1992, he founded DigiCash, an electronic cash company, which eventually went bankrupt in 1998 due to adoption (buyout by another financial institution). Today, David is a leading pioneer of blockchain companies such as [Elixxir](https://xx.network/cmix) and [Praxxis](https://xx.network/xx-consensus) to provide scalable digital sovereignty.

There were many other attempts to create digital cash over the years, but many failed due to a variety of reasons, such as:

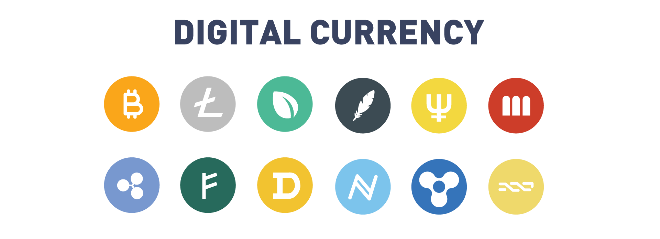


Other attempts include:

* CyberCash in 1994 (failed after the Y2K bug of 2000).
* E-gold in 1996 (sunk by continuous money laundering, hacking, and extortion).
* Liberty Reserve in 2006 (shut down in 2013 due to this becoming a great hangout spot for cybercriminals).

## Digital Currencies Overview

Digital currencies are available only in the digital world and not in the physical world. They can be defined as any currency, money, or money-like asset that is primarily managed, stored or exchanged on computer systems. Examples of digital currencies include cryptocurrency, virtual currency and central bank digital currency.



## Cryptocurrency Defined

According to [Investopedia](https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/),

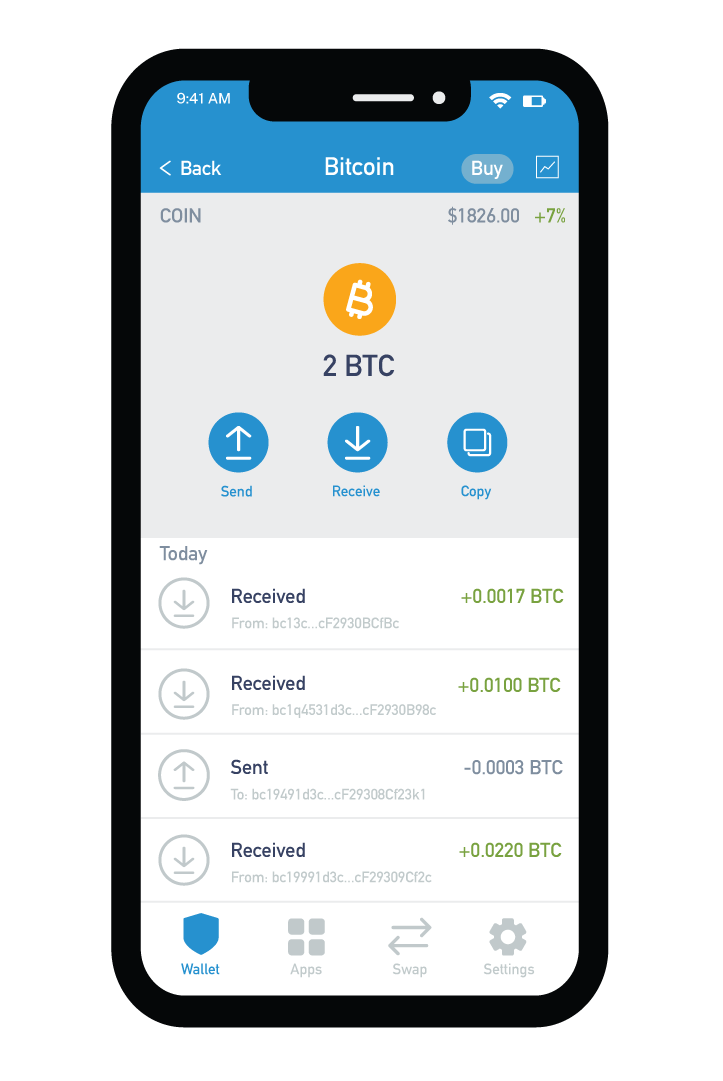
"A cryptocurrency, broadly defined, is currency that takes the form of tokens or “coins” and exists on a distributed and decentralized electronic ledger. While a large majority remain completely intangible, some cryptocurrencies have ventured into the physical world by building associations with companies offering traditional payment rails (credit cards and payment processors)".

## Cryptocurrencies Markets

To break down the crypto markets, let's start with some basic definitions.

## **Crypto Wallet**

A cryptocurrency wallet is an application on your computer or smart phone that connects you to a blockchain where you can trade cryptocurrencies. A Bitcoin wallet allows you to trade Bitcoin, an Ethereum wallet accommodates Ether. You can not send Bitcoin to the Ethereum blockchain, each cryptocurrency must transact on its own blockchain.



### ****Multi-currency Wallets****

Some wallets allow you to hold multiple cryptocurrencies in the same application. In these wallets, each cryptocurrency will have its own balance. To initiate a transaction, the application will create a cryptographically secure address (specific for the particular blockchain). This address acts as your account number and lets you send and receive the cryptocurrency.

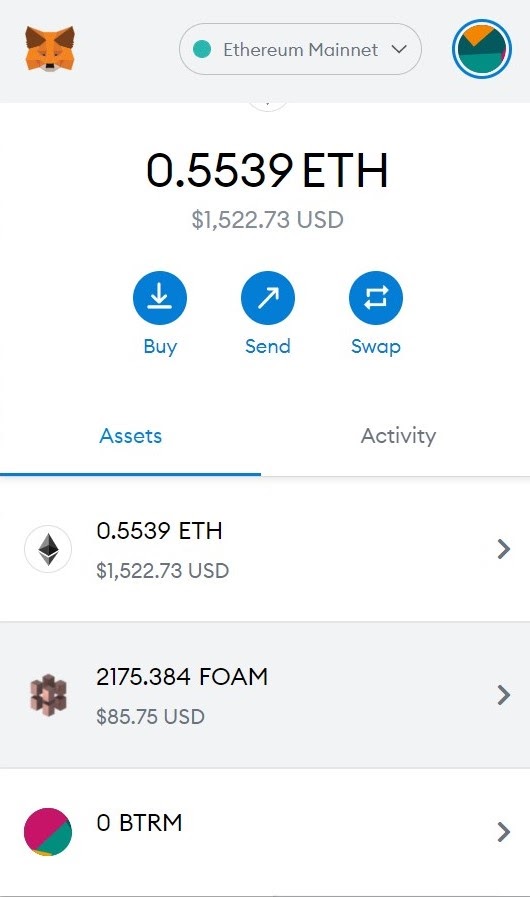


**Atomic Swaps**

Additional features in these wallets lets you “swap” one cryptocurrency for another. The application provider acts as the intermediary to secure the transactions from one chain to the other.

**Metamask**

[Metamask](https://metamask.io/) is a cryptocurrency wallet used to interact with the Ethereum blockchain and other blockchains issued in accordance with the Ethereum Platform. Tokens issued in accordance with the ERC-20 standard for utility tokens can be stored in a metamask wallet. Metamask not only stores cryptocurrencies but acts as a gateway to blockchain applications. You can access the wallet through a mobile application or a browser extension.



ConsenSys, spearheaded by [Joe Lubin](https://consensys.net/about/joseph-lubin-founder-of-consensys/), an early Ethereum programmer, is a software engineering company that helps developers build next-generation networks and enable enterprises to launch more powerful financial infrastructure. [Consensys Mesh](https://mesh.xyz/) is a playground for entrepreneurs and programmers to build decentralized platforms and projects, Metamask is just one project to come out of the efforts at Consensys.

One example of how the Metamask wallet is used is with the [CryptoKittes](https://www.cryptokitties.co/catalogue) project. CryptoKitties are one of the first examples of a digital collectible where you own the rights (private keys) to code that represents a unique kitten. A kitten is a set of identifiers built or “bred” by a smart contract to be one of a kind. In order to purchase, view or interact with a digital kitten you must open your Metamask wallet and connect it to the cryptokitties.co website.

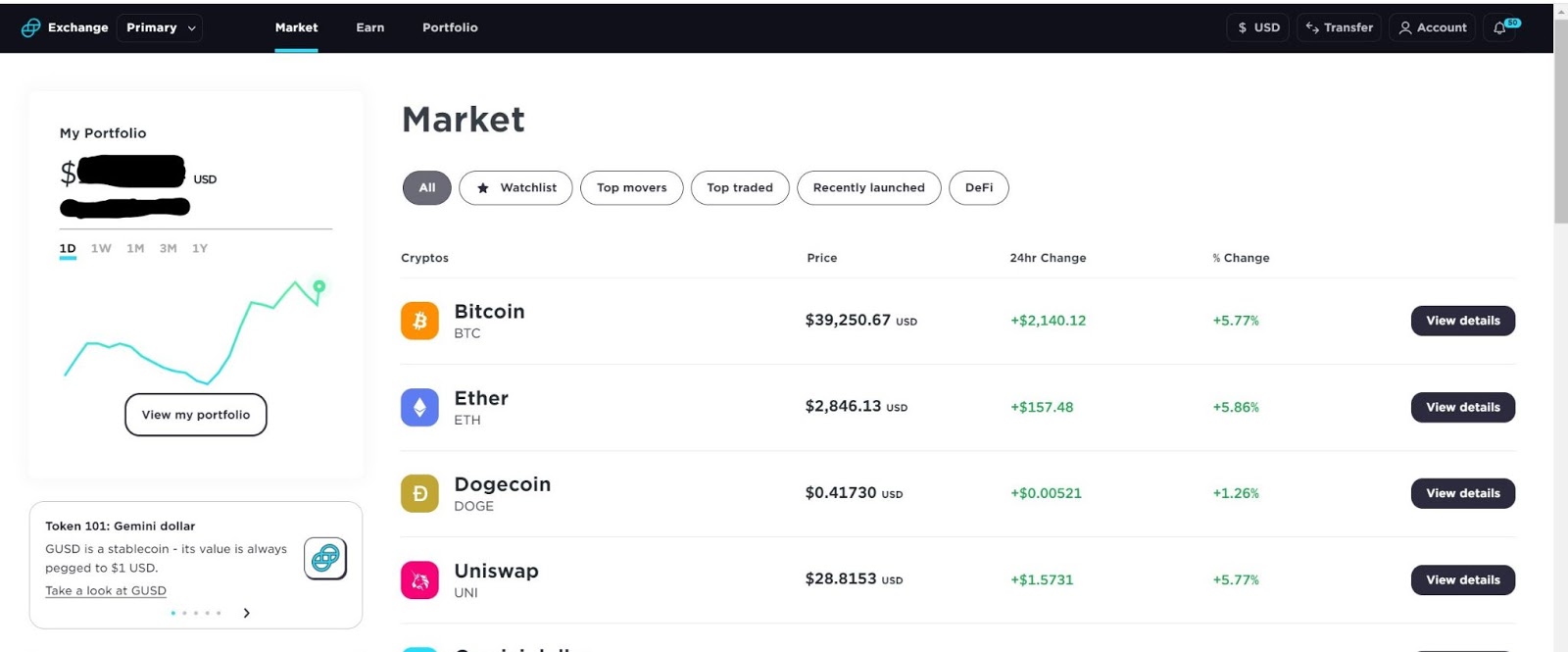


Kittens purchased on the cryptokitties.co site will be stored in the Metamask wallet associated with your account or can be put up for sale at an NFT marketplace. Any fees or revenue from your kittens will automatically be reflected in your Metamask wallet totals. Cryptokitties are the first example of a non-fungible token which we will cover in the next section.

**Exchanges**

Cryptocurrency exchanges vary in complexities and user experience.

**Beginners**  
To start off, it is advantageous to deal with a centralized solution to store your cryptocurrency. These larger exchanges act as a bank for your cryptocurrencies. Offering features like loans and staking rewards (rewards for being an active part in a network).They vet the currencies they allow you to trade and store, while controlling the private keys for you, so accessing your currencies is as easy as a username and password. Such examples of these organizations are [Coinbase](https://www.coinbase.com/) and [Gemini](https://www.gemini.com/). Below you can see a screenshot of the [Gemini Custodial Crypto Account Dashboard](https://exchange.gemini.com/signin?redirect=e2aa461e75019f06a9907a89b5090decb94caf52-1626117922675-%2F):



Advanced  
In keeping with the decentralization nature of the cryptocurrency markets, exchanges exist where you are the custodian of your accounts and trading is done from your computer or smartphone. This is where the term Decentralized Finance was born. It gives you the ability to apply smart contracts to govern your trades and access to markets previously only for accredited investors. Such examples of decentralized exchanges are [Liquid](https://app.liquid.com/exchange/BTCUSD), [SushiSwap](https://app.sushi.com/swap) and [Uniswap](https://uniswap.org/). Below is the screenshot of the [Liquid Exchange](https://app.liquid.com/exchange/BTCUSD):



**Hardware Wallets**

Hardware wallets offer an alternative to storing your cryptocurrency online. These devices plug into a USB port and transfer your private keys (ownership rights to the cryptocurrency) from your “hot wallet” (mobile, computer or web based) to be stored offline. If the device is damaged or lost, so are the cryptocurrencies stored. This is what the [ledger wallet](https://shop.ledger.com/products/ledger-nano-s/?flow_country=USA&msclkid=91c26052e5701161046300fd18bf7e2d) looks like:



## Self-Sovereign Identity (SSI)

As explained by [Drummond Reed](https://www.evernym.com/blog/team/drummond-reed/),

"Web 1.0 used centralized identity; Web 2.0 graduated to federated identity; now Web 3.0 is using decentralized digital identity, a model known as "self-sovereign identity" or "SSI" because now individuals control their own portable digital identity credentials in their own digital wallets—just like we prove our identity with physical credentials from our physical wallets every day. The digital signatures on these credentials use blockchain technology for decentralized public key management. Finally we can have a trust layer for the Internet that doesn't require everyone to rely on centralized authorities".

The concept of self-sovereign identity (SSI) is based on the idea that the Internet was created without a way to properly deal with identifying participants. Innovative minds, such as Drummond Reed and Alex Preukscha, have been working on solutions to this problem. We will start with some key terms taken from the [*"Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials"*](https://www.manning.com/books/self-sovereign-identity?utm_source=freecontentcenter&utm_medium=blog&utm_campaign=book_selfsovereignidentity&utm_content=article_01) book by Reed and Preukscha.

The Internet was designed to identify computers, not users. The result is a tangled web of passwords, and usernames, and siloed data that is bought and sold without our consent. With blockchain and cryptographic techniques, solutions are being developed to fix what is broken with identity and the Internet. The [W3C Consortium](https://www.w3.org/Consortium/) is an international community where members work together to develop web standards. Led by web inventor and Director [Tim Berners-Lee](https://en.wikipedia.org/wiki/Tim_Berners-Lee) and CEO [Jeffrey Jaffe](https://www.w3.org/People/Jeff/), W3C's mission is to lead the Web to its full potential. W3C is working on standards that can be used to define a new paradigm for the Internet and Identity.

## Key Concepts

**Self-sovereign identity (SSI)**

SSI is relatively new, having only emerged onto the Internet stage in 2016. At one level, SSI is a set of principles about how identity and personal data control should work across digital networks. At another level, SSI is a set of technologies which build upon core concepts in identity management, distributed computing, blockchain or Distributed Ledger Technology (DLT), and cryptography.

**Verifiable credentials**

The essence of decentralized identity is transitioning physical identity credentials (birth certificate, driver licenses, passports, college degrees, medical records, etc.) to a digital twin that the individual can possess in a digital wallet.

**Verifier**

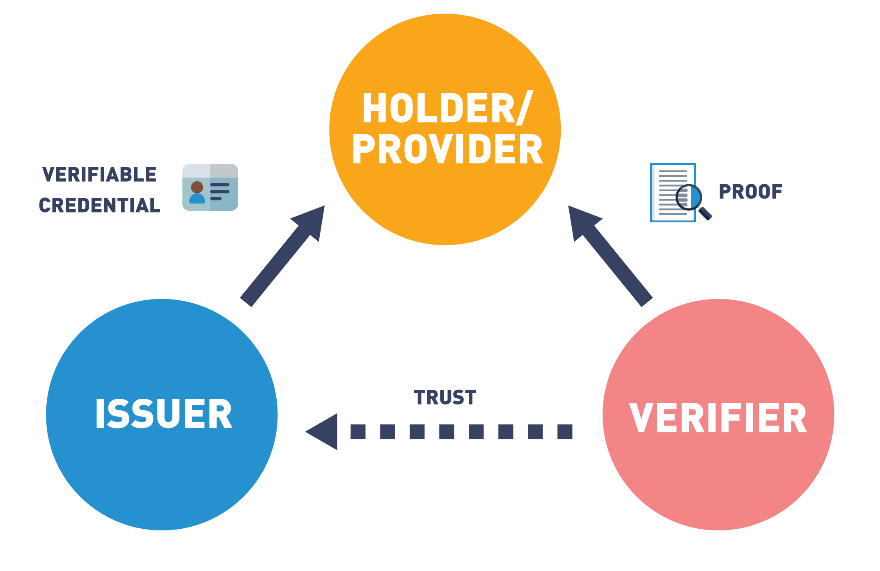
A verifier is the person, organization or computer program granting verification of an assertion. They request proof that a claim or statement about a credential is true.

**Issuers**

Issuers are the source of credentials—every credential has an issuer. Most issuers are organizations such as government agencies (passports), financial institutions (credit cards), universities (degrees), corporations (employment credentials), NGOs (membership cards), or churches (awards).

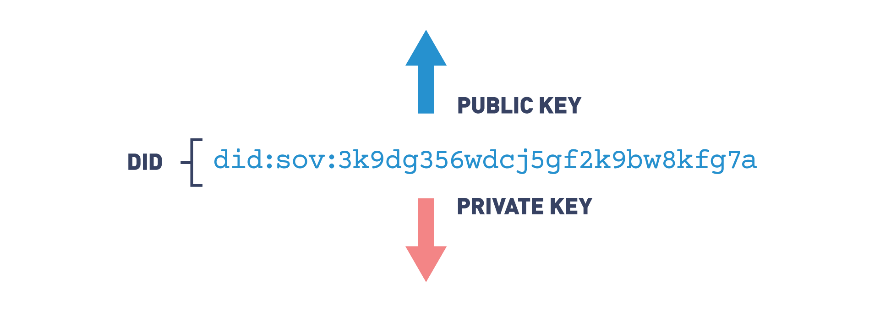
**Holders/Provers**

Providers request verifiable credentials from issuers, hold them in the holder’s digital wallet (below), and present proofs of claims from one or more credentials when requested by verifiers (and approved by the holder). Although we most commonly think of individuals as holders/provers, holders/provers can also be organizations using enterprise wallets, or things in the sense of the Internet of Things (IoT). The trust triangle represents the Trust over IP version of how the new relationship will operate.



**Decentralized identifiers**

According to the WC3, [decentralized identifiers](https://www.windley.com/archives/2020/11/didcomm_and_the_self-sovereign_internet.shtml) (DIDs) are a new type of identifier for verifiable, decentralized digital identity credentials. These new identifiers are designed to enable the controller of a DID to prove control over it and to be implemented independently of any centralized registry, identity provider, or certificate authority. WC3 is working on ways to standardize the format for DIDs.



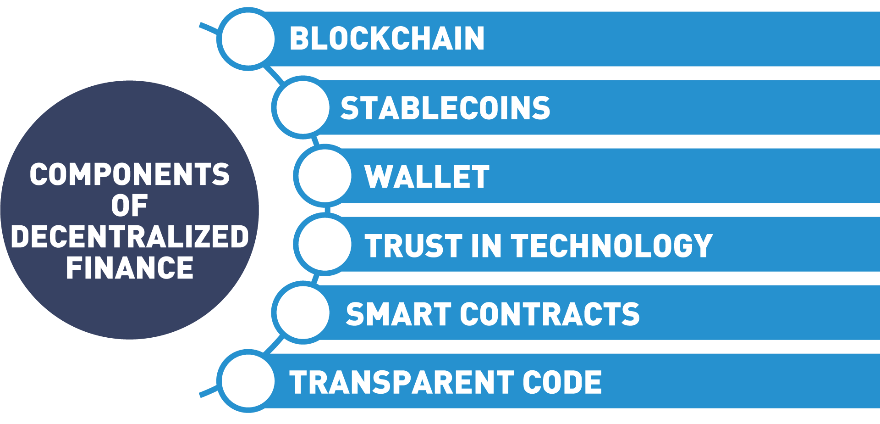
The DID above is structured to identify what type of credential, the issuer and the cryptographic hash of the credential.

The [Sovrin Foundation](https://sovrin.org/) and [Everynym](https://www.evernym.com/) are leading pioneers in this new emerging sector offering identity solutions in sectors such as Healthcare and Refugee Management.

## Decentralized Finance

According to [*"The Complete Beginner's Guide to Decentralized Finance (DeFi)"*](https://academy.binance.com/en/articles/the-complete-beginners-guide-to-decentralized-finance-defi) article by Binance Academy, Decentralized Finance or DeFI refers to a system of financial software that enables financial products to be made available to the public on decentralized blockchains. As we have learned, the term decentralized and its ramifications will revolutionize how we interact with each other. These new interactions can have different effects in various sectors. In the financial markets, new interactions will dramatically change the current structure by eliminating the need for intermediaries. Banks, lending institutions, Money Managers, Market Analysts, Hedge Fund Managers, and other positions and functions can now be performed using smart contracts.

With new technology platforms, open source projects are fueled by blockchains, incentive models, stablecoins, smart contracts and self hosted wallets that remove financial middlemen. Users' funds that are pooled together for investment advantages are now managed by a series of smart contracts that execute programmed financial trades instead of a third party.



## Benefits of Decentralized Finance

Along with the new decentralized financial model come new innovations that have far reaching ramifications. Microloans, smaller loans made from pools of capital, now are available granting access to these financial vehicles to participants previously excluded. For example, in agriculture, farmers are able to secure small loans to help them get crops to market.



Regulating these new financial instruments is proving challenging as government agencies wrestle with controlling currencies that do not recognize borders. And have a steep learning curve. A stable price coupled with the benefits of blockchain, new financial markets are emerging that will change the current financial markets making them more inclusive.

## Central Bank Digital Currencies (CBDC)

Enterprise blockchain solutions are successfully creating efficient micro-economies that are decentralized, immutable and efficient. The success of these projects are forcing governments to take a look at blockchain technology through the lens of streamlining current financial systems. More specifically, studying how blockchain can improve the way governments handle their central banking systems.

Central Bank Digital currencies are a digital form of central bank money that is issued by the central bank as part of its overall monetary policy. In the Ledger Insights article titled [*"IMF Outlines Pros and Cons of Central Bank Digital Currency"*](https://www.ledgerinsights.com/imf-pros-cons-central-bank-digital-currency-cbdc/) it is estimated that 80% of central banks are exploring CBDC.

Some of the benefits of Central Bank Digital Currencies include:

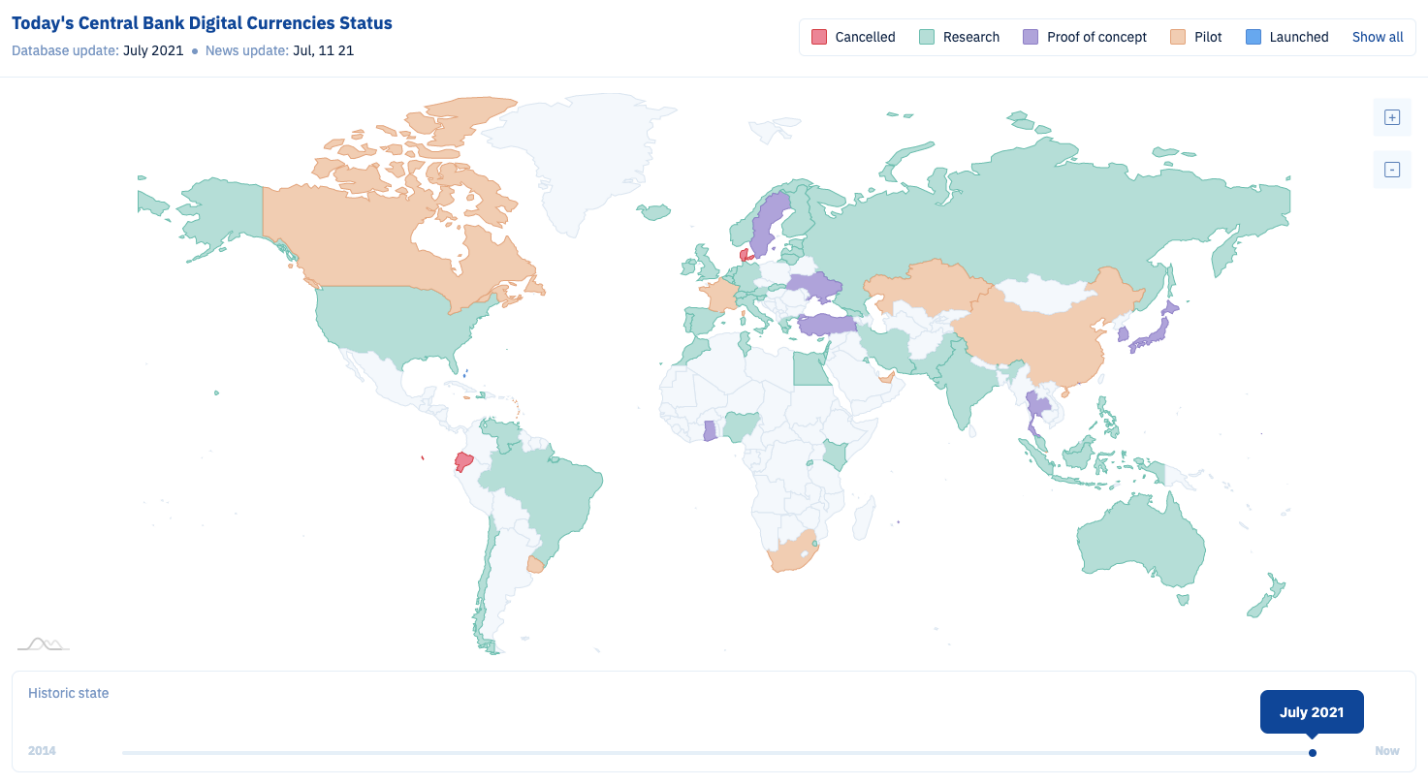
* Transparent monetary policy  
  Due to the distributed ledger technology’s feature of transparency, creating a digital currency will bring clarity to the government's monetary system, where policy can be recorded on the blockchain and remain immutable.
* Combat money laundering  
  Money laundering is converting illegal funds into legal payments systems. Blockchain can eliminate this practice with a shared ledger that keeps a complete transaction history, making it impossible to erase. Like with all money transfers, certain safeguards are in place to identify wallets or accounts to users. Anti Money Laundering (AML) policies like Know Your Customer (KYC) further ensure citizens are following laws in their countries.
* Cross-border payments  
  Blockchain technology eliminates middlemen in cross-border payments, reducing transfer fees, and making interactions faster and frictionless while keeping the integrity of the underlying asset.
* Government efficiency  
  A huge benefit for governments to research CBDC is to overcome existing problems inherent in the existing antiquated systems. By moving to the digital realm, governments can enjoy the cost reductions blockchain offers.
* Banking the unbanked  
  To be unbanked describes a person who does not have a checking or savings account. Being unbanked puts individuals at an extreme dis-advantage as they do not have access to financial services like loans and usually pay more for check cashing. By creating a digital currency governments can include this market segment, onboarding people with mobile phones.

## Types of Central Bank Digital Currencies

According to the "What Is Retail Central Bank Digital Currency?" article by Matthieu Saint Olive, there are two types of central bank digital currencies:

* Wholesale CBDC  
  A wholesale CBCD is a type of currency used by financial institutions to buy and sell financial assets. It would replace real time settlement systems used today.
* Retail CBDC  
  Retail central bank digital currency would be used as a digital twin for fiat currency. Citizens would use it to pay for things, send money and save it.

Central Bank Digital Currencies are being considered across the globe.



According to the [CBDC Tracker](https://cbdctracker.org/), the Sand Dollars, a retail CBDC issued by the Central Bank of the Bahamas is the first nationwide Central Bank Digital Currency. The US Federal Reserve is researching CBDC for the US with the Federal Reserve Bank of Boston and [MIT](https://dci.mit.edu/) committed to a multi-year collaboration to build a hypothetical currency called the Hamilton.

Hyperledger created a [Capital Market Special Interest Working Group](https://wiki.hyperledger.org/display/CMSIG) spearheaded by [Vipin Bharathan](https://www.forbes.com/sites/vipinbharathan/?sh=5b44f4473f76) working on standards for CBDC’s. This working group is just one of many discussing CBDC’s and is open for anyone to [join](https://lists.hyperledger.org/g/capital-markets-sig/).

## 5.4 Non-Fungible Tokens (NFTs)

At the beginning of this course we discussed the Internet and the changes it has gone through. We started with Web 1.0 and how it revolutionized the way exchanged value, looking back it is hard to believe we managed without email. Then came Web 2.0 and our social status and personal information flowed on the net as freely as the air we breathe. Web 3.0 started with blockchain and the transfer of value, the first killer application being Bitcoin.

Now, you may be asking yourself, "What's next?". That's where non-fungible tokens come into play and are set to revolutionize art, music, sports and gaming by offering a new kind of digital ownership and the ability to transfer unique value with digital collectables. We first saw a glimpse of this new market with CryptoKitties but let's look deeper into this phenomenon.

According to [Wikipedia](https://en.wikipedia.org/wiki/Non-fungible_token), a non-fungible token:

"is a unit of data stored on a digital ledger, called blockchain, that certifies a digital asset to be unique and therefore not interchangeable".

NFTs can represent art, music, videos and other digital files where access to the original file is restricted, limited to the owner proving authenticity and providence. The first standard for issuing NFT’s was based on the Ethereum's [ERC-721](http://erc721.org/) that differs from the ERC-20 as ERC-721 tokens are all unique which makes them perfect for the collectibles market. The [ECR-1155](https://eips.ethereum.org/EIPS/eip-1155) aims to improve on the previous token standard by further defining assets.

Let's now take a look at some of the types of non-fungible tokens:

* Digital artwork  
  By guaranteeing uniqueness of a digital item and applying smart contracts to the terms of the sale, artists are now in control of the ownership rights to their work giving control of royalties back to the creator. The New York Times reported art entitled ["Everydays – The First 5000 Days"](https://www.nytimes.com/2021/02/24/arts/design/christies-beeple-nft.html), by artist Mike Winkelmann, also known as [Beeple](https://en.wikipedia.org/wiki/Mike_Winkelmann), sold for $69.3 million USD in 2021.
* Collectables  
  As we saw with CryptoKitties, non-fungible tokens create unique items. One of the more popular collectables are [CryptoPunks](https://www.crypto-news-flash.com/ethereum-eth-cryptopunks-nft-index-fund-migrates-to-sushiswap/), a collection of 10,000 uniquely generated characters each having a unique owner registered on the Ethereum blockchain. A crypto punk, Punk 1651 sold for 78 ETH or $136,850.22 USD.
* Games  
  NFTs can be used to represent assets in computerized games. With the ability to trade assets created in a gaming platform, users and creators of assets in the digital game can trade assets on a third party marketplaces and store them in a wallet where the private keys are controlled by the gamer, taking control away from the game developer.
* Music and film  
  With NFTs, musicians and filmmakers can now tokenize their work where the artist monetizes and profits from their content. When artists release music or film as NFT, they retain control and realize royalties in a more equitable way. Musicians can join in decentralized marketplace such as [Mediachain](http://www.mediachain.io/) a [Ujo](https://mesh.xyz/) to ensure artists are paid fairly, musicians enter into smart contracts that state royalty stipulations without the need of a third party.
* Sports  
  The sports industry has embraced the idea of NFTs from tokenizing memorable sporting moments to trading card collectables. [NBA Top Shots](https://nbatopshot.com/) being the leader for creating a marketplace for NBA collectible cards and moments.
* University research  
  In May 2021, [UC Berkeley](https://en.wikipedia.org/wiki/University_of_California,_Berkeley) announced it would auction off NFTs for the patent disclosure for two Nobel Prize-winning inventions dealing with gene editing and Cancer Immunotherapies.

The younger generation of collectors aren’t interested in China sets and linen, but something they can show their friends on their social media accounts. The future of the non-fungible token promises to be one of the more energetic market segment blockchain has seen.

## Interoperability

To end this section, we must mention interoperability. Interoperability in blockchains deals with creating standards so different types of blockchains can communicate with each other.

If new emerging blockchains can’t communicate with each other, we will have the same issues with siloed data that created frustration with the Internet of Today. As different blockchains take different approaches to interoperability, standards will emerge that will help regulate the industry and help with widespread adoption. Currently Hyperledger and Ethereum are working together on interoperability projects from [Hyperledger Besu](https://wiki.hyperledger.org/display/besu) (to learn more about Hyperledger Besu enroll into [Hyperledger Besu Essentials: Creating a Private Blockchain Network (LFS176x)](https://training.linuxfoundation.org/training/hyperledger-besu-essentials-creating-a-private-blockchain-network-lfs176x/)), an open source Ethereum client for enterprise solutions that can be run on the Ethereum public network or on a private permissioned network. Other projects in the [Hyperledger labs](https://wiki.hyperledger.org/display/labs) that deal with interoperability are working on standards that will make it easier for blockchains to talk to each other.

When considering how blockchain interoperability can work, consider email and smartphone. Both of these technologies have the ability to interoperate. Outlook email server can receive email from the Gmail server and Verizon cell phone carriers can transfer and accept calls from T-Mobile. These services would not operate efficiently, if these companies couldn't exchange data. With this in mind, blockchain are developing projects that, like smartphones and emails, will transfer value and information across blockchain seamlessly.

## 5.5 Summary

In this chapter, we discussed:

* How some features of blockchain are solving real world problems.
* How immutability is opening up new cooperation models for business.
* How the concept of *autonomy* will reduce conflict by eliminating human processes.
* New emerging business models as multiparty exchanges, with built in trust, are being developed.
* How the double spend accounting issue is solved with blockchain.
* Future trends in decentralized finance and Central Bank Digital Currencies.
* The importance of *interoperability* between blockchains.
* Non-fungible tokens (NFTs) and their importance to the blockchain ecosystem.

## 6. Blockchain Use Cases

## 6.1 Overview

This final section will examine blockchains in action. We will see how blockchain is providing solutions for businesses, governments and social projects. Businesses fueled by blockchain solutions are developing new relationships for more efficient communication and trust among untrusting parties, fostering new business models.

Governments are realizing the best way to serve the population is to develop digital identity management systems where individuals hold their credentials and services can instantly be matched to those in need. We will discuss how governments are using blockchain to tackle document and workflow management issues creating better services for their citizens.

Next, we will discuss the impact blockchain is having in developing countries. We will look at examples of how philanthropy is offering new transparency and accountability to charity organizations with massive global benefits.

Then, we will devote some time discussing new technologies and emerging breakthroughs developers are building. Either to enhance existing systems or offering services to help users manage blockchains, these new advances are like nothing we have seen before.

Finally, we will see use cases designed to improve the individual's experience, decentralized gaming platforms and new marketplaces inventing new worlds to interact in. Blockchains are reshaping the way artists and musicians are benefiting from their creativity by having the royalties delivered directly to them, without agents and middlemen.

***Blockchain will be a part of everyone's future.***

## Learning Objectives

By the end of this chapter, you should be able to:

* Discuss blockchain use cases in business enterprises.
* Discuss use cases in the public sector.
* Explain the relevance of blockchain in social impact projects.
* Discuss developing new technologies made possible by blockchain.
* Explain how blockchain will improve the human experience.

## 6.2 Blockchain Use Case Categories (Blockchain in Practice)

Blockchain technology promises sound extremely lofty. Let's take a look at how this technology is improving the way we trust each other and interact. It is showing a new path that will improve the lives of so many. We will see how identity management is key (no pun intended) to all the use cases we discuss. For our discussion, we will categorize use cases by who is developing solutions, starting with large enterprise solutions to smartphone and web browser applications powered by blockchain that put control back in the user's hands:

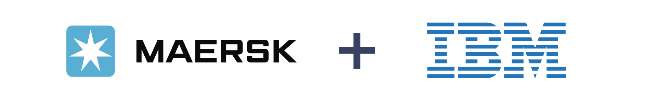
* Enterprise solutions  
  Businesses and organizations are implementing blockchain to overcome obstacles in transparency and trust forging new associations with global implications.
* Public sector solutions  
  Governments are using blockchain solutions to improve services that they provide to their citizens. Digital identity solutions, central bank digital currencies and transparent workflows are bringing efficiency to the public sector system with an end result that benefits citizens. With that, new laws are needed to regulate this technology.
* Social impact solutions  
  Social impact blockchain solutions address social and environmental challenges. Backed by the [17 United Nations Sustainable Development Goals](https://sdgs.un.org/goals) blockchain developers, investors, philanthropists, government agencies and foundations are developing solutions that tackle these global problems.
* Platform developers' solutions  
  Blockchain is a new technology constantly improving and changing. Developers are creating standards and new platforms to bring this technology into the mainstream.
* End user solutions  
  Everyday solutions emerge that put decentralized blockchains and all the benefits they promise in the hands of individuals from new decentralized marketplaces to new ways to express your music, art, and even let you trade property built inside a game.

## 6.3 Enterprise Solutions Overview

Businesses fueled by blockchain solutions are developing new relationships for more efficient communication and workflows, fostering new business models. Problems with how we transact online, to the cost of doing business, are solved with blockchain. Let’s look at an enterprise supply chain solution built with blockchain.

## Global Supply Chains

Supply chain data is not always visible or trusted. In recent times of disruption supply chains matter more than ever. Global supply chain and blockchain are working to secure systems to better handle these disruptions. The Covid pandemic shed light on the frailty of our supply chains which accelerated discussion over blockchain solutions.



Learn more about the collaboration between Maersk and IBM from the [*"Digitizing Global Trade with Maersk and IBM"*](https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/) blog post by Michael White.

## Supply Chain - Maersk

Global trade functions much as it has since the introduction of the shipping container in 1956.

Manual, paper-based processes are still common and information about the status of goods is locked away in organizational silos.

Today, 90% of goods in global trade are carried by the shipping industry with the supply chain slowed by the complexity and sheer volume of point-to-point communication across a loosely coupled web of land transportation providers, freight forwarders, customs brokers, governments, ports, and ocean carriers.

IBM and Maersk are addressing this problem with a distributed permission platform accessible by the supply chain ecosystem designed to exchange event data and handle document workflows.

Maersk and IBM are employing blockchain technology to create a global tamperproof system for digitizing trade workflow and tracking shipments end-to-end, eliminating frictions including costly point-to-point communications.

The collaboration will launch with the potential ability to track millions of container journeys per year and integrate with customs authorities on selected trade lanes.

In a recent test by Maersk, shipping a single container of flowers from Kenya to the port of Rotterdam resulted in a stack of nearly 200 communications.

Using this example, we will examine how blockchain has been implemented to create trust and security in the digitized document workflow and improve the efficiency of global supply chains.

Here we can see each distinct entity involved in the transaction: the growers, export authorities, ports, customs, and importers.

Shipping from the port of Mombasa requires signatures from three different agencies approving the export and six documents that describe the origin, chemical treatments, quality of the produce, and customs duties.

Firstly, using a PC or mobile device the Kenyan farm submits a packing list that becomes visible to all participants.

This action initiates a smart contract that enforces an export approval workflow between the three agencies.

As each agency signs, the status is updated for all to see.

Simultaneously, information about the inspection of the flowers, the sealing of the refrigerated container, the pickup by the trucker, and the approval from customs is communicated to the port of Mombasa allowing them to prepare for the container.

All actions relating to the documents and the physical goods are captured and shared: which documents were submitted, when and by whom, where the flowers are, and who is in possession of them, and the next steps in their journey.

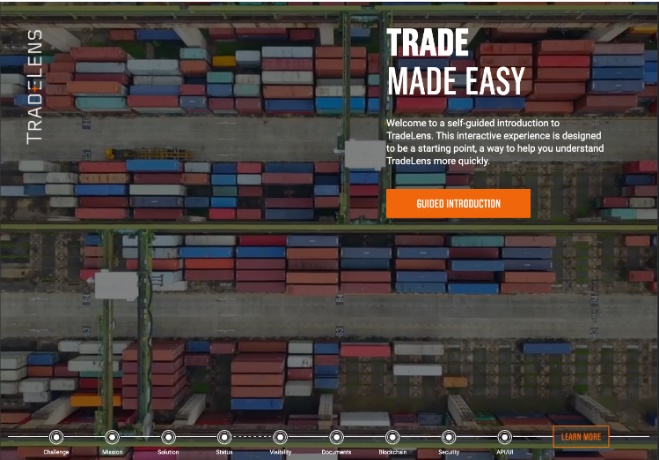
Flowers are perishable, so it's crucial that there are no delays or missed steps .

Blockchain provides secure data exchange and a tamperproof repository for these documents and shipping events.

This system could significantly reduce delays and fraud saving billions of dollars annually.

And, according to the WTO, reducing barriers within the international supply chain could increase worldwide GDP by almost 5% and total trade volume by 15%.

The resulting solution is called [TradeLens](https://www.tradelens.com/). You can take the TradeLens tour [here](https://tour.tradelens.com/).



## Farm to Table

Farms are complicated ecosystems with many moving parts, careful timing, and seasonal financing structures. However, after the food leaves a farm, it becomes part of a wide-reaching supply chain with a lot of parties. Buyers, sellers, distributors, and grocery chains all want to know where the food is along its journey. You also probably want to know where your food has been before you serve it on your dinner table.

The trend toward blockchain agriculture promises to make each step of growing and distributing food simpler. It will offer all parties involved a single source of truth for the agriculture supply chain.



 To learn more, read Hyperledger's case study [*"How Walmart Brought Unprecedented Transparency to the Food Supply Chain with Hyperledger Fabric"*](https://www.hyperledger.org/learn/publications/walmart-case-study).

## Walmart

I purchased a pack of mangos, I came into my staff meeting, I put them on the table, and I said: "Your traceback exercise starts right now".

And we timed how long it took them to get the information for each point in the food system all the way back to the farm.

And I'm not gonna give you the results.

After the pilot, but it's gonna be good.

When a customer shops in our stores, we know they expect great prices, we know they expect fast, clean, and friendly service, but an unspoken expectation is that they expect the products that they buy in our stores to be safe.

You know, when there's a food event or a food scare what you want to do is you want to be fast, but you want to be right.

That food product is guilty until proven innocent.

We at Walmart, will actually pull all the product until we know what is the implicated product and can put then the safe product back out.

And imagine, if we could pinpoint with certainty, within minutes not days, that it was the implicated product.

Walmart and IBM are working to make that a reality.

If you think about the food system, it's pretty complex.

It involves farmers, processors, distributors, and the way traceability is done today, each segment of the food system does it their own way.

Most actually do it on paper or on systems that don't speak to each other, and so you can never have a full view of what's happening in the food system.

What we hope to do with blockchain is bring all food safety system stakeholders and collaborate so that we do it one best way, we can do it very quickly, and efficiently.

Blockchain is a digital ledger that allows different segments of the food system to capture information about the product, what they've done to it, where that product has been.

If we're linking that data with other data points, the Internet of Things, all that information will yield to insights that will allow us to have a safer, more affordable and sustainable food system.

But we don't believe traceability is the goal. We believe that transparency is the ultimate goal.

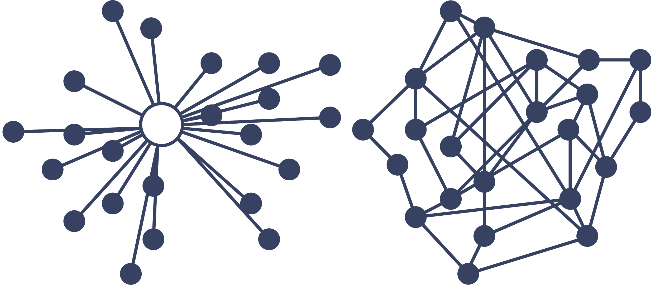
Blockchain will give us the ability to not only track where food came from, but how it was produced, was it produced safely, was it produced responsibly, is it sustainably grown, how many dates of shelf life are left on that product.

The food system is a shared responsibility and for blockchain, and traceability, and transparency to work we need a lot of people working together.

We're excited to be working with IBM on this blockchain initiative, but it's not just Walmart and IBM, we actually have some of our suppliers participating in this pilot, we've got some universities also participating in the pilot.

We'll make sure that all stakeholders work together for a safer and better food system.

* IBM's [Food Trust Solution](https://www.ibm.com/blockchain/industries/supply-chain) building faith in food supply chains.
* Paramount's [Farm to Table](https://www.farmtoplate.io/) creates an inclusive blockchain supply chain solution [from the farm all the way to your plate](https://www.producebluebook.com/2021/05/21/paramount-software-solutions-launches-farm-to-plate-blockchain-platform/).



## Healthcare

Blockchain is transforming the healthcare industry. Some challenges the healthcare industry faces are counterfeit drugs, siloed data, health record management to name a few. Blockchain can solve these issues with interoperability, data integrity and security. Let's look at some solutions.



Moderna uses blockchain to support smart COVID vaccine management. To learn more see [*"Moderna, IBM Explore Blockchain Tech, AI to Support 'Smarter' Management of COVID-19 Vaccines"*](https://www.marketwatch.com/story/moderna-ibm-explore-blockchain-tech-ai-to-support-smarter-management-of-covid-19-vaccines-2021-03-04) article by Tomi Kilgore.



SAP has an existing solution unrelated to blockchain called Advanced Track and Trace for Pharmaceuticals (ATTP) which generates the unique identifiers. To further explore this solution read the following article by Nicky Morris [*"SAP Leads Pharma Supply Chain Blockchain"*](https://www.ledgerinsights.com/sap-pharma-supply-chain/) and watch [*"Verifying Pharmaceutical Products Using Blockchain"*](https://www.sap.com/assetdetail/2018/05/c48ee5c2-047d-0010-87a3-c30de2ffd8ff.html) video.



Also, Pfizer has been using blockchain in transparent [clinical trials](https://www.pfizer.com/science/clinical-trials). You can learn more about this project by reading the following blog post, [*"Clinical Trial Data Should Be Accessible and Transparent"*](https://www.pfizer.com/science/clinical-trials/trial-data-and-results).

## Finance Markets

Reduction of settlement times will improve the flow of money through fintech companies.



Swiss Exchange, [SIX](https://tokenist.com/swiss-exchange-six-to-incorporate-blockchain-and-launch-sto/) has a solution that solves the issue in the trade markets of long settlement times. The new blockchain platform runs parallel to the existing SIX platform, which involves three steps to complete a trade, often over several days. Two of those steps vanish in a blockchain distributed ledger, meaning a transaction can be completed in fractions of a second.

Trade finance is showing promise for blockchain solutions in letter of credits by making available financial mechanisms previously excluded for most people. In a paper from [Andrea Frosinini](https://www.tradefinanceglobal.com/posts/author/andrea-frosinini/), [*"Reshaping Trade Finance: Towards a “New” Letter of Credit"*](https://wiki.hyperledger.org/display/TFSIG/Reshaping+Trade+Finance.+Towards+a+new+Letter+of+Credit?preview=/29035705/29035706/Reshaping%20Trade%20Finance%20(towards%20a%20new%20Letter%20of%20Credit).pdf), he supplied trade finance paired with blockchain that provides delivery and payment assurance to buyers and sellers, reducing operation and transactional cost and opening up market opportunities.

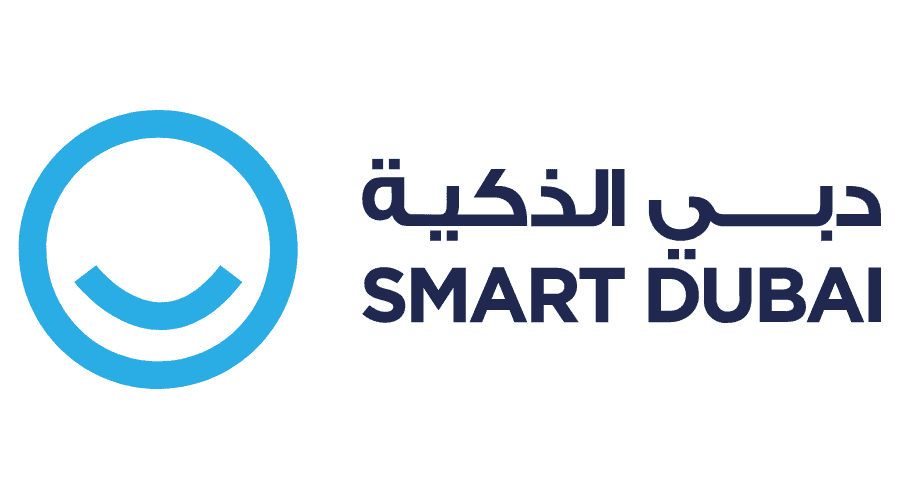


Voltron Trade Finance was co-founded by eight member banks including Bangkok Bank, BNP Paribas, CTBC, HSBC, ING, Natwest, SEB and Standard Chartered. The consortium has since grown to more than 50 banks and corporations. The platform is built on Corda blockchain, it solves the problem that most letters of credit are based on paper and take 5 to 10 days. By using blockchain technology, the letters of credit may be efficiently transacted in less than 24 hours. You can learn more about Voltron from the following two articles ["Blockchain Based Letter of Credit Processed by HSBC on Voltron Trade Finance Platform"](https://www.crowdfundinsider.com/2019/09/151200-blockchain-based-letter-of-credit-processed-by-hsbc-on-voltron-trade-finance-platform/) (by JD Alois) and ["Trade Finance Solution Voltron Launches Open Platform on Corda Blockchain"](https://www.bain.com/about/media-center/press-releases/2018/trade-finance-solution-voltron-launches-open-platform-on-corda-blockchain/).

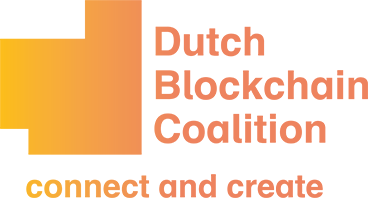
## 6.4 Public Sector Solutions Overview

Blockchain benefits of security, efficiency and speed have government leaders research the far reaching implications that will improve lives and accelerate global blockchain solutions. Public sector can be categorized by, Public Administration, Public Service, Land and Community, and Government. According to a presentation by Bobbi Muscara, Saptarshi Choudhury and Sean O’Kelly, ["Re-thinking Public Sector through Blockchain"](https://www.youtube.com/watch?v=2xtdLefeM14), all blockchain public sector project must consider in the design these four factors:

* Identity management for Governments
* Interactions (highly regulated transactions)
* Regulations
* Governance



One solution that we have already mentioned in Chapter 1 is Smart Dubai. Its goal is to become the happiest city on Earth. Watch these additional resources to learn more about the Smart Dubai initiative, [*"Smart Dubai's Paperless Strategy"*](https://www.smartdubai.ae/initiatives/paperless) and [*"Happy Cities Forum 2019"*](https://www.smartdubai.ae/initiatives/happiness-agenda).



[Dutch Blockchain Coalition](https://dutchblockchaincoalition.org/) established three pillars of society working together to build a blockchain future:

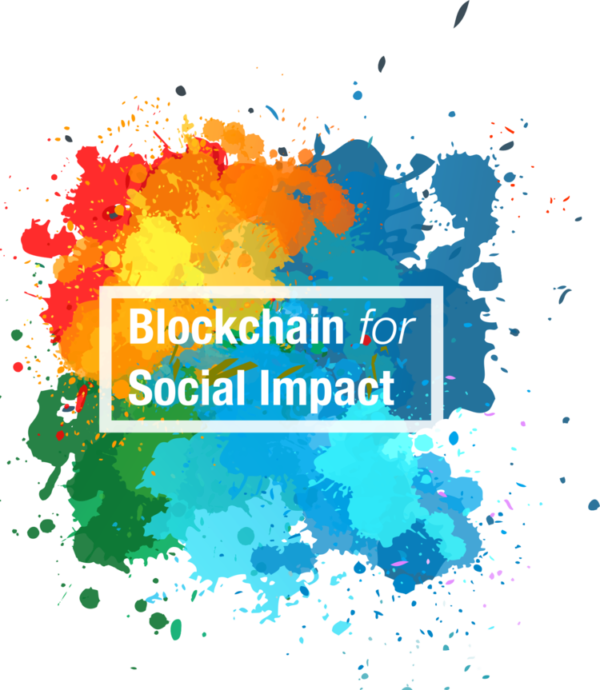
* Developing blockchain building blocks - digital identities
* Realizing the conditions for utilizing blockchain
* Developing and realizing the Human Capital Agenda



Wyoming has now enacted a total of [13 blockchain-enabling laws](https://caitlin-long.com/what-do-wyomings-blockchain-laws-mean/), making it the only US state to provide a comprehensive, welcoming legal framework that enables blockchain technology to flourish, both for individuals and companies. This effort was led by tireless [Caitlin Long](https://caitlin-long.com/).

## 6.5 Social Impact Solutions Overview

The [Blockchain for Social Impact Coalition (BSIC)](https://blockchainforsocialimpact.com/) is a not-for-profit organization that incubates, develops, and collaborates on blockchain products and solutions that can address social and environmental challenges across the United Nations Sustainable Development Goals. The aim is to inspire, federate, and create bridges between NGOs, and government agencies, foundations, impact investors, philanthropists and technologists.

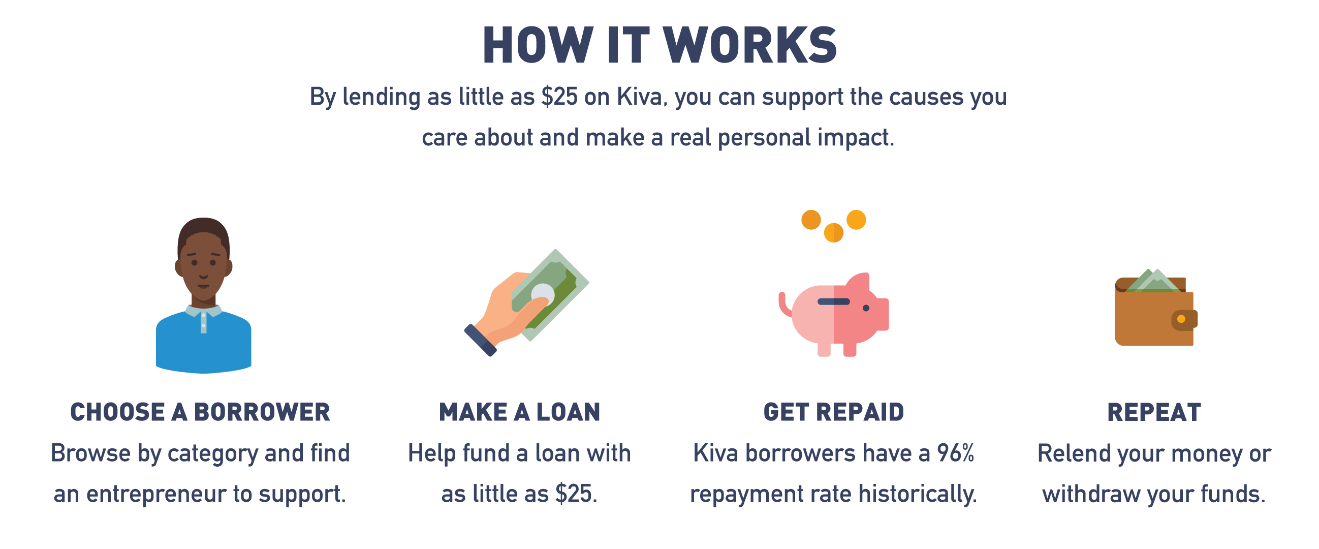


According to the [*"7 Ways Blockchain Can Be Used for Social Good"*](https://innotechtoday.com/blockchain-social-good/) article by Kayla Matthews, areas that are seeing blockchain social impact projects are:

* Philanthropy and remittances
* Financial empowerment
* Identity and land rights
* Governance and democracy
* Supply chain and environmental protections



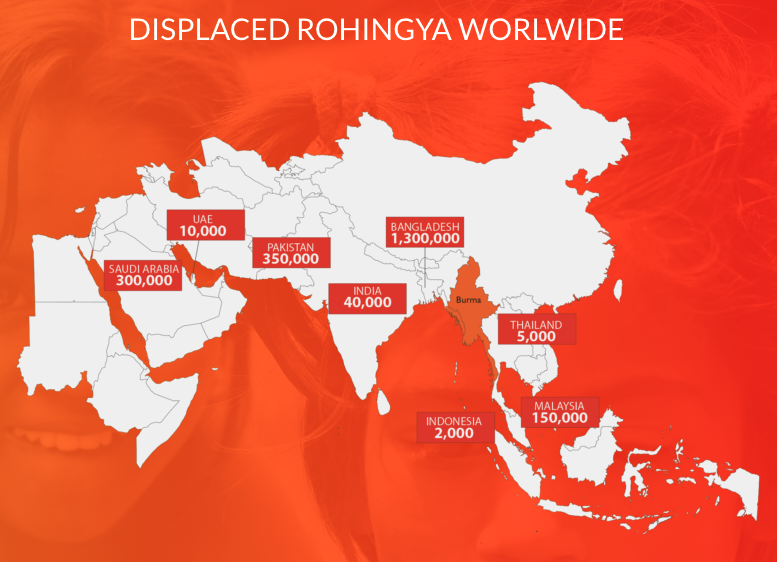
More than 1.7 billion people around the world are unbanked and can’t access the financial services they need. [Kiva](https://www.kiva.org/) is an international nonprofit, founded in 2005 in San Francisco, with a mission to expand financial access to help underserved communities thrive. Kiva accomplishes this by crowdfunding loans and unlocking capital for the underserved, improving the quality and cost of financial services, and addressing the underlying barriers to financial access around the world. Through Kiva's work, students can pay for tuition, women can start businesses, farmers are able to invest in equipment and families can afford needed emergency care.



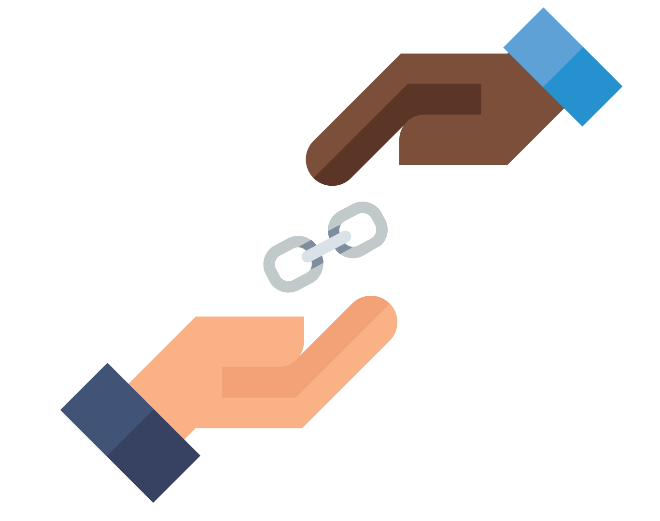
The mission of the [Rohingya Project](https://rohingyaproject.com/) is to create the foundation for a viable future for the stateless Rohingya people by connecting them digitally to opportunities to learn, equip and empower themselves. Through the creation of a Financial and Social Inclusion platform, those Rohingya who for years have been sidelined can be given access to a range of virtual services including online education, digital identity and reward tokens.



The platform will tap into the potential of the Rohingya community and other marginalized people and offer options to counter their exclusion from the mainstream.



The [Giving Chain](https://thegivingchain.org/index.html) is a grassroots Social Impact project designed to improve disaster relief efforts as well as open up new pathways for local charity giving.



Created by three local meetup groups, [Ledger Academy](https://ledgeracademy.com/), [Hyperledger Princeton](https://www.meetup.com/Hyperledger-Princeton/) and [Blockchain & AI Princeton](https://www.meetup.com/Blockchain-Princeton/). The project won the 2021 Government Blockchain Associations Award for Social Impact. The video of the awards ceremony can be viewed on [YouTube](https://www.youtube.com/watch?v=41DYKpLSvrs).



The Giving Chain is now moving from a Proof of Concept project to a prototype as it was selected for the 2021 Hyperledger Mentorship program.

## ConsenSys

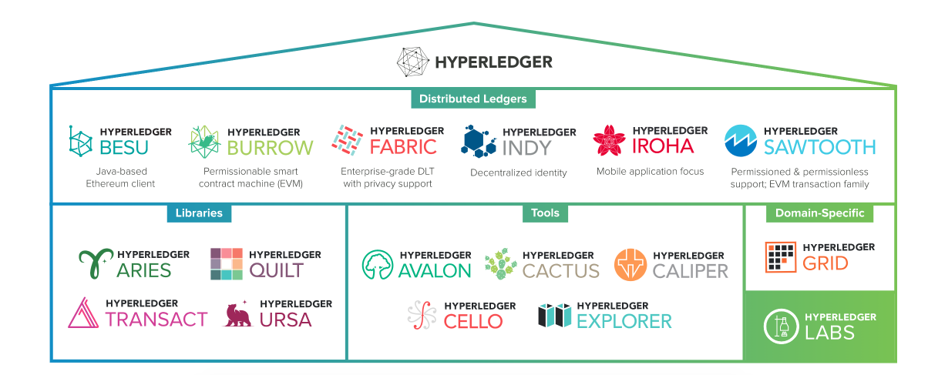
ConsenSys Mesh companies offer solutions to help build out the Ethereum Ecosystem. ConsenSys Mesh acts as an incubator for Ethereum-based projects:

* [Codefi](https://consensys.net/codefi/)  
  Finance and commerce blockchain applications.
* [Diligence](https://consensys.net/diligence/)  
  Ethereum smart contract audits.
* [INFURA](https://media.consensys.net/how-infura-solves-ethereums-other-big-scaling-challenge-b7c4e635121f)  
  Scaling and performance issues.
* [Metamask](https://metamask.io/)  
  Wallet application.
* [Quorum](https://consensys.net/quorum/)  
  open source blockchain platforms.
* [Truffle](https://consensys.net/blog/truffle-suite/)  
  Application builder.

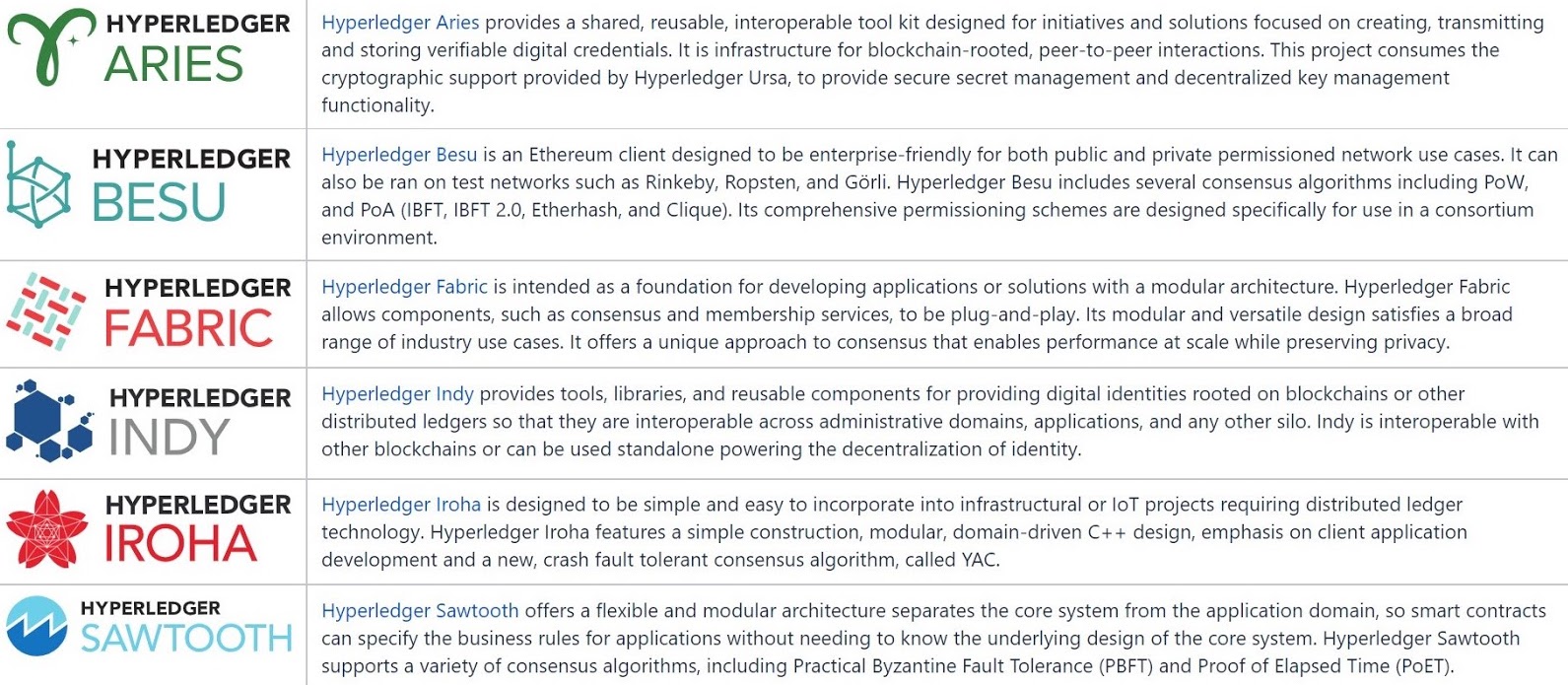


## Hyperledger

[Hyperledger Greenhouse](https://www.hyperledger.org/use) is a graphical representation of the blockchains tools and libraries hosted by the Linux Foundation:



Hyperledger is an open source project with blockchains for you to build your solutions on and tools to support these blockchains. Learn more about Hyperledger [distributed ledgers](https://www.hyperledger.org/use/distributed-ledgers) and [libraries](https://www.hyperledger.org/use/libraries) on the Hyperledger website.



## Daml

[Daml](https://daml.com/) is:

"a development framework for creating systems of record that securely connect across business processes and data boundaries while retaining privacy, guaranteeing data integrity, and enforcing strict authorization. Allowing such systems to cross boundaries — legal, regulatory, organizational, or other — enables them to form seamless economic networks".

* Daml Connect  
  It is a complete development and application stack allowing you to build, integrate, deploy, and maintain full-stack multi-party solutions with a minimum of boilerplate code.
* Daml Drivers  
  They allow you to deploy your application using distributed ledgers, blockchains, or databases. Migrate between ledger drivers without any code changes as business needs evolve.
* Daml Hub  
  It is a cloud service that enables rapid distributed application deployment with an always available, easy-to-use, fully managed cloud environment.



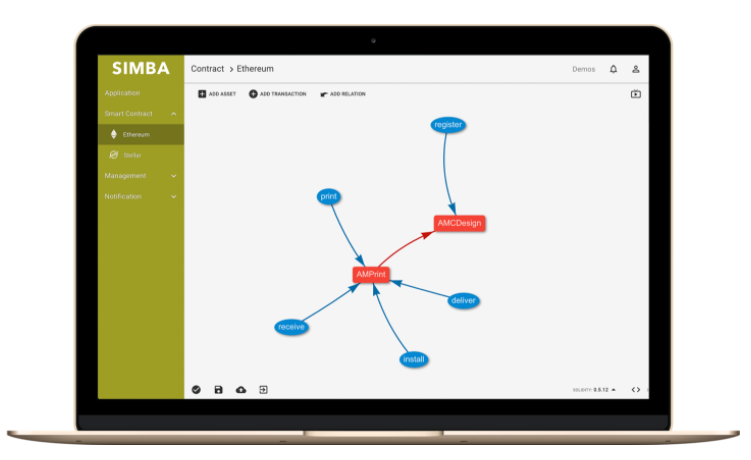
## SIMBA Chain

[SIMBA Chain, Inc.](https://simbachain.com/about/) was formed in 2017 from a grant awarded by the Defense Advanced Research Projects Agency (DARPA) to Indiana Technology and Manufacturing Companies ([ITAMCO](https://itamco.com/)) and the Center for Research Computing ([CRC](https://crc.nd.edu/)) at the University of Notre Dame in order to develop a secure, unhackable messaging and transaction platform for the United States military.

SIMBA Chain is a cloud-based, smart-contract-as-a-service (SCaaS) platform, enabling users across a variety of skill sets to implement dapps (decentralized applications). These apps allow secure, direct connections between users and providers, eliminating third parties. The easy-to-use platform is tailored for users, developers, government, and enterprises to quickly deploy blockchain dapps for their enterprise.



[SIMBA's Smart Contract Designer](https://simbachain.com/solutions/smart-contract-designer/) allows anyone to quickly and easily create smart contracts. The interface allows users to easily build a graph of the relationships between assets and transactions. This graphical model is then converted to Solidity where each asset and transaction becomes a Solidity Smart Contract method that can be executed on the blockchain.



SIMBA Chain also offers management services ([Software as a Service](https://simbachain.com/solutions/smart-contract-as-a-service/)) for your blockchain solution that grant use of software solutions or APIs (application programming interface), across several cloud platforms so companies can effectively create blockchain solutions.

## Identity

Identity management is vital for blockchain operation. Identifying objects that will interact with a blockchain such as people, places, things ([IOT devices](https://www.blockchain-council.org/blockchain/blockchain-and-iot-a-solid-technological-duo/)), is the first step and consideration when developing a blockchain.

One solution is the Verifiable Organizations Network ([VON](https://vonx.io/about/)) project that enables organizations—and the people running those organizations—to conduct business online in a trusted manner. The core challenge is that on the Internet we can’t tell if we’re talking to you, or someone pretending to be you. We need a reliable way to verify that “you are you” in a manner appropriate for the type of transaction that you want to complete and in a privacy-preserving manner.

To learn more, we recommend that you listen the [*"Digital Trust: How the OrgBook Enables the Digital Economy"*](https://bc-von.s3.amazonaws.com/2018-06-VON-Webinar-for-Sovrin-Indy-Community.mp4) webinar.

## Marketplace

Marketplaces exist to shop renewable energies to make sustainable solutions available on open markets. Everyone knows there are countless inefficiencies in the energy grid, stemming from the highly centralized nature of our utilities systems. With the advent of at-home energy production and storage through affordable solar panels and home batteries, many users are storing energy surpluses at home without a way to “sell” clean energy.



[Power Ledger](https://www.powerledger.io/) solution offers a peer-to-peer energy trading platform. It builds global blockchain energy solutions to provide communities access to affordable electricity that is also renewable. By increasing the transparency for energy origins, Power Ledger could assist with providing customers more choices for where their energy comes from. They accomplish these goals through peer-to-peer energy trading, carbon product trading, microgrids management, and more.

## Gaming

The days of video games being just a form of entertainment are long gone. Most of the new video games have in-app purchases and loot box features in them. These features enable users to use real-life currency to buy new skins for their characters and tools. With the use of [DeFi](https://101blockchains.com/defi-use-cases/), game developers can implement the newer incentive or reward models with DeFi coins. In fact, gaming and eSports will likely become one of the major markets as the users are more tech-savvy and open to newer technologies.

To learn more, visit the [Game Developers Conference's website](https://gdconf.com/).

## Decentraland

[Decentraland](https://decentraland.org/) is a virtual world built on top of the Ethereum blockchain. A fully decentralized world where users can interact, build and exchange items, ideas, even enjoy a concert with virtual friends (real life people that they met in Decentraland). Decentraland is run by a DOA, decentralized organization built with smart contracts and dapps (decentralized applications).

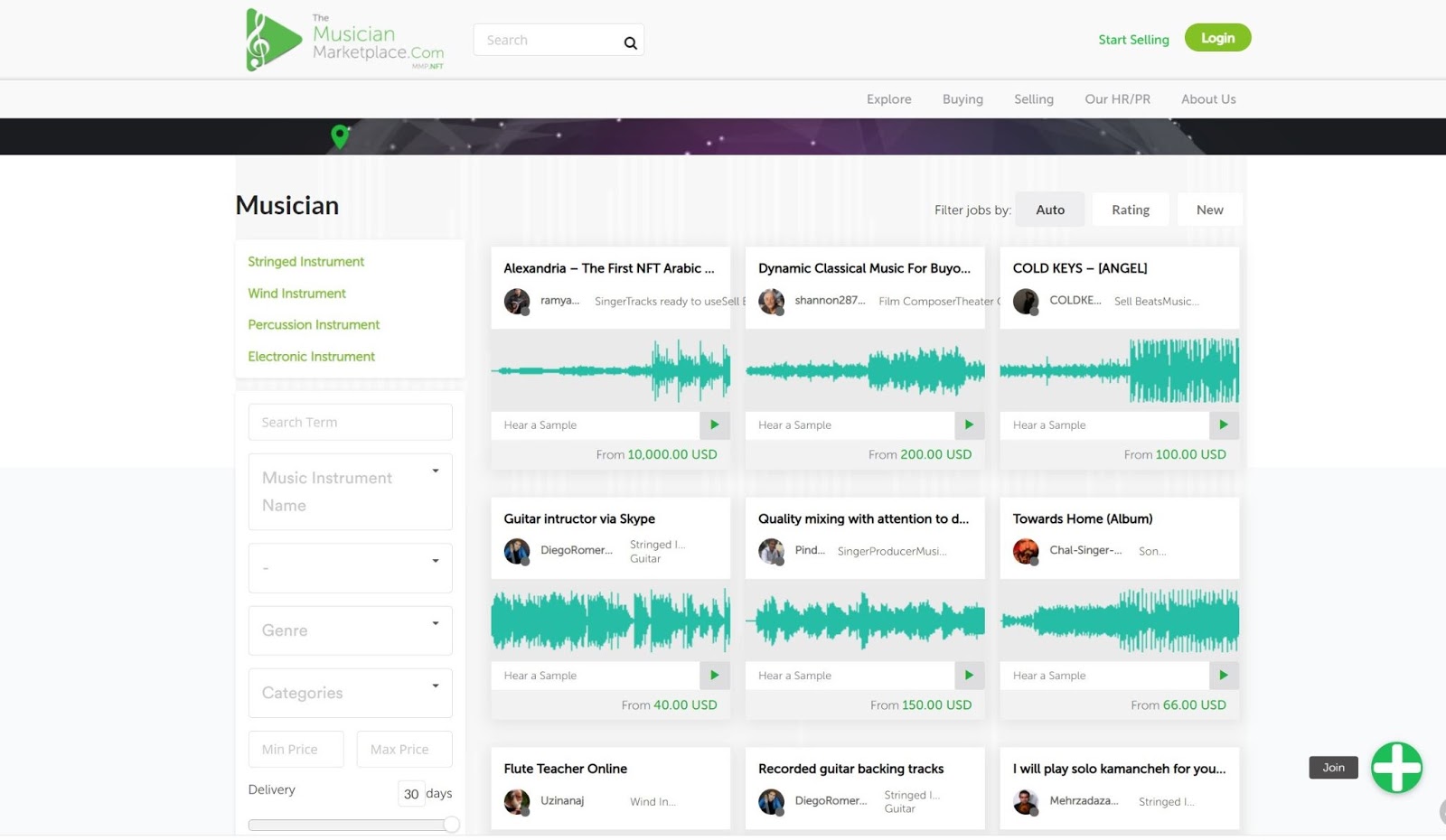
Watch this video to [learn more about Decentraland](https://www.youtube.com/watch?v=qGgYEwJrw0w).

## Music

Experts from [Statista](https://www.statista.com/statistics/239276/growth-of-the-global-music-revenue-by-type/) projected that the music industry will grow from $1.4 billion to $17.2 billion dollars between 2012 and 2021. That’s a lot of dough, and it probably wouldn't all go to deserving parties, until blockchain entered the scene. Now there is a way for artists, producers, and labels to get paid on time, in full with royalties going directly back to the artist.

Read [*"Blockchain for the Music Industry: 9 Possible Use Cases"*](https://www.disruptordaily.com/blockchain-use-cases-music/) by Sam Mire to learn more.

[themusicianmarketplace.com](https://www.themusicianmarketplace.com/) was built to establish one profile for each artist, but each artist can list talents for any job they want. For example, John is a guitar player, a songwriter who is recording songwriting gigs, composes original music, resells his software, and sells his guitar instrument all in one place. The options on themusicianmarketplace.com are unlimited. Below you can see themusicianmarketplace.com dashboard:



## 6.6 What Is the Future of Blockchain?

What is the future of blockchain?

That is a big question.

And unlike everything we have already talked about in this course, this is nothing factual, but just my own opinion.

I think blockchain is a really, really exciting place right now.

Blockchain tends to get talked about in the context of a lot of other exciting emerging technologies, things like IoT and smart devices, self-driving cars and autonomous devices, AI, virtual and augmented reality.

The truth is, in my opinion, I see blockchain as an enabling layer for many of these other technological revolutions.

Everybody is excited about the idea of smart devices.

Wouldn't it be great if I had a smart refrigerator that automatically reordered more ketchup as it started to get low?

Everyone gets a little nervous when it comes time to actually talk about implementing something like this, because how do we protect it?

How do we ensure that the data the system uses is immutable and secure?

Blockchain provides that.

I think that we are going to see a lot of growth in emerging technologies as blockchain continues to emerge, because it's going to make more and more things possible.

And if we talk long term, and again, only my opinion, I think blockchain becomes the enabling layer for a multi-planetary human economy.

You might have seen earlier this year, February 2018, SpaceX put up Falcon Heavy.

Because SpaceX and Elon Musk are committed to getting us to Mars.

And I truly believe in the next 20 to 50 years we are going to see a human colony on Mars.

Now, one interesting thing about Mars is that it's really really far away.

At the closest Earth gets to Mars, it's a 26 minute roundtrip at light speed, and there's two weeks out of every March and year, where Earth and Mars can't communicate because the Sun is right in the middle.

Well, think about this: if you run a small pizza shop on Mars, you close out your register for the day, and you need to deposit funds into your bank account, and that is a bank on Wall Street, New York City, and under the best case scenario, that's a 26-minute roundtrip, you can see how centralized models of the Internet aren't going to scale.

So, if you ask me, I really believe technologies like blockchain and supporting technologies like IPFS are the enabling technologies to allow humans to continue to trade and interact and conduct commerce with each other when we become a multi-planetary society.

And that's why I think there's a ton of potential in blockchain and it's something really exciting, and hopefully, you're all inspired to stay up-to-date with.

## 6.7 Summary

In this chapter, we discussed:

* Blockchain use cases in an enterprise environment.
* Public sector and how blockchain is important in shaping citizens' futures.
* The relevance of blockchain in social impact projects.
* Developing new blockchain platforms emerging as the ecosystem evolves.
* Blockchain and how it will improve human experience.

The end . . .

© 2021 edX Inc. All rights reserved.  
深圳市恒宇博科技有限公司 [粤ICP备17044299号-2](http://www.beian.miit.gov.cn/)