**LFS171x - Linux FoundationX –**



**Introduction to Hyperledger Blockchain Technology**



Welcome to LFS171x: Introduction to Hyperledger Blockchain Technology

LFS171x 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

### Chapter 1. Discovering Blockchain Technologies

#### **Introduction and Learning Objectives**

#### **Distributed Ledger Technology (DLT)**

#### **Bitcoin and Ethereum Blockchains**

#### **Exploring Permissionless Blockchains**

#### **Consensus Algorithms**

#### [**Hyperledger**](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS171x+3T2020/block-v1:LinuxFoundationX+LFS171x+3T2020+type@sequential+block@a24e7d7d6d8b4a7a803d950bcfe9df33)

#### **Other Open Source Permissioned Distributed Ledgers**

#### **Challenges in the Adoption/Deployment of Distributed Ledger Technologies**

### Chapter 2. Introduction to Hyperledger

#### **Introduction and Learning Objectives**

#### [**Hyperledger**](https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS171x+3T2020/block-v1:LinuxFoundationX+LFS171x+3T2020+type@sequential+block@f4538b2b3e9a4a859097247df7a4e80d)

#### **Q/A with Brian Behlendorf, Executive Director of Hyperledger**

### Chapter 3. Hyperledger: Distributed Ledger Frameworks and Domain Specific Blockchains

#### **Introduction and Learning Objectives**

#### **Hyperledger Frameworks**

#### **Hyperledger: Domain-Specific Blockchain Technologies**

### Chapter 4. Hyperledger Tools

#### **Introduction and Learning Objectives**

#### **Hyperledger Tools**

### Chapter 5. Hyperledger Libraries

#### **Introduction and Learning Objectives**

#### **Hyperledger Libraries**

### Chapter 6. The Promise of Business Blockchain Technologies

#### **Introduction and Learning Objectives**

#### **Existing Hyperledger Blockchain Use Cases**

### Chapter 7. What's Next?

**What's Next?**

### About this course

Blockchain technology is changing how businesses operate. With trust built into blockchain solutions, it is important to understand how this new technology is different and how it works in comparison with technologies of the past.

First, we cover the main concepts of what blockchain is and some of its major characteristics.

We take you through the important players in this diverse community.

We discuss how it began, first introduced for the administration of the Bitcoin cryptocurrency, and how it is now applied to all aspects of business including government, banking, supply chains, and other industries.

Next, we analyze the mechanics of blockchains and how they work. We will cover the concept of transparent ledgers, public and permissioned, and focus on using cryptography to achieve consensus, immutability, and transparency.

This is all part of blockchain's ability to provide "trusted data from untrusted sources", disrupting traditional accounting methodologies and international trade.

We will cover some of the functions of blockchain.

You will discover the power of the smart contract, the building blocks for transactions on the blockchain.

You will gain an understanding of the different blockchain structures and how start up decisions influence how your blockchain deals with security, identity, consensus, and governance.

We then dive into the various methods of blockchain governance.

You will understand how different governance models dictate how your blockchain operates, and gain insight into consortiums and how this transformative technology is creating new avenues of communication.

Next, we examine the problems blockchain solves that have been difficult to overcome in the past with more centralized architectures, discovering how blockchain tackles the double spend issue, creates autonomy and transparency while facilitating innovative ways for multiple parties to interact.

You will then discover the new and creative ways blockchain is changing the future.

New insights and models dealing with Identity will be explored.

You will look at trends in Decentralized Finance, NFT (non-fungible tokens),

CBDC (central bank digital currencies) and how the push for interoperability between blockchains is becoming increasingly important.

Finally, we take a deep dive into the various use cases of blockchain, complete with analyzing real examples of how different industries are executing the technology and opening up new avenues for improving their businesses.

## Chapter 1. Discovering Blockchain Technologies

### A Word from Brian Behlendorf, Executive Director at Hyperledger

Hi, I'm Brian Behlendorf. I'm Executive Director of Hyperledger, a collaborative project hosted at the Linux Foundation.

I want to welcome you to the first ever training course for Hyperledger and our related technology projects.

Hyperledger is really the first series of projects focused on enterprise blockchain applications.

And that means using distributed ledger technologies in a permissioned setting, it means using smart contracts to automate various business processes, and it means building a really exciting new world of secure, trustworthy information systems and automation of business processes.

In this course, you'll learn about these different projects.

This course is designed for people on the full spectrum, from working on purely as a software developer, all the way to those who just really want a business level understanding of what these technologies can accomplish, and what are the kinds of use cases that you might apply this to.

This is really designed for the full breadth of those technologies

### Introduction

Chapter 1 introduces the building blocks of distributed ledger technologies, including blockchains.

It lays the foundation for an in-depth understanding of the content that follows in the course.

You should engage with the content in this chapter both to learn, as well as brush up your blockchain knowledge.

### Learning Objectives

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

* Explain the concepts of blockchain and distributed ledger technologies (DLT).
* Explore permissioned and permissionless blockchains and their key characteristics.
* Discuss various components of distributed ledger technologies, including consensus algorithms and smart contracts.
* Provide a high-level explanation of what Hyperledger is.

### Distributed Ledger Technology (DLT)

### Background - The Rising Interest in Distributed Ledger Technologies

Looking back to the last half century of computer technologies and architectures, you may observe a trend of fluctuation between the centralization and subsequent decentralization of computing power, storage, infrastructure, protocols, and code.

Mainframe computers are largely centralized.

They typically house all computing power, memory, data storage, and code. Access to mainframes is mainly by "dumb terminals", which only take inputs and outputs, and do not store or process data.

With the advent of personal computers and private networks, similar computational capabilities were now housed both on the clients, as well as the servers.

This, in part, gave rise to the "client-server" architecture, which supported the development of relational database systems. Massive data sets, which are housed on mainframes, could move onto a distributed architecture.

This data could replicate from server to server, and subsets of the data could be accessed and processed on clients, and then, synced back to the server.

Over time, Internet and cloud computing architectures enabled global access from a variety of computing devices; whereas mainframes were largely designed to address the needs of large corporations and governments.

Even though this "cloud architecture" is decentralized in terms of hardware, it has given rise to application-level centralization (e.g. Facebook, Twitter, Google, etc.).

Currently, we are witnessing the transition from centralized computing, storage, and processing to decentralized architectures and systems.

According to [Muneeb Ali](https://medium.com/@muneeb/the-next-wave-of-computing-743295b4bc73" \t "_blank), these systems aim to

"give explicit control of digital assets to end-users and remove the need to trust any third-party servers and infrastructure".

Distributed ledger technology is one of the key innovations making this shift possible.

A distributed ledger is a type of data structure which resides across multiple computer devices, generally spread across locations or regions.

Distributed ledger technology (DLT) includes blockchain technologies and smart contracts.

While distributed ledgers existed prior to Bitcoin, the Bitcoin blockchain marks the convergence of a host of technologies, including timestamping of transactions, Peer-to-Peer (P2P) networks, cryptography, and shared computational power, along with a new consensus algorithm.

In summary, distributed ledger technology generally consists of **three** basic components:

* A data model that captures the current state of the ledger
* A language of transactions that changes the ledger state
* A protocol used to build consensus among participants around which transactions will be accepted, and in what order, by the ledger.

### Blockchain

According to [hyperledger.org](https://hyperledger.org/about),

"A blockchain is a peer-to-peer distributed ledger forged by consensus, combined with a system for "smart contracts" and other assistive technologies. Together these can be used to build a new generation of transactional applications that establishes trust, accountability, and transparency at their core, while streamlining business processes and legal constraints."

Smart contracts are simply computer programs that execute predefined actions when certain conditions within the system are met.

Consensus refers to a system of ensuring that parties agree to a certain state of the system as the true state.

Blockchain is a specific form or subset of distributed ledger technologies (DLTs), which constructs a chronological chain of blocks, hence the name "block-chain".

Examples of other DLTs are Chain Core, Corda, Quorum, and IOTA. They will be covered later in this chapter.

A block refers to a set of transactions that are bundled together and added to the chain at the same time.

Timestamping is another key feature of blockchain technology. Each block is timestamped, with each new block referring to the previous block. Combined with cryptographic hashes, this timestamped chain of blocks provides an immutable record of all transactions in the network, from the very first (or genesis) block.

In the Bitcoin blockchain, the miner nodes bundle unconfirmed and valid transactions into a block. Each block contains a given number of transactions. In the Bitcoin network, miners must solve a cryptographic challenge to propose the next block. This process is known as "proof of work", and requires significant computing power. We shall discuss proof of work in more detail in the Consensus Algorithms section. For more information about blockchain technology, please read the following article: "[*A Brief History of Blockchain*](https://hbr.org/2017/02/a-brief-history-of-blockchain)" by Vinay Gupta.

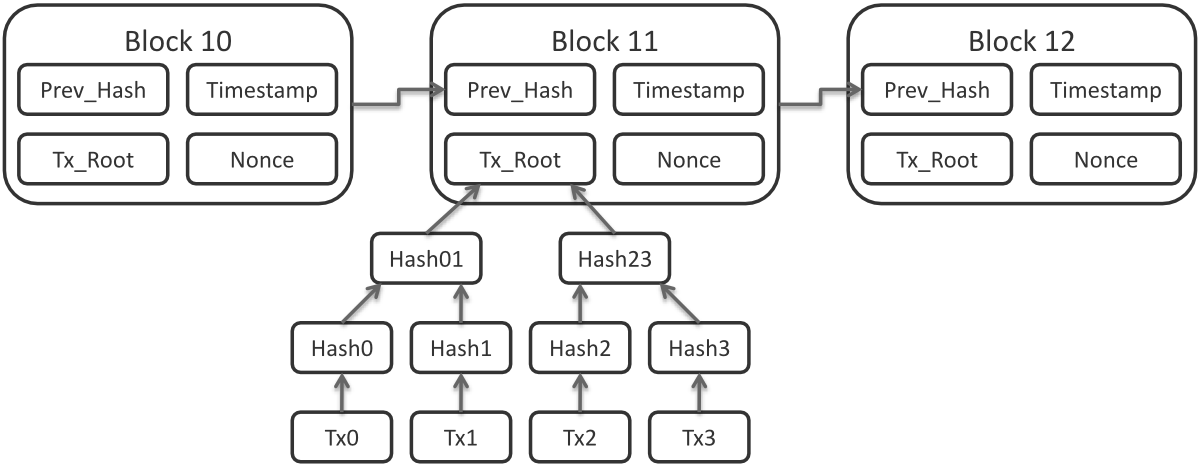
A Bitcoin block consists of **four** pieces of metadata:

* The ***reference*** to the previous block
* The ***proof of work***, also known as a **nonce**
* The **timestamp**
* The ***Merkle tree root*** for the transactions included in this block (Merkle tree is explained next).

### Merkle Tree

The Merkle tree, also known as a binary hash tree, is a data structure that is used to store hashes of the individual data in large datasets in a way to make the verification of the dataset efficient. It is an anti-tamper mechanism to ensure that the large dataset has not been changed. The word "tree" is used to refer to a branching data structure in computer science, as seen in the image below. According to Andreas M. Antonopoulos, in the Bitcoin protocol,

"Merkle trees are used to summarize all the transactions in a block, producing an overall digital fingerprint of the entire set of transactions, providing a very efficient process to verify whether a transaction is included in a block".



**Bitcoin Block Data**  
(licensed under [Creative Commons](https://en.wikipedia.org/wiki/Creative_Commons) [Attribution-Share-Alike 3.0 Unported](https://creativecommons.org/licenses/by-sa/3.0/deed.en), retrieved from [Wikipedia](https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.png))

### What is a Blockchain?

What is blockchain?

As the Security Maven at Hyperledger, I have somewhat of a different perspective on what a blockchain is.

I'm a developer, primarily, and I look at the world in an adversarial way.

It's usually my software versus the world kind of thing.

Blockchains, to me, definitely open up the world of possibilities for solving problems that have plagued us for many years.

It breaks down to being able to create distributed consensus between mutually distrustful parties, in many ways.

It also allows us to create an instantaneous single source of truth.

In the past, we've always had problems with trying to figure out what really happened over the course of a day.

Banks reconcile their books, inventory systems clear sales and deliveries...

With blockchains, we're recording things in real time, and it provides us with sort of an up-to-date accounting of the state of the world.

A lot of these old systems are going away, a lot of the work load management systems are going away. We're not doing batch processing at night anymore.

Instead, we're doing validation in real time, and we always know the state of the world.

This opens up a whole new host of applications that can be based around...

If we knew exactly where every bolt was, could we make sure that there are always bolts at the place where they're going to be installed two minutes before they are needed... things like that...

Like lean manufacturing is one case...

But, it also applies to every other process in the world where we have to track materials and effort, and money, things like that.

Let me think...

The blockchain, for me, actually is just sort of rethinking of our existing business processes around how we can be more effective when we know the state of the world as it is right now, and we know it in two minutes, and we know it in two hours, rather than having to wait until the end of the day for everything to be reconciled.

This is actually a transition from human scale to computer scale.

This was... all of these processes were done on a daily basis, and things like that, and with blockchain, we're now... we're doing it instantaneous, because computers have made it that way.

From a security perspective, blockchains are not a silver bullet.

They're not going to replace the existing business logic.

They're more of a log-based system, so recording what has happened, as it is happening, rather than being the source of what to do with money from a customer, and things like that.

It's not business process type of software.

Because it is a log, and because it is the source of truth, and because a lot of other business logic will be based upon it, the security concerns on it, related to blockchain, are roughly the same as existing business practices, or business logic.

You have to think of all the members of a distributed ledger as participating in a closed network, because that's what they are, at least in permissioned networks, we're not operating on the public Internet, we're not operating in a trustless environment.

It's the exact opposite. We... all the participants in the distributed ledger are known, they're permissioned, that's where that term comes from, and they all participate as if they are in a private network.

When deploying blockchain software, it's typically done behind a firewall, and, anytime you have multiple organizations participating in the distributed ledger, we will use tunneling technology and other VPN firewall tricks to make a virtual LAN exist, so that all of their organizations can talk over it.

Different Hyperledger projects have different trade-offs.

Fabric, for instance, has a more centralized ordering service, and so, it makes more sense to organize one of those networks into a hub-and-spoke model, where each peer connects to the ordering service, which is run either on one of the nodes, or on a neutral third party, and all of the gossip messages that do the consensus mechanism go through a central hub.

Now, that sounds counterintuitive because just distributed ledgers are supposed to be distributed...

They still are, they're distributed in the sense that the blockchain itself is replicated amongst all of the nodes, and so, your data is much more resilient to disruption... resilient against disruption.

The coordination can still be done in a fairly centralized manner.

With Sawtooth, it is not so much the case, right?

The organization of the network for Sawtooth is probably more of like a star model, where you pick some subset of nodes, and your node connects to those and, as long as all nodes are fairly well connected, they can all eventually talk to each other, either one hop, or two hops, or three hops away, depending on the size of your network.

With Iroha, they... their topology is a lot different than the others, because they designed their distributed ledger to function well in a mobile environment, where a lot of the clients are intermittently connected.

They're mobile phones that can be connected and disconnected at random.

Their structure is more of a layered network, where the end clients' mobile phones submit transactions to servers, which then, amongst the servers, do the distributed ledger.

And there's no right answer, right?

The business process dictates which one you choose, but the security is pretty much the same in all of these.

We use cryptography and digital signatures to validate all the messages.

Tampering with messages is essentially impossible.

The immutability of the distributed ledger is guaranteed by the cryptography, but the nature of the trusted network, of the permissioned network, means that we have to treat it like any other back-office service.

You want to deploy it behind a firewall, you want to use tunneling to connect between nodes across the Internet, and you want to maintain it, just like any other service that deals with Internet traffic...you have firewalls, and load balancers, and things like that.

That's all I've got to say about security. And thanks for taking our course.

### Transactions

The record of an event, cryptographically secured with a digital signature, that is verified, ordered, and bundled together into blocks, form the transactions in the blockchain.

In the Bitcoin blockchain, transactions involve the transfer of bitcoins, while in other blockchains, transactions may involve the transfer of any asset or a record of some service being rendered.

Furthermore, a smart contract within the blockchain may allow automatic execution of transactions upon meeting predefined criteria.

Cryptography has a key role to play both in the security, as well as in the immutability of the transactions recorded on blockchains.

Cryptography is the study of the techniques used to allow secure communication between different parties and to ensure the authenticity and immutability of the data being communicated.

For blockchain technologies, cryptography is used to prove that a transaction was created by the right person. It is also used to link transactions into a block in a tamper-proof way, as well as create the links between blocks, to form a blockchain.

### Differences Between Blockchains & Databases

Blockchain technology has some key differentiators from databases.

A blockchain is a write-only data structure, where new entries get appended onto the end of the ledger.

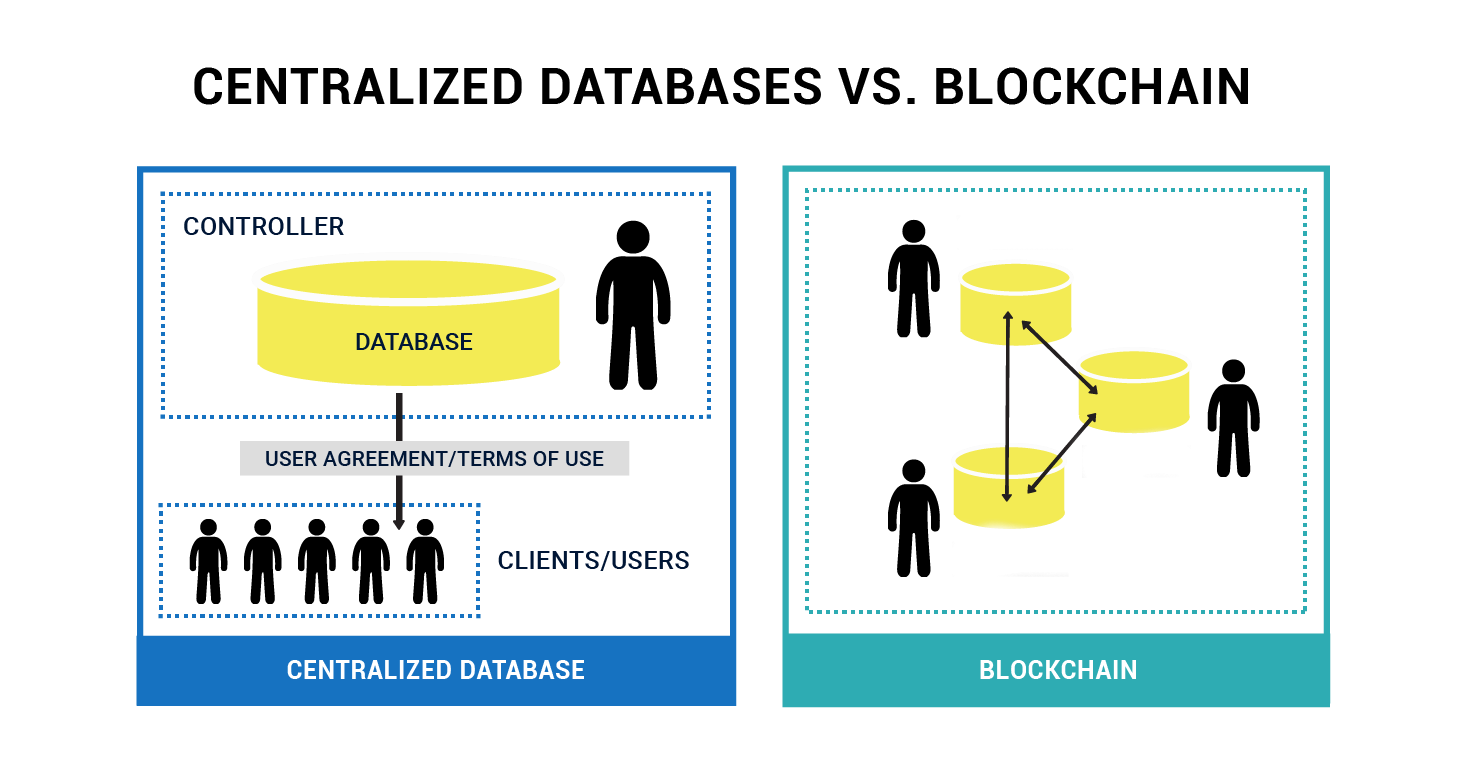
Every new block gets appended to the blockchain by linking to the previous block's "hash" (you can check the *Glossary* tab for a refresher on hash functions).

There are no administrator permissions within a blockchain that allow editing or deleting of data.

In a relational database, data can be easily modified or deleted.

Typically, there are database administrators who may make changes to any part of the data and/or its structure.

Additionally, blockchains were designed for decentralized applications, whereas relational databases, in general, were originally designed for centralized applications, where a single entity controls the data.

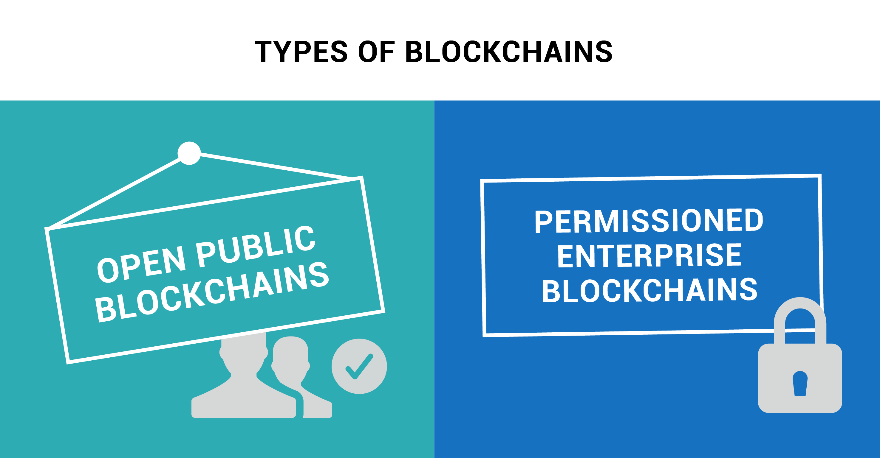


### Types of Blockchains

A blockchain can be both permissionless (like Bitcoin or Ethereum) or permissioned (like the different Hyperledger blockchain frameworks).

A permissionless blockchain is also known as a public blockchain, because anyone can join the network.

A permissioned blockchain, or private blockchain, requires pre-verification of the participating parties within the network, and these parties are usually known to each other.



The choice between permissionless versus permissioned blockchains should be driven by the particular application at hand (or use case).

Most enterprise use cases involve extensive vetting before parties agree to do business with each other.

An example where a number of businesses exchange information is supply chain management.

The supply chain management is an ideal use case for permissioned blockchains. You would only want trusted parties participating in the network.

Each participant that is involved in the supply chain would require permissions to execute transactions on the blockchain.

These transactions would allow other companies to understand where in the supply chain a particular item is.

On the contrary, when a network can "commoditize" trust, facilitating parties to transact without necessarily having to verify each other's identity, like the Bitcoin blockchain, a permissionless blockchain is more suitable.

Many of these instances involve the sale or distribution to the public.

Cryptocurrencies and Initial Coin Offerings (which are not backed by national governments) usually involve implementations of permissionless blockchains.

You will learn about a variety of use cases in Chapter 6, "*The Promise of Business Blockchain Technologies"*.

### Peer-to-Peer Network Architecture

Historically, most applications utilize a central server (or servers).

For one user/client to send a message to another user/client in the network, the request has to be sent to the hub or a central server, which then directs it to the right computer.

Peer-to-peer (P2P) networks were first made popular by Napster (and later BitTorrent) and consist of computer systems which are directly connected to each other via the Internet, without a central server.

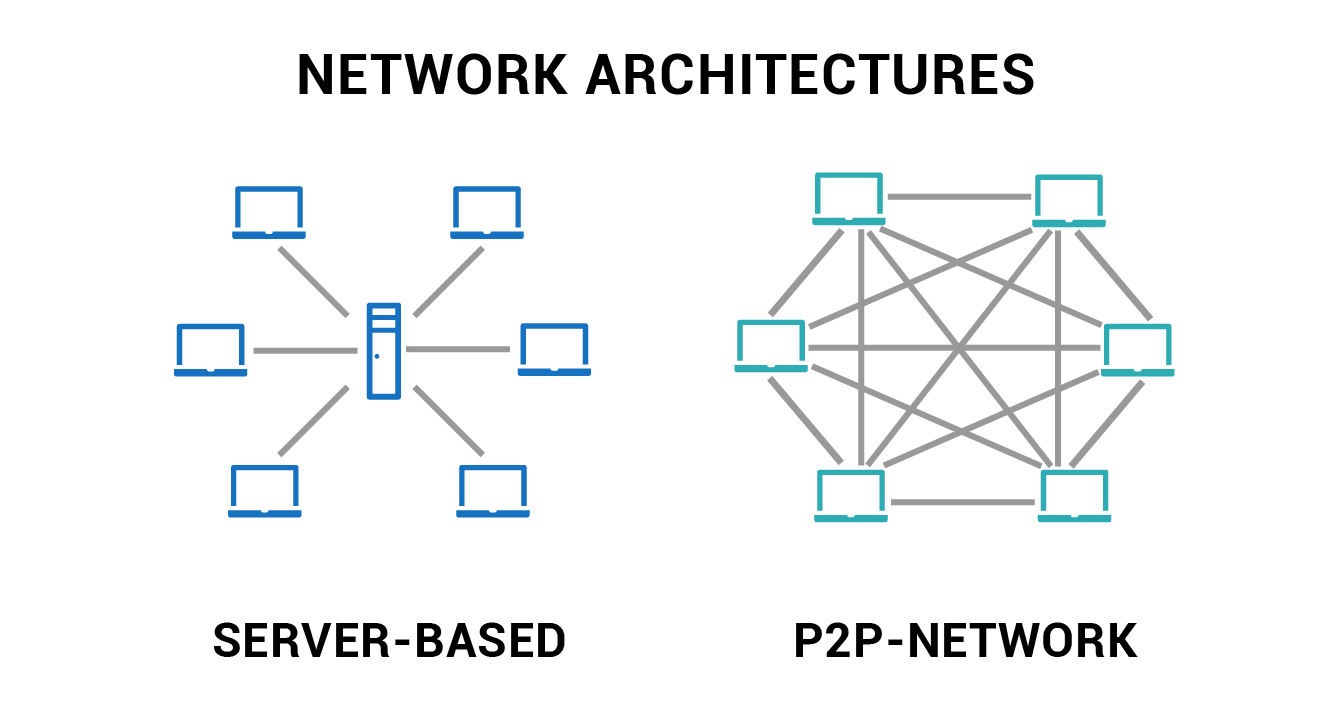
Peers contribute to the computing power and storage that is required for the upkeep of the network.

P2P networks are generally considered to be more secure than centralized networks, as they do not have a single point of attack, as in the case of a server-based network, where the security of the entire network can be compromised if the central server is successfully attacked. [*The Global Risks Report 2018*](https://www.weforum.org/reports/the-global-risks-report-2018), created by the World Economic Forum, reveals a grim picture: cyberattacks are on the rise at an alarming rate, and financial costs related to them are skyrocketing, with more than 25% increase year-over-year. It is estimated that cybercrime will cost businesses more than $8 trillion over the next five years.

And the damages go far beyond financial costs: they affect critical, strategic infrastructure, such as telecommunications providers, energy companies, government agencies, banks, hospitals, and much more.

As a result, large corporations and federal governments invest significant amounts of financial resources to fortify their central servers.

Permissionless P2P systems do not require a set amount of peers to be online and are generally slower. Permissioned P2P networks have to guarantee uptime and require a high level of quality of service on the communication links.



### Peer-to-Peer Networks (Robert Schwentker)

What is a Peer-to-Peer network, and how do peers come to agreement about what is on the blockchain?

A blockchain network is a group of computers that informally are organized in a Peer-to-Peer architecture.

Consensus is a process whereby the peers synchronize the data on the blockchain.

There are a number of consensus mechanisms or algorithms.

One is Proof of Work.

Another is Proof of Stake.

There's also Proof of Elapsed Time, as well as Simplified Byzantine Fault Tolerance.

Bitcoin uses Proof of Work, while Ethereum uses Proof of Work currently, but is moving towards Proof of Stake.

The Hyperledger Sawtooth uses Proof of Elapsed Time.

### Immutability of Data

The immutability of the data which sits on the blockchain is perhaps the most powerful and convincing reason to deploy blockchain-based solutions for a variety of socio-economic processes which are currently recorded on centralized servers.

This immutability, or "unchanging over time" feature makes the blockchain useful for accounting, financial transactions, identity management, and asset ownership, management and transfer, just to name a few examples.

Once a transaction is written onto the blockchain, no one can change it, or, at least, it would be extremely difficult to change it.

According to [Antony Lewis](https://www.linkedin.com/pulse/gentle-introduction-immutability-blockchains-antony-lewis/), the Director of Research at R3,

"When people say that blockchains are immutable, they don't mean that the data can't be changed, they mean it is extremely hard to change without collusion, and if you try, it's extremely easy to detect the attempt".

Let's dig into this statement a bit further. It is extremely hard to change the transactions in a blockchain, because each block is linked to the previous block by including the previous block's hash.

This hash includes the Merkle root hash of all the transactions in the previous block.

If a single transaction were to change, not only would the Merkle root hash change, but so too would the hash contained in the changed block.

In addition, each subsequent block would need to be updated to reflect this change.

In the case of proof of work, the amount of energy required to recalculate the nonce for this block and each subsequent block would be prohibitive.

On the other hand, if someone did modify a transaction in a block without going through the necessary steps to update the subsequent blocks, it would be easy to recalculate the hashes used in the blocks and determine that something is amiss.

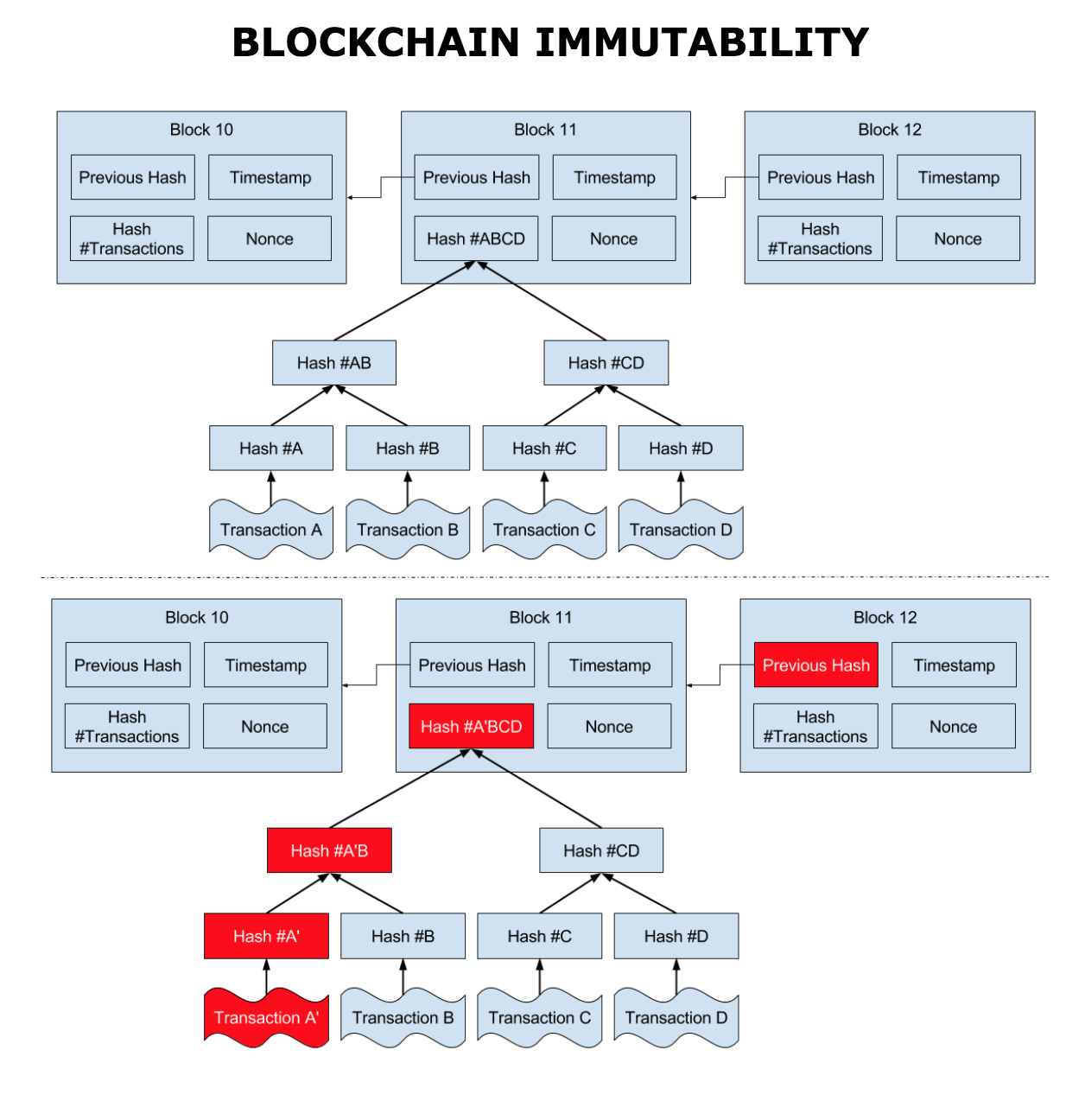
Let's look at an example of how this works. In the following diagram, we see the original blocks and the transactions for Block 11.

Specifically, we see that the Merkle root for the transactions in Block 11 is **Hash #ABCD**, which is the combined hash for the four transactions in this block.

Now, let's say that someone comes in and attempts to change Transaction A to Transaction A'.

This, in turn, modifies the hashes that are stored in the Merkle tree, and the Merkle root changes to **Hash #A'BCD**.

In addition, the Previous Block hash stored in Block 12 also needs to be modified to reflect the overall change in the hash for Block 11.



### Blockchain Applications

Since blockchain is a form of digital infrastructure, applications built on top of a blockchain provide a gateway to accessing information that sits on that blockchain.

In other words, clients/users interact with the blockchain through applications.

Starting from the simple wallets that hold bitcoins, sophisticated applications which encompass applications addressing digital identity (e.g. UPort, KYC-Chain, Netki, etc.), and complex financial transactions are being built on the blockchain.

A more exhaustive list of companies using blockchain technology for identity management and authentication can be found in the following article: "[*21 Companies Leveraging Blockchain for Identity Management and Authentication*](https://gomedici.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/)" by Elena Mesropyan.

For more details about blockchain applications, you can refer to Daniel Palmer's article entitled "[*7 Cool Decentralized Apps Being Built on Ethereum*](https://www.coindesk.com/7-cool-decentralized-apps-built-ethereum/)".

### Smart Contracts

What is a smart contract?

Back in 1996, a man named Nick Szabo coined the term 'smart contract'.

You can think of them as computer protocols used to facilitate, verify, or enforce the negotiation of a legal contract.

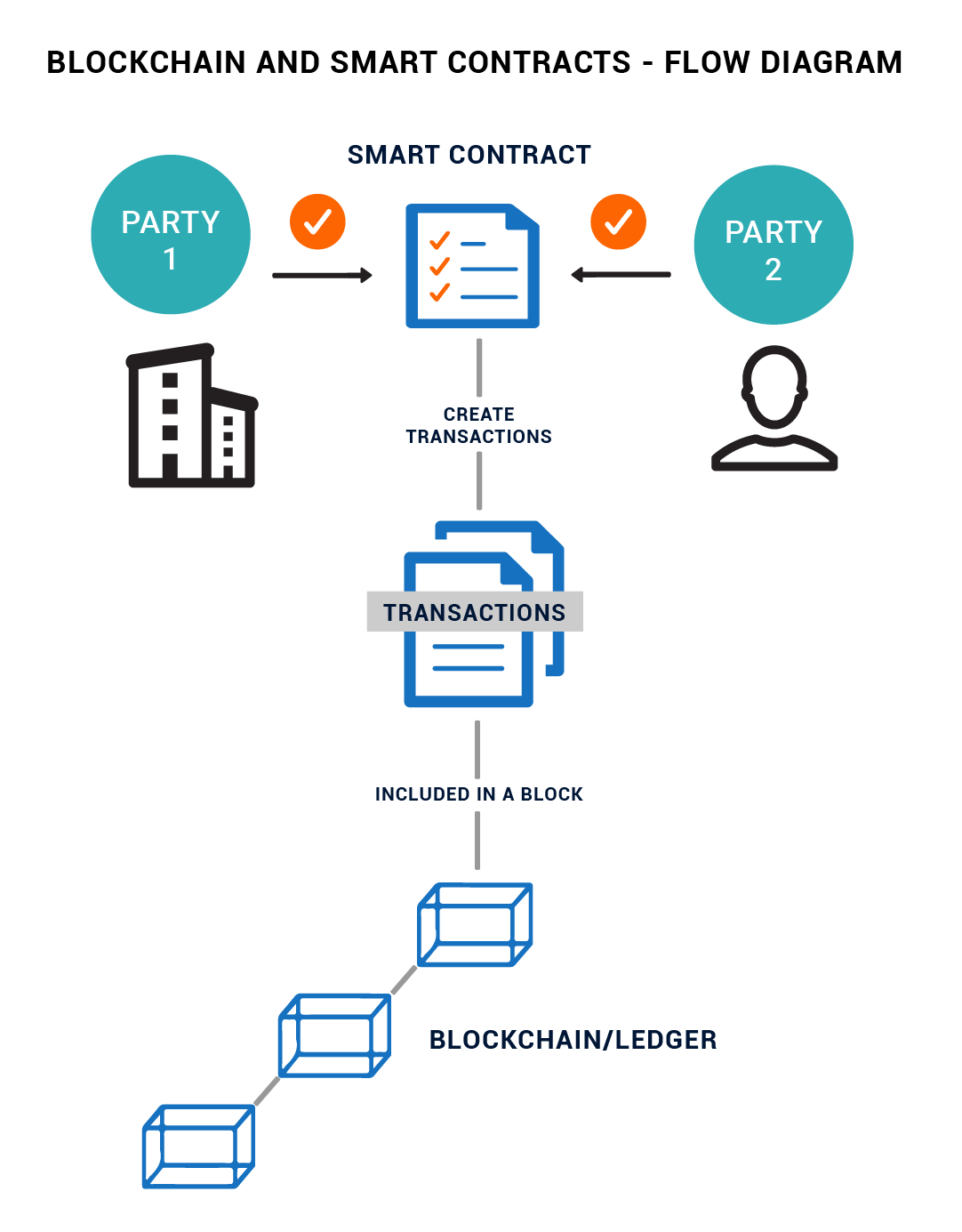
A smart contract is a phrase to describe computer code.

Today, Ethereum smart contracts are designed to run on all nodes of the Ethereum network.

Those smart contracts facilitate the exchange of value, including money, content, property, or shares between a fixed number of parties.

Smart contracts are simply computer programs that execute predefined actions when certain conditions within the system are met.

Smart contracts provide the language of transactions that allow the ledger state to be modified. They can facilitate the exchange and transfer of anything of value (e.g. shares, money, content, property).



### Bitcoin – A Popular Blockchain Deployment

With the invention of the peer-to-peer (P2P) cash system known as Bitcoin in 2008, we have an example of a global decentralized payment network with a distributed and publicly-owned infrastructure, operating as a "permissionless" system.

There is a persuasive case that Bitcoin is the first "killer application" of decentralized computing. One can send and receive bitcoins anywhere in the world in a completely P2P manner, without having to intermediate through a trusted third party, such as a bank.

According to the [Coin Market Capitalizations website](https://coinmarketcap.com/currencies/bitcoin/), as of November 2020, bitcoin's market capitalization (market cap) was over $286 billion.



**Bitcoin Charts**   
(Source: <https://coinmarketcap.com/currencies/bitcoin/>)

According to [AngelList](https://angel.co/blockchains), over five thousand startups have been created to leverage Bitcoin and blockchain-related technologies since the inception of the Bitcoin payment system.

Hundreds of large companies, and dozens of governments and universities have become actively involved in researching, testing, and prototyping blockchain protocols, platforms, and applications.

In particular, the financial services sector has been actively investing in exploring wider applications of distributed ledger technologies (of which, blockchain is a subset) since late 2015.

### Bitcoin & Ethereum

Why were Bitcoin and Ethereum created? What problems do they solve?

Bitcoin was first launched in January of 2009, as a response to the global financial crisis at the time.

Part of the motivation for the system was to be able to transfer value over the internet, without an intermediary.

One of the biggest inventions and problems that it solved was that of the 'double spend' problem.

Bitcoin, in fact, is programmable money.

Ethereum, on the other hand, was created as a response to Bitcoin.

While Bitcoin is focused upon transferring monetary value between parties, it has a very limited programming language.

Ethereum, on the other hand, uses a more expansive set of programming languages and tools to allow for many other types of programs and applications.

The core invention of Ethereum is it's EVM, or Ethereum Virtual Machine.

The EVM runs on the Ethereum network, and it runs a Turing-complete software.

Vitalik Buterin is the person who wrote the white paper for Ethereum.

Some of its key features include the immutability of data, that unauthorized users cannot make changes to that data, the Ethereum development platform is designed to make corruption and tamper proof applications, the secure apps are sent decentralized and secured with cryptography, and they're protected against hacking attacks and fraudulent activities, and lastly, it's designed with zero downtime.

That is because the applications on the network are decentralized, and on many, many machines, if some of those machines go down, the Ethereum network maintains a stable state of the Ethereum network.

### Bitcoin and Cryptoeconomics

Bitcoin has also ushered in tremendous academic and research interest in the area of Cryptoeconomics and Cryptoeconomic security.

According to [Vitalik Buterin](https://www.youtube.com/watch?v=pKqdjaH1dRo),

"Cryptoeconomics is about building systems that have certain desired properties using cryptography to prove properties about messages that happened in the past while using economic incentives defined inside the system to encourage desired properties to hold into the future".

In other words, the field of Cryptoeconomics explores the intersection of cryptography and economic incentives. While cryptography is used for ensuring network security at various levels and functions, the built-in economic incentives provided to the participating nodes in the network ensures that, at any given point, the majority of players in the network operate in a desirable way.

Rather than imposing barriers to entry, permissionless blockchains are public and open for anyone to join.

Since such networks can reasonably expect all kind of agents - including malicious actors - the key lies in incentivizing good behavior in a critical majority of the network, such that:

* The malicious actors cannot take over the network through an escalated attack.
* The malicious actors cannot collude to undertake an organized majority attack on the network.
* The payoffs of securing the network are consistently higher than the cost of attacking the network.
* The cost of attacking the network is prohibitively high.

You can find more about Cryptoeceonomics read "[The Blockchain Economy: A Beginner’s Guide to Institutional Cryptoeconomics](https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4)".

### Ethereum – An Alternative to Bitcoin

According to [Ethereum's official documentation](http://ethdocs.org/en/latest/introduction/what-is-ethereum.html),

"Ethereum is an open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology".

The Ethereum blockchain platform facilitates scripting functionality, or "smart contracts", which are run through the nodes in the network.

As a result, unlike the Bitcoin blockchain, it does not just track transactions, it also programs them. Technically, Ethereum is a Turing-complete virtual machine with its native cryptocurrency called "ether".

The platform was proposed in 2013 in a white paper by the then 19-year old Vitalik Buterin.

As of November 2020, Ethereum had a [market cap](https://coinmarketcap.com/currencies/ethereum/) of over $49 billion, making Ether the second most valuable cryptocurrency after Bitcoin.



**Ether Historical Market Capitalization Chart**  
(Source: <https://etherscan.io/chart/marketcap>)

As the second best known public blockchain after the Bitcoin blockchain, Ethereum has ushered in an era of unprecedented activity around blockchain and distributed ledger technology.

### Ethereum

Can you give another example of a production blockchain system, such as Ethereum, and how is it different from Bitcoin?

Sure. Ehereum also has a public blockchain. It also groups and orders transactions into blocks.

However, Ethereum may be defined as an open source platform that enables developers to build and deploy both smart contracts and decentralized applications, also known as Dapps.

In addition to the Ethereum public blockchain, there are numerous versions of Ethereum which are designed to be private and are permissioned.

### Dapps

As [Stephan Tual](https://www.youtube.com/watch?v=Clw-qf1sUZg) explains, Ethereum applications do not have a middleman; instead, users interact in a P2P fashion with other users through a variety of interfaces - social, financial, gaming, etc.

Since the applications are developed on the decentralized consensus-based network itself, third-party censorship is virtually impossible.

Malicious actors cannot secretly tamper with the application by changing the code and compromise all application users (or nodes that are actively interacting with it).

These Decentralized Applications have come to be known as Dapps.

Since they are cryptographically secured, Dapps are referred to as "secure applications". Some of the [high profile Dapps](http://www.ethdocs.org/en/latest/introduction/web3.html) built on the Ethereum platform include:

* [Augur](https://augur.net/), which is a Decentralized Prediction Market
* [Digix](https://digix.global/), which tokenizes gold on Ethereum
* [Maker](https://makerdao.com/), which is a Decentralized Autonomous Organization (DAO).

The Ethereum network is a distributed global public network, which means it is not run on central servers in a certain geographical location.

Instead, the computing power that runs the network is contributed by nodes that are spread across the globe.

In other words, Dapps have "zero downtime" - they never go down and, in general, cannot be switched off.

### Ethereum Smart Contracts

A hypothetical example of an Ethereum-based smart contract may involve the following transaction: in an equity raise, transfer amount X from the investor to the company upon receiving the given shares from the company.

The monetary amount X, which was pre-validated by the company for the transaction (much like in a credit card purchase), is held in escrow by the smart contract, until the shares have been received by the investor.

Any kind of arbitrary sophisticated business logic can be committed to the blockchain.

The Ethereum blockchain only encodes these "rules of the games". The actual payoffs occur by interacting with the blockchain.

The illustration below describes this process.

The smart contract encodes the agreement between the company raising funds and its investors (Panel 1).

The smart contract sits on the Ethereum public blockchain, and is run on the Ethereum Virtual Machine (EVM).

Once hitting a triggering event, like an expiration date or a strike price that has been pre-coded, the smart contract automatically executes as per the business logic (Panel 2).

As an added benefit, regulators are able to scrutinize the market activity on an ongoing basis, without compromising the identity of specific players in a permissionless public blockchain, as Ethereum (Panel 3).



Note: With the advent of the Ethereum blockchain platform and the scripting functionality or smart contracts that it enables, there are ongoing attempts to do the same for the Bitcoin blockchain, which does not allow for this, due to security reasons. [RSK](http://www.rsk.co/) is one such smart contract platform that seeks to achieve this "with a 2-way peg to Bitcoin". The added functionality can go a long way in making the Bitcoin blockchain useful for use cases other than cash transfers.

### Exploring Permissionless Blockchains

We will examine the Bitcoin and Ethereum blockchains, both of which are permissionless, public blockchains.

We will examine several large transactions, and the genesis block for each blockchain.

We will look at block heights, transaction times, mining pools, timestamps, and block rewards.

### Exploring Bitcoin and Ethereum Blockchains

Let's take a look at a couple of public blockchains: those of Bitcoin and Ethereum, and let's examine the genesis block, or the first block, of each one of them.

Then, we'll take a look at a couple of large transactions, including the most famous transaction in cryptocurrency history: the purchase of a pizza for 10,000 bitcoins.

First, we'll go to this blockchain explorer, and see that there is a Height column, which indicates the number of blocks in this particular blockchain; it's nearing a half a million.

These blocks are created approximately every 10 minutes, and there's a Transactions column that shows how many transactions are included in each block, as well as the Total Sent, or the amount of Bitcoin that was transferred in each of those blocks.

Finally, you can notice that there's... they relate by column, which is essentially the miner or mining pool that created that block.

From here, let's take a look at another blockchain explorer, and you can see here the genesis block of the Bitcoin blockchain.

Notice that the timestamp is January 3rd 2009.

That's the genesis block of the Bitcoin blockchain.

Now, moving on to the Ethereum blockchain, we'll look at another blockchain explorer.

And this one shows you that there's approximately 5 million blocks in the Ethereum blockchain.

Notice that each block is created much more quickly than in the Bitcoin blockchain.

From here, we'll examine the genesis block of the Ethereum blockchain, and notice that it was mined about two years ago, and the mining reward for this was approximately five ether.

From here, we'll take a look at the very interesting transaction: that of the pizza transaction.

On Bitcoin Forum, there was somebody on May 18th of 2010 who was requesting that they would pay 10,000 bitcoins for a pizza.

They provided their address and someone in fact sent them a pizza. In fact, it was from Europe.

And you can see here that that was this transaction here: of 10,000 bitcoins.

And lastly, a very large and interesting transaction of 658 bitcoins, done recently.

Notice that the value of that is close to 3 million dollars.

You can examine these transactions on both the Bitcoin and Ethereum blockchains, and many other blockchains.

In Chapter 2 of this course, we'll touch upon the Hyperledger Explorer, which can be configured to examine blockchains you might develop with other of the Hyperledger frameworks.

### Consensus Algorithms

Consensus in the network refers to the process of achieving agreement among the network participants as to the correct state of data on the system. Consensus leads to all nodes sharing the exact same data. A consensus algorithm, hence, does two things: it ensures that the data on the ledger is the same for all the nodes in the network, and, in turn, prevents malicious actors from manipulating the data. The consensus algorithm varies with different blockchain implementations.

While the Bitcoin blockchain uses Proof of Work as the consensus algorithm, other blockchains and distributed ledgers are deploying a variety of consensus algorithms, like the Proof of Stake, Proof of Burn, Proof of Capacity, Proof of Elapsed Time, and many others, depending on their unique requirements.

Next, we will briefly explain some of these algorithms.

### Proof-of-Work (PoW)

The Proof of Work consensus algorithm involves solving a computational challenging puzzle in order to create new blocks in the Bitcoin blockchain. Colloquially, the process is known as 'mining', and the nodes in the network that engage in mining are known as "miners". The incentive for mining transactions lies in economic payoffs, where competing miners are rewarded with 12.5 bitcoins and a small transaction fee.

As described in the 2016 Kudelski Security report,

"Proof-of-work (PoW) is the outcome of a successful mining process and, although the proof is hard to create, [it] is easy to verify".

For better understanding, please consider the following example provided by [Ofir Beigel](https://99bitcoins.com/proof-of-work-proof-of-stake/" \t "_blank):

"(...) guessing a combination to a lock is a proof to a challenge. It is very hard to produce this since you will need to guess many different combinations; but once produced, it is easy to validate. Just enter the combination and see if the lock opens".

Multiple criticisms exist for the PoW consensus algorithm. PoW requires a huge amount of energy to be expended, given the computationally heavy algorithm. In addition, PoW has a high latency of transaction validation, and the concentration of mining power is located in countries where electricity is cheap. In terms of the network security, PoW is susceptible to the "51% attack", which refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's computing power.

### Proof-of-Stake (PoS)

The Proof of Stake algorithm is a generalization of the Proof of Work algorithm. In PoS, the nodes are known as the "validators" and, rather than mining the blockchain, they validate the transactions to earn a transaction fee. There is no mining to be done, as all coins exist from day one. Simply put, nodes are randomly selected to validate blocks, and the probability of this random selection depends on the amount of stake held. So, if node X owns 2 coins and node Y owns 1 coin, node X is twice as likely to be called upon to validate a block of transactions. The specific implementation of PoS can vary, depending on the use case, or as a matter of software design. Instances include [Proof of Deposit](https://www.linkedin.com/pulse/blockchain-consensus-algorithm-proof-of-work-satyakam-chakravarty/) and [Proof of Burn](https://en.bitcoin.it/wiki/Proof_of_burn). The PoS algorithm saves expensive computational resources that are spent in mining under a PoW consensus regime.

### Proof of Elapsed Time (PoET)

Developed by Intel, the Proof of Elapsed Time consensus algorithm emulates the Bitcoin-style Proof of Work. Hyperledger's Sawtooth implementation is an example of PoET at work. Instead of competing to solve the cryptographic challenge and mine the next block, as in the Bitcoin blockchain, the PoET consensus algorithm is a hybrid of a random lottery and first-come-first-serve basis. In PoET, each validator is given a random wait time.

"The validator with the shortest wait time for a particular transaction block is elected the leader".- [sawtooth.hyperledger.org](https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction.html)

This "leader" gets to create the next block on the chain.

### Simplified Byzantine Fault Tolerance (SBFT)

The Simplified Byzantine Fault Tolerant consensus algorithm implements an adopted version of the [Practical Byzantine Fault Tolerant](https://blog.acolyer.org/2015/05/18/practical-byzantine-fault-tolerance/) (PBFT) algorithm, and seeks to provide significant improvements over Bitcoin's Proof of Work consensus protocol. The basic idea involves a single validator who bundles proposed transactions and forms a new block. Note that, unlike the Bitcoin blockchain, the validator is a known party, given the permissioned nature of the ledger. Consensus is achieved as a result of a minimum number of other nodes in the network ratifying the new block. In order to be tolerant of a Byzantine fault, the number of nodes that must reach consensus is **2**f**+1** in a system containing **3**f**+1** nodes, where f is the number of faults in the system. For example, if we have 7 nodes in the system, then 5 of those nodes must agree if 2 of the nodes are acting in a faulty manner.

The practical example would be that of [ByzCoin](http://hackingdistributed.com/2016/08/04/byzcoin/" \t "_blank), which seeks to make key improvements over the original Bitcoin protocol. Addressing the challenge around scalability due to high latency, ByzCoin transactions are irreversibly committed to the blockchain within seconds. The added advantage is the communication trees to "(...) optimize transaction commitments and verification under normal operations" ([*2016 Kudelski Security report*](https://www.kudelskisecurity.com/sites/default/files/files/Kudelski_Security_Publication_Blockchain_EN.pdf)).

### Proof-of-Authority (PoA)

Proof-of-Authority (PoA) is a consensus algorithm which can be used for permissioned ledgers. It uses a set of "authorities", which are designated nodes that are allowed to create new blocks and secure the ledger. Ledgers using PoA require sign-off by a majority of authorities in order for a block to be created.

### Comparing Permissioned Consensus Approaches and Standard PoW

[***Consensus***](https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf)can be implemented in different ways, such as through the use of lottery-based algorithms (PoET or PoW), or through the use of voting-based methods (SBFT), each targeting different network requirements and fault tolerance models.

Lottery-based algorithms are advantageous in that they can scale to a large number of nodes. Voting-based algorithms provide low-latency finality.

The following table offers an at-a-glance view of the main considerations and pros and cons of different business blockchain approaches to reaching consensus.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Permissioned Lottery-Based | Permissioned Voting-Based | Standard Proof of Work (Bitcoin) |
| Speed | \*\*\*\*\* GOOD | \*\*\*\*\* GOOD | \* POOR |
| Scalability | \*\*\*\*\* GOOD | \*\*\* MODERATE | \*\*\*\*\* GOOD |
| Finality | \*\*\* MODERATE | \*\*\*\*\* GOOD | \* POOR |

## Hyperledger

[Hyperledger](https://www.hyperledger.org/) is an open source effort created to advance cross-industry blockchain technologies. Hosted by The Linux Foundation, it is a global collaboration of members from various industries, including finance, banking, Internet of Things (IoT), supply chain, manufacturing, healthcare and more. Hyperledger boasts a host of enterprise-ready solutions. Hyperledger is about communities of software developers building blockchain frameworks and platforms. We will take a closer look at some of the current Hyperledger projects in the coming chapters.

"One of the first things people learn when coming to Hyperledger is that Hyperledger isn’t, like its name may imply, a ledger. It is a collection of blockchain technology projects."

Dan Middleton, [*All Are Welcome Here*](https://www.hyperledger.org/blog/2018/12/03/all-are-welcome-here) (2018)

### Hyperledger Blockchains: Permissioned or Permissionless?

Hyperledger blockchains are generally permissioned blockchains, which means that the parties that join the network are authenticated and authorized to participate on the network. Hyperledger’s main goal is to create enterprise grade, open source, distributed ledger frameworks and code bases to support business use cases.

### Advantages of Using a Permissioned Blockchain over a Permissionless Blockchain

If you look at permissionless blockchains, like the Bitcoin blockchain or the Ethereum blockchain, anyone can join the network, as well as write and read transactions. The actors in the system are not known, which means there could be some malicious actors within the network.

Hyperledger reduces these security risks and ensures that only the parties that want to transact are the ones that are part of the transaction and, rather than displaying the record of the transactions to the whole network, they remain visible only to the parties involved. Hyperledger provides all the capabilities of the blockchain architecture - data privacy, information sharing, immutability, with a full stack of security protocols - all for the enterprise. Permissioned blockchains offer more efficient transaction performance, thus being highly scalable, and have a clearly defined governance structure.

### Hyperledger vs. Other Permissioned Ledgers (Brian Behlendorf)

What makes Hyperledger so unique, compared to other permissioned ledgers?

Hyperledger is a really unique community in the open source landscape of different blockchain technologies.

We kind of model ourselves a little bit after Apache, and some of the other organizations out there that really are communities of communities, right?

Within Hyperledger, we have different technology code projects, essentially.

Projects like Fabric and Sawtooth, and a lot of the others that all of you will be finding out about, but, what these projects have in common is a set of development principles around working in the public, around, you know... even from the earliest ideas, you know, developers should be sharing that with other developers, right, not just something they build privately, then throw over the wall, and release this open code, but that starts out from day one as a public process, right, and multi-stakeholder as well.

While projects do often start out as the work of one company or one small set of developers, we really come to trust technologies when we see that there's lots of people both using it and contributing to it.

And so, that way, we know this is actually a project that will likely outlast any one company's commitment to it, right?

That's a good basis for deciding what open source technologies to build on.

At Hyperledger, we're trying to make sure that each of these projects fulfills that goal of being multi-stakeholder, of being active software development projects that get as quickly as possible to a production release, something that organizations can actually use in real production environments, and yet, still has the flexibility to explore a new concept, to explore a new consensus mechanism, a new way of writing smart contracts, right?

That balancing act is really what we're trying to strive for inside of Hyperledger.

### Other Distributed Ledger Technologies (Robert Schwentker)

What are some examples of other blockchain and distributed ledger technology systems, and what are their benefits?

Chain Core, created by chain.com, has initially been designed for financial service institutions, and for things like securities, bonds, and currencies.

Their company has strong ties with Visa, Citigroup, and Nasdaq.

The Corda distributed ledger platform is designed to record, manage, and automate legal agreements between businesses.

It was created by the R3 company, which is a consortium of over a hundred global financial institutions.

Quorum is a permissioned implementation of Ethereum, which supports data privacy.

Quorum achieves this data privacy through allowing data visibility on need-to-know basis by a voting-based consensus algorithm. Interestingly, Quorum was created and open sourced by JPMorgan.

### Chain Core

[**Chain Core**](http://fedchains.com/core/) is an enterprise permissioned blockchain system that is mostly focused on financial services, like currencies, securities, derivatives, gift cards, and loyalty points. The company partners with clients to launch and operate a network under the client's brand. Thanks to its strategic partnerships with companies such as Capital One, Citigroup, Fiserv, Nasdaq, Orange, Visa, etc., the company raised over $40 million in funding since 2014.

Within the Chain Core network, the creation and transfer of assets is decentralized. However, as stated in the [2016 Kudelski Security report](https://www.kudelskisecurity.com/sites/default/files/files/Kudelski_Security_Publication_Blockchain_EN.pdf),

"the operation of the network is governed by a designated set of entities known as a federation".

The platform features the Chain Testnet, which allows decentralized application development on Chain Core, operated by Chain, Microsoft, and the Initiative for Cryptocurrencies and Contracts (IC3).

### Corda

[**R3**](https://www.r3.com/about/)is an enterprise blockchain software firm that works with over three hundred members and partners across multiple industries, that seeks to leverage distributed ledger technologies to record, manage, and automate legal agreements between businesses through its software solution, called Corda.

Launched in 2016**,**[**Corda**](https://www.corda.net/) is an open source distributed ledger platform, which features a blockchain-style P2P network; however, it is not a blockchain platform. Unlike blockchains, which involve global availability of data across the network and third party validators, Corda only allows information access and validation functions to parties actually involved in the transaction. Featuring a different software architecture, "Corda achieves consensus between firms at the level of individual deals, not the level of the system" ([Richard Gendal Brown](https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/), 2016), while supporting a variety of consensus mechanisms.

### Quorum

Created by JPMorgan, [Quorum](https://www.goquorum.com/) is, in fact, a fork of the Ethereum public blockchain, which uses a voting-based consensus algorithm to facilitate an enterprise-focused distributed ledger and smart contract platform. Data privacy is achieved within the network by allowing data visibility on a need-to-know basis. This open source blockchain platform is designed to support "both transaction-level privacy and network-wide transparency". The network validates all smart contracts and overall system state through the involvement of all running nodes. As with other permissioned ledgers, regulatory compliance is front and center in the Quorum platform.

### IOTA

[**IOTA**](https://www.iota.org/) is an open source permissionless distributed ledger technology that has been around since 2015; it has a cryptocurrency called mIOTA. According to [Martin Rosulek](https://medium.com/@MartinRosulek/how-iota-makes-future-for-internet-of-things-af14fd77d2a3), "It is the first cryptocurrency that provides the whole ecosystem based on blockless blockchain" to enable machine-to-machine (M2M) transactions.

IOTA, however, is more than just a cryptocurrency. Essentially, the platform entails a generalization of the blockchain protocol (the technology called Tangle) that sits at the backend of the IOTA platform. The platform uses a Decentralized Acyclic Graph (DAG) instead of a blockchain to store its ledger.

Instead of paying miners to validate the transactions, the architecture of the network involves peer-based validation. We can think of a simple analogy, that of a teacher grading students' homework: the students are the clients/users in the Bitcoin protocol, and the teacher is the miner/validator. Tangle technology asks students (users) to grade each other's homework, making the need for a teacher (external validator) redundant, and avoiding expenses related to the teacher's/validator's work. This allows the platform to be completely free of cost, without facing the scaling challenges that are inherent in the first generation of blockchains.

Additionally, the use of the platform with connected devices or the Internet of Things

"enables companies to explore new business-to-business models by making every technological resource a potential service to be traded on an open market in real time, with no fees".  
- [Roger Aitken](https://www.forbes.com/sites/rogeraitken/2017/06/15/iotas-bitfinex-listing-surges-to-1-5b-record-breaking-crypto-capitalization-on-market-debut/#7e4170e275a5), 2017

IOTA focuses mainly on enabling the emerging Internet of Things (IoT), but also plans to go beyond this, on being the transaction settlement and data integrity layer for the Internet of Everything (IoE).

### Challenges in the Adoption/Deployment of Distributed Ledger Technologies

There are a number of challenges to the widespread use of permissioned distributed ledger technologies. Key among them are challenges around the lack of standards, regulatory challenges, and the lack of knowledge about distributed ledger technologies. These challenges are inherent to any new technological infrastructure that replaces an older infrastructure.

Other challenges encountered when it comes to the adoption and deployment of distributed ledger technologies are:

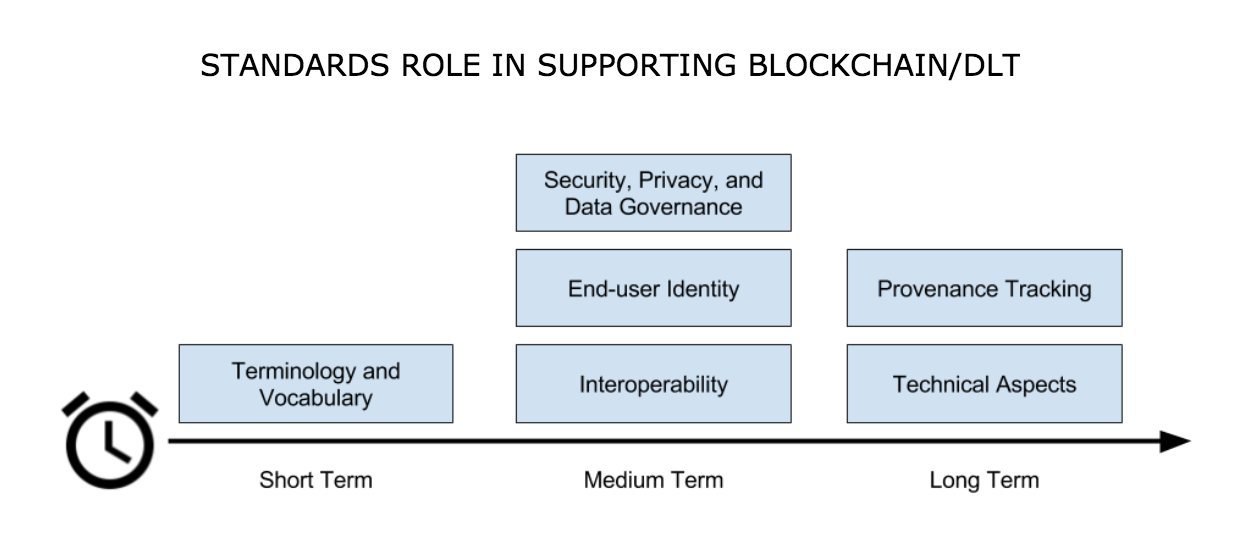
* Resistance to change
* Scalability concerns
* Interoperability and integration with legacy systems
* Unproven business case
* Lack of capital to fund new investments
* System complexity and costs.

We hope you go on to address some of these challenges and contribute to building a secure digital future!

### Standards

Since we are still witnessing the early days of blockchain technology, there is very little agreement on standards in the developer and business community, as of yet. Standards are key in ensuring interoperability and avoiding risks associated with a fragmented ecosystem. Standards are critical not just for the distributed ledger itself, but also for supporting services, like identity, privacy, and data governance. Furthermore, the management of keys, as well as protocols and standards around key loss and theft, will be critical ([Deshpande, Stewart, Lepetit, & Gunashekar](https://www.bsigroup.com/PageFiles/508003/BSI_Blockchain_DLT_Web.pdf), 2017).

As a result, the International Organization for Standardization for Blockchain and Distributed Ledger Technologies was established in 2016 and has defined areas for future standardization work ([Clare Naden](https://www.iso.org/news/Ref2188.htm), 2017). More about the ISO/TC 307 technical committee can be found at the [ISO/TC 307 website](https://www.iso.org/committee/6266604.html).



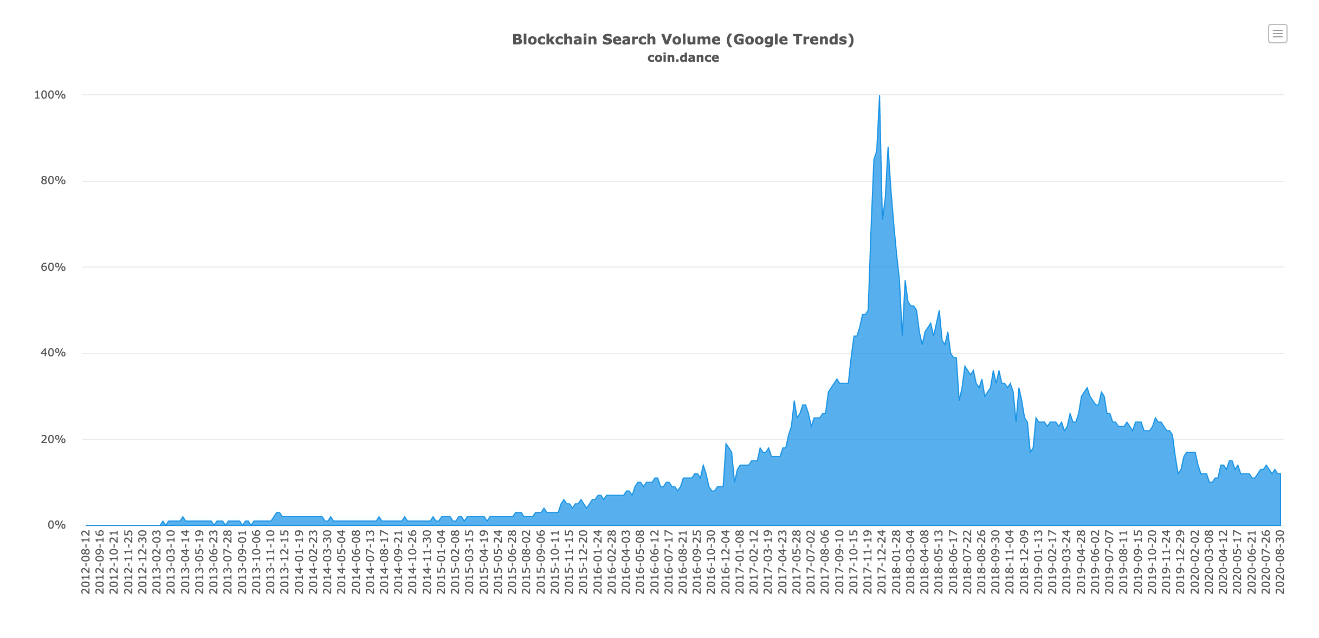
### Regulation

The lack of regulation around transactions on the blockchain creates an environment of uncertainty for all players. Highly regulated industries like financial services are treading carefully in the DLT space. The Securities and Exchange Commission of the United States has clarified its stance on [Initial Coin Offerings (ICOs)](https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings) in 2017. The Chinese government has, in fact, banned all ICOs, while 60 major ICO platforms are being investigated ([Saheli Roy Choudhury](https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html), 2017).

Similarly, there are no regulatory guidelines governing smart contracts, causing much anxiety among various players like lawyers, regulators, programmers, and businesses. The lack of regulatory guidelines, along with a lack of industry standards, exacerbates hindrances to rapid adoption of DLT.

### Lack of Know-How

The lack of know-how (and know-whom and know-where) around distributed ledger technologies and the availability of experts in the area is a major challenge in the adoption of distributed ledger technologies. While there has been an exponential increase in the interest around 'blockchain', as indicated in the figure below, there is a huge lag of technical talent in the space. In fact, the origin of this course stems from the need to address this gap in know-how.



**Blockchain Search Volume**  
Retrieved from <https://coin.dance/stats/blockchain> on November 6, 2020

Jobs in the blockchain development space are among the top 20 fastest growing, and the number of positions available increased [over 200% in 2018](https://www.computerworld.com/article/3277617/the-top-blockchain-jobs-you-need-to-know-about.html) over those available the previous year. However, there is not a large enough pool of qualified blockchain developers, and this is a major concern. The emergence of more and more blockchain training courses and certifications is aiming to slowly close this gap.

## Chapter 2. Introduction to Hyperledger

This chapter provides an overview of Hyperledger, a collaborative project hosted by The Linux Foundation that is focused on business blockchain technologies. It also provides a brief introduction to the projects advanced under the Hyperledger greenhouse, as of November 2020.

### Learning Objectives

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

* Explain the differences between Hyperledger and permissionless blockchain technologies.
* Discuss how Hyperledger leverages open standards and open governance to support business solutions.
* Define what a project is according to the Hyperledger documentation.
* Discuss the project lifecycle process adopted by Hyperledger, and the five possible states.

### Hyperledger (Navroop Sahdev)

Hyperledger is an open source effort created to advance cross-industry blockchain technologies.

It's a global collaboration hosted by The Linux Foundation that encompasses various industries and organizations worldwide.

You may think of Hyperledger as an operating system for marketplaces, data sharing networks, microcurrencies, and decentralized digital communities.

A shared goal is to significantly reduce the cost and complexity of doing business.

Hyperledger blockchains are permissioned blockchains, which means that the parties that join the network are generally authenticated via an identity module.

Essentially, Hyperledger blockchains are specifically designed to be enterprise solutions.

If you look at permissionless blockchains, like the Bitcoin blockchain or the Ethereum blockchain, anyone can join the network, which means there would invariably be some malicious actors within the network.

Hyperledger reduces these security risks, and ensures that only the parties that want to transact are the ones that are part of the transaction.

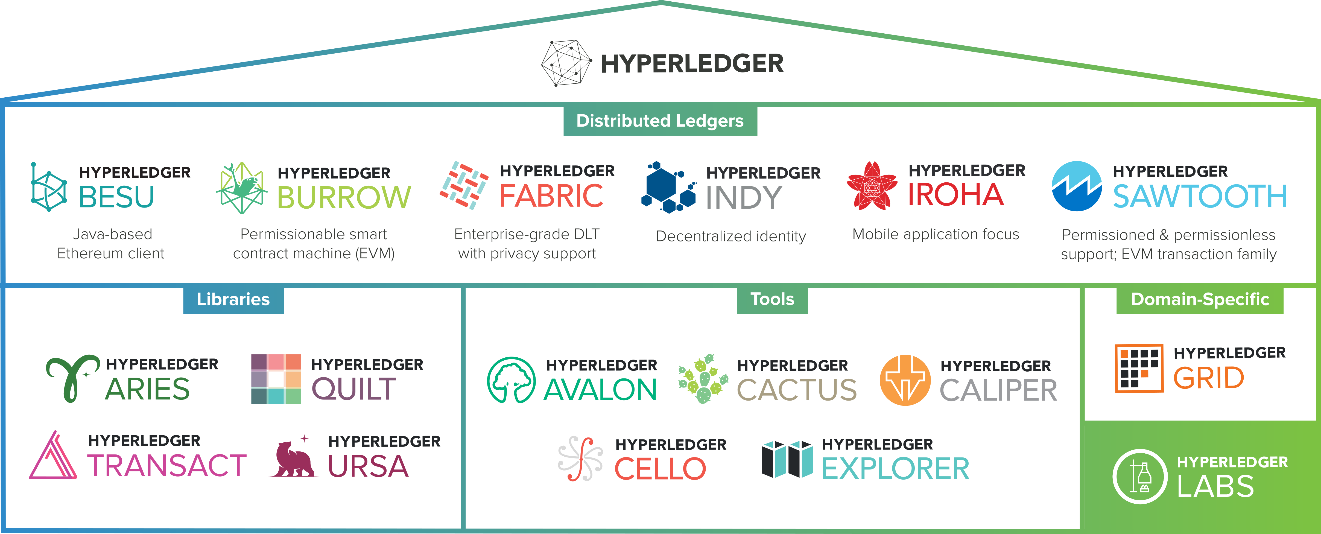
Rather than displaying the record of the transactions to the whole network, they remain within the parties involved.

Hyperledger provides all the capabilities of blockchain architecture, data privacy, information sharing, immutability, with a full stack of security protocols, all for the enterprise.

### 2.2 Hyperledger

[Hyperledger](https://www.hyperledger.org/about) incubates and promotes a range of business blockchain technologies, including distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, utility libraries, and sample applications. Hosted by The Linux Foundation, collaborators include industry leaders in technology, finance, banking, supply chain management, manufacturing, and IoT.

As of November 2020, there are 16 projects in the Hyperledger greenhouse, six of which are distributed ledger and domain specific frameworks. The other 10 projects are tools and libraries that support these frameworks.



As [Arnaud Le Hors](https://www.hyperledger.org/blog/2017/09/12/3431), member of the Hyperledger Technical Steering Committee, emphasized,

"these projects show how broadly applicable blockchain technology really is. This goes way beyond cryptocurrencies".

Hyperledger provides an alternative to the cryptocurrency-based blockchain model, and focuses on developing blockchain frameworks, tools and libraries to support global enterprise solutions. The focus of Hyperledger is to provide a transparent and collaborative approach to blockchain development.

### The Birth of Hyperledger

It's amazing how quickly Hyperledger has developed and evolved over the past few years.

I was wondering if you could tell me a bit about the journey of how Hyperledger has come to be.

The Hyperledger Project began when a set of companies who were starting to pay attention to this Bitcoin space, this cryptocurrency space, this blockchain space, approached The Linux Foundation and said "Let's do a project together".

The Linux Foundation has been at the heart of the Linux ecosystem, bringing together companies and developers to try to, you know, serve, say, air traffic control to the development of a common technology platform.

And, over the last few years, it has grown into other related technology spaces: software-defined networking, cloud computing, all these kinds of things... domains that also needed this focused effort to bring these two kinds of communities together.

It's very natural when companies like IBM, or even new ones, that had never worked with The Linux Foundation before, like JPMorgan, or startups in this space, like Digital Asset, when they started to talk with each other, and tried to figure out where a good home for this would be, they approached The Linux Foundation, right?

Some conversations got started, and there was a sense that what was interesting about this space wasn't so much the cryptocurrencies, and, you know, the make-money-fast kind of mentality, but the underlying distributed ledger and smart contract technology platforms, right?

And there's still a lot of hard work to do to figure out the right approaches to this.

In December of 2015, The Linux Foundation, in conjunction with those companies, and about 30 more, announced the launch of the Hyperledger effort.

Alright, the Hyperledger Project, which we really just call Hyperledger now.

The first code drop, meaning the first release of software, happened just two months later, in February of 2016, when the Fabric codebase came over.

Initially, it had been built inside of IBM, but, when it came over, it was now part of the community, right, followed soon after by Sawtooth Lake.

And it wasn't just code; the community started to meet face to face on a pretty regular basis, about once every two months.

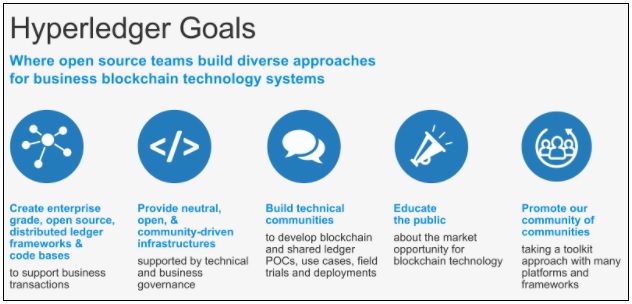
And this was because there was a lot to sort out, a lot of knowledge to share.

I joined in May of 2016, so, a little bit of a late comer, I guess, to the launch of it.

I joined partly because I saw how transparent, and how engaging, even from day one, all of these processes have been.

### Hyperledger Goals

Hyperledger has taken a leadership role to develop cross-industry standards and provide a neutral space for software collaboration. The financial services industry, in particular, is witnessing an unprecedented level of collaboration between institutions that have traditionally been competitors. The advent of a new foundational or infrastructural technology like the blockchain - much like the Internet - requires collaboration of various actors in order to realize the full benefits of the technology. Unless all actors use a certain standard, the pace of technological dissemination will continue to be slow. Technological adoption is characterized by network effects, where the costs decrease with the increase in use of a certain technology. Since shifting to distributed ledger technology involves significant costs, open source software, communities and ecosystems that develop around these have a significant part to play.



### The Importance of Open Source

You had mentioned before how Hyperledger is different from other consortiums because of its focus on creating an open community, not just open sourcing code.

Can you tell us a little bit about why this is important?

Open source communities, I believe, live and breathe on not just, you know, reporting bugs or, you know, downloading code, but, actually, live and breathe on true collaboration, on saying not just, you know, "I have a bug and somebody needs to fix it", but, instead, saying "Here's how I'd like to solve this", right? What do people think?

"Here is a design for implementing a new feature." What do people think?

And I think the evidence shows that that creates higher quality code. It also creates more long lasting code.

I don't think you have a project like the Linux kernel, which has now been around for 26 years, right, without having a mechanism for a community to develop an institutional memory, right?

Why were certain decisions made? What were some ideas that were proposed and, ultimately, found to either be shot down or not really good enough, right, so that we don't end up changing things back and forth, right, we don't end up making mistakes that we could have avoided before or learning from previous...how do we make sure we learn from previous mistakes, right?

And that's only possible in an open source community if, on top of just releasing code, you're also engaging in the creative process itself, and making that public facing.

And I think, really, we found out over 25 years of open source that that's the best way to build trustworthy software.

I believe it leads to higher security software and higher quality software, but really, the question is trust.

This is code that sits... At Hyperledger, this is code that will sit at the heart of these enterprises.

This will be their system of record, right? It's essential that we develop this code in a trustworthy way and, while we do all sorts of things to help them trust the data in the system, ultimately, they have to trust the software, as well.

And what I hope is that, through these processes, they can rest assured that, when they pick up Hyperledger, anything, right, that anything will be software that they can trust.

### Open Standards

"Only an Open Source, collaborative software development approach can ensure the transparency, longevity, interoperability and support required to bring blockchain technologies forward to mainstream commercial adoption. That is what Hyperledger is about - communities of software developers building blockchain frameworks and platforms".  
- [hyperledger.org](https://www.hyperledger.org/about)

As we learned in Chapter 1: "Discovering Blockchain Technologies", the non-availability of standards in distributed ledger technologies is one of the major hurdles in scaling them. One of Hyperledger's key goals is to facilitate the process of standards formation, not by promoting its own distributed ledger(s), but by providing a space for a variety of standards to co-exist simultaneously:

"Rather than declaring a single blockchain standard, it encourages a collaborative approach to developing blockchain technologies via a community process, with intellectual property rights that encourage open development and the adoption of key standards over time".  
- [hyperledger-fabric.readthedocs.io](https://hyperledger-fabric.readthedocs.io/en/latest/)

Hyperledger aims to adhere to "open standards", which means they are

"(...) interoperable through open published interfaces and services".- John Palfreyman, [ibm.com](https://www.ibm.com/blogs/insights-on-business/government/open-innovation-blockchain-hyperledger/)

### Open Source and Open Standards

The [Enterprise Ethereum Alliance](https://entethalliance.org/) (EEA) and [Hyperledger](https://www.hyperledger.org/) formally joined each other's organizations as Associate Members in October 2018. This [strategic partnership](https://www.hyperledger.org/blog/2018/10/01/growing-the-enterprise-blockchain-ecosystem-through-open-standards-and-open-source-code) aims to grow the blockchain ecosystem by enabling "active and mutual cross-community collaboration through event participation, connecting with other members, and finding ways for our respective efforts to be complementary and compatible."

* EEA promotes the development of specifications and standards for enterprise blockchain networks
* Hyperledger advances the development of open source software for establishing, managing and connecting enterprise blockchain networks.

This announcement came as a confirmation of an already fruitful collaboration between the two organizations; some examples of this collaboration:

* Hyperledger Burrow is an implementation of the Ethereum Virtual Machine (EVM) bytecode interpreter
* Hyperledger Sawtooth support for the EVM as a transaction processor (Seth)
* Hyperledger Fabric support for the EVM
* The existence of an EEA working group on Trusted Execution Environments, along with a prototype implementation of the proposed standards, Private Data Objects, built as a lab at Hyperledger.

"...simultaneously developing community-driven open standards and production-quality open source reference implementations is a best practice of Internet-scale software development work."

While working together, the two organizations will also continue to collaborate with other standard bodies and open source communities, all with the common goal of accelerating the adoption of enterprise blockchain technologies.

### Open Source and Open Governance

"Today, most people understand the concept of Open Source. What many people don't get, and something we here at Hyperledger and The Linux Foundation pride ourselves on doing well, is Open Governance".  
- [*hyperledger.org*](https://hyperledger.org/blog/2017/09/06/abcs-of-open-governance)

Open source software is software that is made freely available and may be redistributed and modified. In other words, anyone has the ability to view the code, use the code, copy the code, change the code, and, depending on the open source license, contribute back changes.

Open governance means that technical decisions for an open source project are made by a group of community-elected developers drawn from a pool of active participants. These decisions include things such as which features to add, how, and when to add them.

To learn more about the specifics of Hyperledger's open governance read the following article "[*ABCs of Open Governance*](https://www.hyperledger.org/blog/2017/09/06/abcs-of-open-governance)".

### Software Governance of the Hyperledger Projects (Brian Behlendorf)

How does the software governance of all of the Hyperledger projects work?

In open source projects you do... it's not a free-for-all, right? It's not just everybody throwing in every line of code, hoping that what, you know, it sticks to the wall, and that everything is fine, right?

There actually is a development process that involves decision-making about what comes in and what doesn't, right?

At the core of each of the projects at Hyperledger is a set of maintainers.

These are individuals who either were with the project when it came in, as initial maintainers, right, because they had been working on the code before, or were invited in by that initial set of maintainers to become maintainers, after demonstrating, you know, a history of contributions to the project, alright?

These are now individuals who are trusted.

Once you're in that group, obviously, everything those maintainers do is public.

If they commit to the source code repository, approve a a patch, a commit request, or pull request, everything they do is public anyway, so there's always that accountability for their actions.

If somebody does something wrong, anybody can always say "I think that's wrong", and the set of maintainers can sometimes come to a decision to reverse a commit, right?

That's within their power.

It's really up to those maintainers to also chart the path forward: what's the roadmap, when will we do the next release, right, the next minor point released, the next major release.

Obviously, they do that in a public way.

Sometimes, they'll use a phone call, sometimes, they'll use chat on Rocket Chat, sometimes, they'll use email, but they know that their job is to be accountable and responsible to the broader development community.

Now, from a Hyperledger perspective, if we leave it up to the projects to really decide the roadmap of what they're trying to solve, there's a group called the Technical Steering Committee, though, that is elected by all the contributors across all the projects, not even just the maintainer...anybody who has contributed a line of code, contributed to the wiki in some substantial way, they elect a group of eleven developers who form this Technical Steering Committee.

And the TSC is kind of an oversight body.

They make sure that the projects are growing, and that they're healthy.

They review activity in those projects, they also approve new projects when they come in, and they approve the graduation from the Incubator, right?

What they don't get to do is, you know, tell us, tell a project "Hey, you're working on the wrong thing. Go work on this, instead", right?

They really have to depend on this kind of decentralized governance, right, to aim in the right direction.

By and large, we try to make sure though that every project has some sort of relation to distributed ledgers and smart contracts.

Our goal is not to be the GitHub of distributed ledgers and smart contracts projects.

There's already a GitHub for that, alright?

We want these projects to be a curated, you know, coherent portfolio of different projects that might even compete with each other, right?

In many ways, Fabric and Sawtooth and Iroha do overlap, and you can build an implementation of something in all three of those. That's okay, right?

We're going to discover over time how these projects differentiate with each other, and it's the role of the Technical Steering Committee, and a bunch of other committees we have around identity, and architecture, and white papers, and things, to try to weave these different efforts together in something that looks coherent, something that makes sense for developers.

### Strength Through Diversity

As you familiarize yourself more with Hyperledger and the blockchain technologies it fosters in its greenhouse, you will notice the similarities between some of its projects, but most importantly, what differentiates them from one another and the use cases they were designed to address. The idea behind this approach was and continues to be that there is no one solution to address the myriad of needs, requirements and use cases.

"Having a portfolio of projects, though, enables us to have the variety of ideas and contributors to become a strong open source community... It's not that our multiplicity of projects has given us strength through numbers, but rather strength through diversity."

Dan Middleton, [*All Are Welcome Here*](https://www.hyperledger.org/blog/2018/12/03/all-are-welcome-here) (2018)

### Blockchain Security at Hyperledger (David Huseby)

Security with distributed ledgers really begins here at Hyperledger with our culture of secure software development.

Every aspect of the software, from development, through testing, through bug fixing, and vulnerability resolution, it's done in a completely open process.

It's open to anybody to participate.

We have maintainers that do all the code reviews.

Changes to code is driven by requirements, and patches come in to implement those requirements...

They're reviewed... we have requirements for tests to be written before it's accepted, and we have pretty rigorous testing infrastructure in place.

We use continuous integration, so, it's always building, and we have also initiated security reviews outside security audits of all our projects as they approach 1.0.

And it's that culture that really builds the foundation of trust for the Hyperledger projects.

Because we're radically transparent, and because we do the correct things from a software engineering perspective, we deserve the trust that consumers of our products put in our hands.

And then, building on top of our process, comes all of the cryptography and the data resiliency that you get with a distributed ledger.

Once we can ship a product, a piece of software that's been built to the best of our ability, then the guarantees provided by the cryptography really carry weight, or really, are ironclad.

It's a very holistic approach to security here at Hyperledger: everything, from the way we write software to the way the software works.

### How Will Hyperledger Change the Blockchain Ecosystem? (Brian Behlendorf)

How do you think Hyperledger will change the industries that adopt the technology?

In the Internet era, we, as technologists, have gotten really good at building big central databases and big central services, right?

Think about the move to the cloud. The move to the cloud wasn't a move to, a really dispersed, diffused, decentralized kind of system.

It often meant a move to one company's servers, right, or one company's products, right?

And I feel like, today, the Internet is more decentralized... more centralized than it used to be, right?

And that decentralized systems tend to grow quicker, they tend to be more adaptable, that nature looks a little bit more decentralized, right?

And, for businesses, I think you often don't want to be just sitting on the outside as a satellite on another centralized business, right?

Everyone would want to be the Uber of this, or the Uber of that.

Well, that's great for Uber and its investors. It's not so great when you're sitting on the outside, right?

A lot of industries kind of want... don't want to see their own industry move into that centralized approach.

And, typically, today, to be able to facilitate that, they have lots of point-to-point integrations, right?

Something like Hyperledger offers the potential for integration of an industry at a time, right, into a system that can not only become a system of record for recording transactions between parties in a network, in a marketplace, but also allow for the automation of a whole bunch of business processes through the use of smart contracts, right?

And, in a permissioned ledger, you still have an organization that acts somewhat like the referee on a football field, right, sets the rules of the game, watches how players play and, if somebody acts out of turn, even if the technology allows it, if they violate the spirit of the contract so-to-speak, or the human conditions, then, the referee can kick them out. And, by the way, if the referee does their job poorly, the two teams can kick the referee out, right?

This type of governance mechanism for something like a football game, right, is actually not too far from the kind of governance mechanisms that many industries deploy today, right?

With distributed ledger technologies like Hyperledger, we can actually have the information systems work and look a lot more like the way that the business processes look and work, especially in a more decentralized setting.

We can avoid the over-centralization of industries, and the over-centralization of society through the use of these technologies.

### Blockchain for Business

The cryptocurrency-based blockchain model, popularized by public blockchains like Bitcoin and Ethereum, currently falls short of fulfilling a host of requirements that many types of organizations would have to fulfill in order to be compliant when using blockchain and distributed ledger technologies - for instance, in the areas of financial services, healthcare, and government.

Hyperledger is a unique platform that is developing permissioned distributed ledger frameworks specifically designed for enterprises, including those in industries with strong compliance requirements. Enterprise use cases require capabilities such as scalability and throughput, built-in or interoperable identity modules for the parties involved in a transaction or a network, or even access to regulators who can access all data in the ledger as read-only to ensure compliance. The latter is particularly important because, regardless of the innovation, it has to operate within the current regulatory framework, as well as comply with any new rules that come into place specifically targeted at blockchain technologies.

The enterprise continues to be at the heart of this course.

### Why Businesses Choose to Use Hyperledger? (Brian Behlendorf)

And, as a follow-up, why are businesses choosing to use Hyperledger over other distributed ledger technologies?

Companies, when they decide what open source technologies to use, right, they should evaluate an open source project based on a number of factors, not just, you know, is the code available, does it run, how mature is it, right, have they released a 1.0, and a 1.1, and a 1.2...

You want to see a kind of a regular stream of these things.

We also believe companies make decisions... I believe companies make decisions about what open source technologies to choose based on the health of the community, right?

And how many other companies are embedding this technology inside of their own solutions, right, inside of other products and services, how many people out there are using it... that sort of thing.

And, at Hyperledger, what we're trying to do is not just build a very healthy developer ecosystem around our technologies.

We also do a lot to try to talk with our members and others who are using Fabric, or using Hyperledger Sawtooth, or these other technologies, to understand where are they using it and what's the value that they're getting from it.

And can we talk about that to the outside world, alright, which is hard.

Sometimes, people don't want to talk about their behind-the-scenes projects, right?

When we can talk about the application of that in music licensing, or food supply chain projects, alright, and start to talk about kind of a higher level impact that these projects can have, then, that I think gets companies really interested.

They don't make the decision to jump in, unless they can see that this is not just a piece of code, that this is a movement.

That's really what we're trying to build, and that's why we believe companies can confidently decide to pull down and start using Hyperledger Fabric, Hyperledger Sawtooth, and any of these projects.

And hopefully, become contributors to them, as well.

### Hyperledger, A Greenhouse for Blockchain Projects

Welcome to the Hyperledger greenhouse: an incubator for open source blockchain technologies for business hosted by the Linux Foundation.

What does that mean exactly?

Let's start here, with you: you're a business, large or small, participating in a commercial ecosystem.

Your business partners and peers want to do business with you, but in order to do that, you'll need a ledger.

This ledger contains a record of your transactions, along with many, if not all of the other transactions in the network.

It is vitally important to know that your copy of the ledger is identical to everyone else's, so you'll need a distributed ledger.

It's a new kind of network database that lets everyone in an ecosystem keep a copy of a common system of record.

But how does everyone agree on which transactions succeed or fail?

That's where Hyperledger software comes in.

This plant is actually software. Software that each business runs on systems it controls to broadcast out its transactions with other parties and receive, validate, and interact with messages delivered by others.

With any network like this, a particular software standard is used to keep everyone in sync.

But there are other ways to build these kinds of networks, using different consensus algorithms and different smart contract languages.

There will be many different ledger networks out there.

Ideally, they would all be able to interoperate due to certain common properties, much like how the Linux community uses various operating systems with a common kernel.

At Hyperledger, we're growing many different kinds of ledger technologies.

Here, you'll find communities of software developers working together to propel open source blockchain frameworks and tools into the future to deployment and adoption.

Businesses with strict blockchain requirements trust Hyperledger because it's hosted by the Linux Foundation, and its projects are developed by an open source community.

Developers can collaborate on a global level across company and industry lines to create innovative, modular, open source components and platforms.

It's this open source approach that allows for the kind of transparency, longevity, collaboration, community, and, of course, security that blockchain needs to become more mainstream, which is what Hyperledger is all about.

Hyperledger projects are meant to help you focus on developing your business solutions and feel confident that the legal, technical and organizational infrastructure is in place, thanks to Hyperledger and the Linux Foundation.

These are all open source projects, and anyone is welcome to pick them up and use them, no fee or permission required.

Of course, this only represents a fraction of what open source blockchain technologies can do now and in the future.

It's time to ask yourself: who will you trust with your trust network?

### Project Lifecycle and Hyperledger Incubator

According to the Hyperledger documentation, a **project** refers to a collaborative endeavor to deliver a work item. Projects can vary in terms of scope: some are intended to produce a document, some may develop new capabilities or refactor/remove an existing capability.

In general, open source initiatives use an incubation process for new work items: this allows members of the community to contribute new ideas and code in a more structured and transparent workflow. Hyperledger has adopted a rigorous project lifecycle process that has six possible states:

* **Proposal**   
  If an open source initiative wants to be hosted under the Hyperledger greenhouse, a proposal is submitted to the TSC for review. The proposal must have a clear description and a well-defined scope, must identify the development resources that are committed to the project, as well as the initial maintainers, and must be vendor neutral.
* **Incubation**  
  Once a project proposal is approved, it enters the Incubation phase, and the community has a chance to explore different idea related to the project. When a project reaches a mature-enough stage and qualifies to be declared *Active*, the maintainers will vote to submit a graduation review request to the TSC. All projects ready to graduate from Incubation must have a fully functional code base, test coverage commensurate with other *Active* projects, an active and diverse community of developers, and a history of releases that follow the *Active* release process. A project in the Incubation stage is not guaranteed to eventually graduate - some projects never get to *Active* state.
* **Active**  
  Projects that successfully exit the Incubation phase are considered *Active*. If reasons exist, an Active project can be deprecated.
* **First Major Release**  
  If the maintainers of a project are looking to publish the project's first major release, they will have to obtain approval from the TSC.
* **Deprecated**  
  All deprecated projects are maintained for a six month period by their communities; after that, the projects are removed from subsequent formal releases. A deprecation notice is given to the public. After a six-month deprecation period, projects are labeled *End of Life*.
* **End of Life**These are projects that are no longer developed or maintained.

New projects wanting to join are evaluated on a number of things:

* How do they fit with the portfolio of other projects
* How mature are they, to understand where they're going
* Who are the developers around the projects, etc.

When a project goes through a rigorous vetting process and graduates from the incubator, it signals to the public that they can now trust the code, that the code can be used to build applications upon it.

There are sixteen projects in the Hyperledger greenhouse, as of June 2019. And the door is open to new projects joining. There are four fully-fledged Hyperledger projects, that have graduated from the Incubator and are in an Active state (as of June 2019):

* Hyperledger Fabric (March 2017)
* Hyperledger Sawtooth (May 2017)
* Hyperledger Iroha (May 2018)
* Hyperledger Indy (March 2019)
* Hyperledger Besu (March 2020).

The other projects are still working through the process, and the goal is to get every one of them out of the Incubator.

### Hyperledger Labs

Currently, the Hyperledger Project Lifecycle is a very rigorous process that includes 6 possible states. For a project to join the Hyperledger Greenhouse, it must have a certain degree of maturity even in the early proposal and incubation stages.

[Hyperledger Labs](https://www.hyperledger.org/participate/labs) provides a [space](https://github.com/hyperledger-labs) where work can easily be started without the creation of an official Hyperledger project. Developers working on projects that are immature (incomplete code, not ready from a production-quality point of view, with small communities) or experimental will thus get the opportunity to work in a space suitable for innovation and testing of new ideas; moreover, they will work within a legal framework that would ease the transition to the Hyperledger Incubator (if the project matures enough and reaches that stage). Hyperledger Labs have similarities with the Apache Labs and the W3C Community Groups.

There is a specific process that must be followed when proposing a new lab. Labs that become dormant or unresponsive for 6 months or more, or are deemed deprecated or obsoleted by their committers are archived.

### Q/A with Brian Behlendorf, Executive Director of Hyperledger

Before diving deeper into the projects advanced under the Hyperledger umbrella, we asked Brian Behlendorf, Executive Director of Hyperledger at The Linux Foundation, some questions.

### Reasons Why Developers Would Become Interested in Open Source Software

Many of the students taking this course are more familiar with working with Devs within the same room.

But why do you think developers would be excited in becoming involved with open source projects, such as Hyperledger?

Well, open source software represents, generally, the largest software development classroom ever, right?

When I was learning about software development as an undergraduate at the University of California at Berkeley,

I was taking classes, you know, I was learning kind of the formal bits about, you know, data structures and algorithms, but the biggest education came from sitting on development mailing lists around the standards around HTTP and HTML, and, eventually, the software development mailing lists and open source communities for the early days of the web.

And seeing, really, how software gets built, right, what are the trade-offs, what are the negotiations, the back-and-forths, the messiness of software development, which doesn't look that different than, say, how Congress, you know, works on the bills sometimes, right?

Sometimes, it can be, you know, not very pretty, but you realize that software engineering is as much a technical pursuit, as it is a social pursuit.

And, in open source projects, I think we've figured out how do we have technical differences of opinion and work through them, how do we create the best software, the software with the greatest longevity, right? Why should we document our code...

Well, it's because we don't want to have to answer silly questions from the next person trying to understand what we wrote, right?

All of this is a really great education, I think, in understanding how to write higher quality code, whether that ends up being open source code or not...

That's one reason, I think, for developers to participate in open source projects, whether at Hyperledger or any place else.

The other is that open source projects are a really good way for you, as a software engineer, to understand what are the kinds of companies I want to work for, right?

The ones that are actively involved in open source projects, right?

How do I get to know people at those companies, right? And also, make them aware of my own skills, right?

And start to develop my own public history of my contributions.

These days, if you're a software engineer, if you're a software engineer and you're applying to any place interesting, they're going to look at your GitHub repository, right?

They're going to want to know about your history of contributions to open source projects as a way to evaluate your skills, and not just technical, but also your communication skills, your collaboration skills...

All of that means working on open source projects can be tremendously beneficial to your own ongoing education, as well as your ability to build your career.

### Hyperledger vs. Apache

While at Apache, you were able to successfully build an open software developer community.

What are some similarities and differences between Hyperledger and Apache in its evolution as an open source project?

Right... Well, on the Apache web server project, which later became the Apache Software Foundation, a lot of what happened was due to luck, was due to inheriting a tradition that had been established since the beginning of the internet, of technologists working together on common standards and common code.

And, there was kind of a DNA that was built-in and, as you know, the web was not that complicated at that point in time, either.

These standards were pretty simple, right?

We just kind of did what seemed natural. We started a mailing list.

We started an issue tracking system, a version control system, and we just started working together, very ad hoc, very informally.

And we became a non-profit about three years after we got started, when we realized we wanted a little more formalism, and a little more protection for the developers.

But it was all very informal, ad hoc, and many developers took on roles beyond development, such as marketing, such as legal, such as accounting, right?

Apache's culture has been a guild, right? Almost like a user community... a very community-driven kind of thing, where there's this validity that comes from that grassroots-kind-of-sense, right?

Which is great for the kinds of projects that Apache was interested in.

And Apache has become a home for over 300 different individual software development projects, beyond the web server, right?

But it has always grown by happenstance, and it's always been open to whatever technology project wanted to come in.

There are some upsides and downsides to that all, right?

One of the downsides is, by not having a full time staff, it's hard for Apache to really take advantage of all the opportunities out there, to get the word out about who they are.

It means that developers, you know, have to do these non-developer activities, right?

And it's hard to do things like police your trademark usage, right, when people are working as volunteers.

The Linux Foundation took a slightly different approach.

The Linux Foundation said "We don't..." You know, just like with Apache, "we don't want to write software, we don't want to have to pay all the software developers", because there's actually a lot to the validity that comes from all of the software development happening by volunteers, but there's a lot of non-software development things: marketing, legal, PR, and even the hosting of meetings, the hosting of phone calls, all of the logistics of helping these communities operate that perhaps can be taken on, right, by a full-time staff.

Now, how do you pay that staff, right? You could ask for, you know, cutting charity contributions, right?

But, a better, more scalable approach is to ask companies to join as corporate members of an organization, right?

And, they don't get any special privileges on the code, right?

Well, they don't get their patches in by default, they don't get to veto anyone else's work.

If you're a developer from IBM, there's no special status.

You have to still prove your worth, and to which, you would, you know, and be seen as a peer to, say, a 15 year old kid in Romania, who also is really eager to work on distributed ledgers and smart contract systems.

What members do get is some help in marketing their activities, building on top of Hyperledger projects, ways to participate at the events that we do.

When a journalist calls us and asks us for a story about somebody doing something interesting with Hyperledger, we've got a set of members that we... whose stories we can draw from, right?

This balancing act of, you know... as I mentioned, there's a developer community, and there's a commercial community, a corporate community...

That's the balancing act... that The Linux Foundation has really developed a process for, a template for, and a real science around, and that's what we're bringing to bear on the Hyperledger project.

### Interoperability Between Hyperledger Frameworks

What do you think will help foster interoperability between these three different Hyperledger frameworks?

There's a number of things that we can do to assist in the interoperability between the different projects at Hyperledger.

One thing we're working on is kind of an overall architectural view of all the different projects, right?

What are the technologies that sit at kind of the DLT layer, at the smart contract layer, where does identity sit in, right?

And then, we can start to look at these projects and go, "Okay, could we put Fabric down here, could we put Burrow up here?"

Maybe we start to tease apart the distributed ledger part of Fabric from the smart contract part of Fabric, right, into separate components, so that, when somebody new arrives at the project, or they take a training course like this, they can start to pick and choose, you know, as building blocks, as appropriate for whatever use case that they want to target, right?

That's something over time, this kind of modularity approach... Along with that, defining standardized APIs between these different levels, right, so that we can get to an ideal, where you could pick the Ethereum virtual machine from Burrow, and run that on top of Fabric or on top of Sawtooth, and, in fact, the Sawtooth and Burrow communities have now actually progressed, and you can now run Ethereum smart contracts on top of Sawtooth, which is pretty cool.

I think we'll see more activity like that.

## Chapter 3: Hyperledger: Distributed Ledger Framework & Domain-Specific Blockchains

In this chapter, we will briefly explore the frameworks developed under the Hyperledger umbrella (as of November 2020), highlighting their key features and use cases. We will dive deeper in discussing use cases in the last chapter of this course.

### Learning Objectives

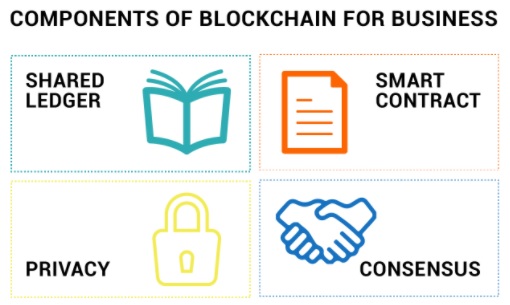
By the end of this chapter, you should be able to:

* List the components of Hyperledger frameworks.
* Get a high-level understanding of the Hyperledger frameworks and domain-specific blockchain technologies: Hyperledger Besu, Hyperledger Burrow, Hyperledger Fabric, Hyperledger Grid, Hyperledger Indy, Hyperledger Iroha, and Hyperledger Sawtooth.

### Components of Hyperledger Frameworks

Hyperledger business blockchain frameworks are used to build enterprise blockchains for a consortium of organizations. They are different than public ledgers like the Bitcoin blockchain and Ethereum. Hyperledger frameworks include:

* An append-only distributed ledger
* A consensus algorithm for agreeing to changes in the ledger
* Privacy of transactions through permissioned access
* Smart contracts to process transaction requests.



Now, let's explore the Hyperledger frameworks (as of November 2020)!

## Hyperledger Besu



[Hyperledger Besu](https://www.hyperledger.org/use/besu) is an open source Ethereum client developed under the Apache 2.0 license and written in Java. It can be run on the Ethereum public network or on private permissioned networks, as well as 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. Hyperledger Besu joined the Hyperledger Incubator in August 2019; PegaSys has been its primary contributor and maintainer since its launch in November 2018, when it was known as Pantheon.

Among its features:

* Implements the [Enterprise Ethereum Alliance](https://entethalliance.org/) (EEA) specification
* The Ethereum Virtual Machine (EVM), which allows deployment and execution of smart contracts via transactions within an Ethereum blockchain
* Implements various consensus algorithms, such as Proof of Authority (with several protocols, such as IBTF 2.0 or Clique) and Proof of Work (Ethash)
* Uses a RocksDS key-value database to persist chain data locally
* P2P networking
* Provides user-facing APIs
* Allows you to monitor node and network performance
* Ability to keep transactions private between the involved parties
* Allows permissioning.

### Hyperledger Burrow



Welcome to the Hyperledger greenhouse, an open source consortium for developing business blockchain technologies hosted by the Linux Foundation.

Within the greenhouse, diverse global communities collaboratively develop open source projects that uniquely approach enterprise blockchain challenges.

These technologies can cross-pollinate and interoperate, just like how the community is driving the projects, collaborate in an open and neutral environment.

Hyperledger Burrow is a modular blockchain framework in the Hyperledger greenhouse, with a permissioned smart contract interpreter, developed partly to the specifications of the Ethereum Virtual Machine.

Smart contracts provide the base functionality and computational muscle within blockchain networks.

Smart contracts are written into lines of code, and distributed across blockchain networks.

They can be configured to manage processes, exchange value, or perform calculations, all without intermediaries.

Because of its lightweight and fast smart contract design, and the Byzantine fault tolerant consensus algorithm with transaction finality,

Burrow is optimized for sharing processes across organizations.

Burrow operates as Hyperledger's library for Ethereum Virtual Machine-based smart contracts.

If you wrote Solidity contracts for the public Ethereum network, Hyperledger Burrow allows you to bring those smart contracts over to Hyperledger.

Burrow helps organizations better meet their cross-functional business needs, and opens the door for other Hyperledger projects to incorporate the Ethereum Virtual Machine into their platforms.

Get started with Hyperledger Burrow today, by downloading the source code, accessing the documentation, and joining our community from our website: hyperledger.org.

[Hyperledger Burrow](https://www.hyperledger.org/projects/hyperledger-burrow) was released in December 2014. It was originally designed by Monax, and co-sponsored by Intel. The project is generally updated on a quarterly basis, and is licensed under the [Apache 2.0. license](https://www.apache.org/licenses/LICENSE-2.0). Currently under incubation, "Hyperledger Burrow is a complete single-binary blockchain distribution focussed on simplicity, speed, and developer ergonomics. It supports both EVM and WASM based smart contracts and uses BFT consensus via the Tendermint algorithm".

Hyperledger Burrow components are:

* **Consensus Engine** - Hyperledger Burrow uses the Byzantine fault-tolerant [Tendermint protocol](https://tendermint.com/) to order and finalize transactions
* The **API Gateway** provides interfaces for systems integration and user interfaces
* The **Smart Contract Application** engine facilitates integration of complex business logic (maintaining the networking stack between the nodes and ordering transactions)
* **Permissioned Ethereum Virtual Machine** - it is built to observe the Ethereum operation code specification, and asserts the correct permissions have been granted
* **Application Binary Interface** (ABI) - transactions must be formulated in a binary format, which is processed by the blockchain node.
* The **Application Blockchain Interface** (ABCI) provides interface specification for the consensus engine and smart contract application engine to connect.

### Hyperledger Fabric



Welcome to the Hyperledger greenhouse, an open source consortium for developing business blockchain technologies hosted by the Linux Foundation.

Within the greenhouse, diverse global communities collaboratively develop open source projects that uniquely approach enterprise blockchain challenges.

These technologies can cross-pollinate and interoperate, just like how the community is driving the projects collaborate in an open and neutral environment.

Hyperledger Fabric is an enterprise-grade, permissioned distributed ledger platform in the Hyperledger greenhouse that offers modularity and versatility for a broad set of industry use cases.

The modular architecture for Fabric accommodates the diversity of enterprise use cases through plug-and-play components, such as consensus, privacy, and membership services.

One of the many compelling Fabric features is the enablement of a network of networks.

Members of a network work together, but because businesses need some of their data to remain private, they often maintain separate relationships within their networks.

Rather than an open, permissionless system, Fabric offers a modular, scalable and secure platform that supports private transactions and confidential contracts.

Fabric helps members manage confidential obligations to each other without first passing it through a central authority.

That way, personal data isn't available to the entire network.

If a member is not an agreed-upon party, the transaction shouldn't appear on their ledger.

This architecture allows for solutions developed with Fabric to be adapted for any industry, thus ushering in a new era of trust, transparency, and accountability for businesses.

Get started with Hyperledger Fabric today by downloading the source code, accessing the documentation, and joining our community from our website:

hyperledger.org.

[Hyperledger Fabric](https://www.hyperledger.org/projects/fabric) is an open source, production ready, permissioned blockchain framework implementation that was designed to serve as a foundation for developing applications or solutions with a modular architecture. It was the first proposal for a codebase (2016), combining previous work done by Digital Asset Holdings, Blockstream's libconsensus, and IBM's OpenBlockchain. It graduated from the Hyperledger Incubator in March of 2017.

Key characteristics of Hyperledger Fabric are:

* High-performance, secure, permissioned blockchain network
* Features powerful container technology to host any mainstream language for smart contracts development
* Code written in Go, chaincode written in Go, Javascript, or Java, SDKs written in Node.js, Java, Go, REST and Python.

Its modular architecture allows components such as consensus and membership services to be plug-and-play. One of the key advantages of Hyperledger Fabric is that it allows entities to conduct confidential transactions without passing information through a central authority. This is accomplished through different channels that run within the network, as well as the division of labor that characterizes the different nodes within the network.

### Hyperledger Indy



Welcome to the Hyperledger greenhouse, an open source consortium for developing business blockchain technologies hosted by the Linux Foundation.

Within the greenhouse, diverse global communities collaboratively develop open source projects that uniquely approach enterprise blockchain challenges.

These technologies can cross-pollinate and interoperate, just like how the community is driving the projects, collaborate in an open and neutral environment.

Hyperledger Indy, one of the frameworks in the Hyperledger greenhouse, is a distributed ledger that provides tools, libraries, and reusable components for creating and using independent decentralized identities.

As the world becomes more interconnected, individuals are disclosing personal information creating multiple usernames and passwords and leaving digital traces across platforms.

Indy represents the idea of a self-sovereign identity, which would dispose of the need for multiple logins and passwords.

Rooted on a distributed ledger, this digital identity interoperates across different domains, applications and organizational silos.

Additionally, Indy puts identity control in the hands of the user, not the organization.

Individuals will not have to rely on big organizations to store and share their personal data.

Instead, the user controls what data they want to provide access to and for how long.

Indy provides strong privacy guarantees because private data is not written on the ledger, but exchanged over peer-to-peer encrypted connections.

A unique ID for each relationship ensures that data doesn't leak from one relationship to the next.

Indy also ensures that both individuals and institutions always know who they are dealing with.

Companies can store less personal data and spend less time and money trying to protect it.

This combination of privacy and trust enables meaningful interactions.

By providing a solution for digital credentials that preserves privacy, Indy makes self-sovereign identities possible and practical for individuals, institutions and Internet of Things.

Get started with Hyperledger Indy today by downloading the source code, accessing the documentation and joining our community from our website: hyperledger.org.

The Hyperledger consortium has many different projects that focus on different aspects of how ledgers can work and what use cases they can be applied for.

Hyperledger Indy is a distributed ledger purpose-built for doing distributed identity, and what that means is, it allows you to have a route of trust to manage the keys, schemas, proofs, and other information that you need to, in order to enable trusted peer interactions between different identities, as stored on a Hyperledger Indy blockchain instance.

If you have an identity it belongs to you, and only you, and no one can pull the plug on you.

And you can use that identity to manifest different correlatable pieces of data between you and other identities you want to interact with, without leaking private information or disclosing information that you don't want shared across all those different aspects of who you are.

And when you control your identity, it makes it so that you are also a party to the kinds of data sharing, claims, and proofs that can be made about you, as information is shared across all the different interactions you might do online.

One of the main use cases of Hyperledger Indy is to create a global public utility for identity that's being created by the Sovrin Foundation, which allows us to take these identifiers, and to anchor them on a public ledger, so that different pieces of truth or pieces of information can be trusted and shared with other people across the world, and they can be trusted and validated, so that self-attested data can be shared, as well as third-party attestations can be shared across all kinds of interactions and across all kinds of data silos, and what this makes possible is the ability to no longer have to function as an identity provider as a business, but to rather let users authenticate based on the attributes that they're willing to store and share themselves, which allows for GDPR-compliant use cases, where you're expressing consent on behalf of the user, and also reducing the amount of liability contained within a business, because the data can be kept with the user and presented to you again in a way that you can trust and validate, that what has been said, really was said, and is trusted by the other parties you do business with.

[Hyperledger Indy](https://www.hyperledger.org/projects) is a distributed ledger purpose-built for decentralized identity, that upholds the standards mandated by [GDPR](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en). Hyperledger Indy "provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo."

Hyperledger Indy was contributed to the Hyperledger greenhouse by the Sovrin Foundation in 2017, and it graduated from the Incubator in March of 2019. It allows individuals to manage and control their digital identities. Rather than having businesses store huge amounts of personal data of individuals, Hyperledger Indy allows businesses to store pointers to identity. Once the company verifies the other party's identity, it throws it away.

According to Brian Behlendorf,

"(...) identity is a toxic asset that could present a liability to organizations".

Indeed, since 2013, over 14 billion data records were lost or stolen. What is striking is that, out of these, only 4% were encrypted, and hence, rendered useless after being stolen (also called "secure breaches"). You can find detailed statistics at the [Breach Level Index website](https://breachlevelindex.com/).



One of the key principles of Hyperledger Indy is its "[privacy by design](https://en.wikipedia.org/wiki/Privacy_by_design)" approach. Given the immutable nature of the DLT, it is all the more important that digital identities be handled with the utmost care, keeping human values front and center.

"Hyperledger Indy lets users authenticate identity based on the attributes they are willing to store and share themselves. This can reduce the amount of liability contained within a business because the data can be kept with the user and presented to you again in a way that you can trust and validate that what has been said really was said and is trusted by the other parties you do business with".  
- Nathan George, Maintainer, Hyperledger Indy

Further information about the history of the project can be found at the [Sovrin's website](https://sovrin.org/" \t "_blank).

### Hyperledger Iroha



Welcome to the Hyperledger greenhouse, an open source consortium for developing business blockchain technologies hosted by the Linux Foundation.

Within the greenhouse, diverse global communities collaboratively develop open source projects that uniquely approach enterprise blockchain challenges.

These technologies can cross-pollinate and interoperate, just like how the community is driving the projects collaborate in an open and neutral environment.

Hyperledger Iroha is a permissioned blockchain framework in the Hyperledger greenhouse designed for simple and easy management of digital assets.

Iroha helps bring greater trust and reliability into business.

Only participants granted access to a Hyperledger Iroha network may join the network, query data, or perform commands.

Iroha' robust permission system ensures that all interactions within the system are secure and controlled.

Iroha's features are helpful for creating applications for end users.

With Iroha, a business can create and manage simple or complex digital assets, from cryptocurrency to personal medical data.

Iroha's built-in smart contracts, called commands, allow developers to incorporate blockchain into their business processes.

Iroha presents users with lower complexity and lower risk by allowing them to perform common functions using built-in commands.

This simplifies tasks, improves performance efficiency, and allows less room for error.

Compared to other platforms, these commands also free up developers by ridding them of the need to write complex smart contracts.

In Iroha, you can set up a network, create assets, and make a transaction in about 5 minutes time.

Iroha's consensus algorithm allows full Byzantine fault tolerance with no mining, making it ideal for businesses that require verifiable data consistency at low cost.

Users are able to interact with Iroha similarly to how they would with a client server, so while some knowledge is required, you don't need to be a blockchain guru to incorporate Iroha into your business.

Get started with Hyperledger Iroha today by downloading the source code, accessing thedocumentation and joining our community from our website:

### hyperledger.org.

[Hyperledger Iroha](https://hyperledger.org/projects/iroha) is a free, open source blockchain framework contributed by Soramitsu, Hitachi, NTT Data, and Colu (2016). Hyperledger Iroha is a simple blockchain platform that can be used to make trusted, secure, and fast applications that leverage the power of permission-based blockchain with Byzantine fault-tolerant consensus. Among its key features are:

* Simple deployment and maintenance
* Variety of libraries for developers
* Role-based access control
* Modular design, driven by command-query separation principle
* Ready-to-use set of commands and queries
* Multi-signature transactions
* Uses a high-performance Byzantine fault-tolerant consensus algorithm called [YAC](https://iroha.readthedocs.io/en/latest/architecture/index.html#block-consensus-yac).

According to the [Hyperledger Iroha documentation](https://iroha.readthedocs.io/en/latest/overview.html), "it can be used to manage digital assets, identity and serialized data, and can be useful for applications such as interbank settlement, central bank digital currencies, payment systems, national IDs, and logistics, among others". Its documentation provides an extensive list of use cases, and specific advantages the use of Hyperledger Iroha can introduce - you can read about these [use case scenarios](https://iroha.readthedocs.io/en/latest/use_cases/index.html) online.

Hyperledger Iroha emphasizes mobile application development with client libraries for Android and iOS, making it distinct from other Hyperledger frameworks. Inspired by Hyperledger Fabric, Hyperledger Iroha seeks to complement Hyperledger Fabric and Hyperledger Sawtooth, while providing a development environment for C++ developers to contribute to Hyperledger.

Hyperledger Iroha is an active project, and reached a significant milestone in May 2019, the 1.0 release. To learn more about it, you can read the [announcement](https://www.hyperledger.org/announcements/2019/05/06/hyperledger-launches-hyperledger-iroha-1-0).

### Hyperledger Sawtooth

Welcome to the Hyperledger greenhouse, an open source consortium for developing business blockchain technologies hosted by the Linux Foundation.

Within the greenhouse, diverse global communities collaboratively develop open source projects that uniquely approach enterprise blockchain challenges.

These technologies can cross-pollinate and interoperate, just like how the community is driving the projects collaborate in an open and neutral environment.

Built from the ground up for enterprise use, the Hyperledger Sawtooth design philosophy targets development of decentralized ledgers and secure, scalable smart contracts.

The Sawtooth security model uses a single node type, which simplifies deployment.

Plenty of examples exist for both on-prem and cloud installations.

On chain governance lets enterprises manage all aspects of the Sawtooth network with the network itself.

Participants add policies and agree on configuration changes using Sawtooth transactions.

In fact, even consensus algorithms can be changed real time in a running network: start with Raft, them harden with PBFT, or switch to Proof of Elapsed Time as the network grows.

Sawtooth software development kits cover a wide variety of languages.

The smart contract model supports deploying any and all of these languages alongside each other.

Ethereum contracts, for example, can be deployed alongside WebAssembly and Java contracts.

Sawtooth distributed ledger technology can integrate with existing internal databases by keeping internal relational and key/value databases in sync with the Sawtooth network.

Whether you are using Sawtooth for healthcare, supply chain, or financial services, your internal systems can make use of all the data managed on the Sawtooth blockchain.

Get started with Hyperledger Sawtooth today by downloading the source code, accessing the documentation and joining our community from our website:

hyperledger.org.

[Hyperledger Sawtooth](https://www.hyperledger.org/projects/sawtooth), is an open source blockchain framework that utilizes a highly modular platform for building, deploying, and running distributed ledger applications and networks, making smart contracts safe, particularly for enterprise use. It was originally contributed by Intel and joined the Hyperledger greenhouse in April of 2016. In May of 2018 it graduated from the Hyperledger Incubator.

Some of its key characteristics are:

* Uses pluggable consensus algorithms, which allows consensus to be changed by transaction on the fly
* Smart contracts can be written in almost any language
* Parallel transaction execution for added throughput, while at the same time preventing double spending
* Ethereum contract support via Hyperledger Burrow integration
* No central authority or implementation. This increases security as there is no centralized service that could leak transaction patterns or any other confidential information
* Supports creating and broadcasting events.

Distributed ledger solutions built with Hyperledger Sawtooth can utilize various consensus algorithms based on the size of the network (PoET SGX, Raft, etc.). Hyperledger Sawtooth is designed for versatility, with support for both permissioned and permissionless deployments. This technology simplifies blockchain application development and deployment by clearly separating the core system from the application domain.



### Hyperledger Sawtooth Characteristics Relative to Use Cases (Dan Middleton)

Unique characteristics of Sawtooth... There's several, but one that comes to mind for a provenance or supply chain use case, is that that network will probably grow over time.

The reason that a lot of us are starting blockchain networks, a lot of companies are invested in looking at blockchain networks, because we think that we're going to be in them for a long time and they're going to continue to grow.

Sawtooth is designed so that you can grow the size of the network, you can actually change the consensus mechanism on the fly...

I think this is a unique characteristic of Sawtooth amongst all of the other ledgers...you can submit as a transaction and then have a policy within your network to accept that new consensus, and then, your network can move from say a PBFT-style consensus to something like PoET, or some sort of random leader election consensus...

It allows you to have tens, or hundreds, or potentially thousands of different nodes on your network, and you really can't beat that kind of availability and integrity guarantees, or that kind of flexibility for a network that needs to be up for years.

### Hyperledger Sawtooth - Supply Chain Use Case Example (Courtesy of Sawtooth)

Meet Rich: he owns a popular seafood restaurant in Boston, Massachusetts.

Rich strives to serve only the freshest, highest quality fish to his patrons, but he often has difficulty knowing exactly where it was caught, how it got to his restaurant, or if it's even the right species of fish.

From ocean to table, the fish supply chain is difficult to track, and usually follows this pattern: the fish is caught by a commercial fisherman in the ocean, the fisherman then sells the fish to a market, processor, or broker, a distributor then transports the fish to a restaurant or grocery store for a consumer to purchase.

Rich typically only buys from one or two fish distributors that he has built a foundation of trust and personal history with.

He'd like to expand his menu by adding some different kinds of seafood from other distributors, but he worries about integrity, and for good reason.

He recently read a study by Oceana, which showed that 33% of fish purchased from retail outlets is incorrectly labeled, and that illegal fishing represents losses between 10 to 23 billion dollars worldwide.

Rich knows that mislabeled and illegally sourced fish could hurt his customers, his restaurant's reputation, and the environment of our planet.

Fortunately for Rich and others in the seafood industry,

Sawtooth Lake blockchain technology can provide an immutable record of the provenance and lineage of various goods, like fish.

In combination with Internet of Things-enabled sensors, Sawtooth Lake can manage the ownership and journey of fish from ocean to table.

Sensors can be attached to fish the moment they are harvested, immediately and continuously recording data such as the location and temperature of the fish.

Now, Rich can validate when and where his fish was caught, and that it was stored properly on ice while it was transported.

The Sawtooth Lake platform can also manage the Chain of Custody fish, enabling ownership to be transferred and traded on the blockchain according to smart contracts.

With Sawtooth Lake as a traceability blockchain, Rich can easily see which fishermen meet his quality standards and feels comfortable doing business with new tradesmen.

When he serves up a new special to a cherished customer, he can confidently and accurately assure her it's the type of fish she ordered, it was stored at safe temperatures, when and where it was caught, how long it took to get to her plate, and the fish's name... just kidding.

Sawtooth Lake blockchain technology can be used for a wide variety of applications, from capital markets to international trade.

The Internet of Things ties the physical world to the digital world, with Sawtooth Lake recording the generated data in a way that all parties can trust its accuracy and completeness.

This is extremely useful for tracking perishable goods, like fish.

These sensors can track many key parameters, such as location, temperature, humidity, motion, shock, and tilt.

This technology could be added to any package or sensitive good you're entrusting to other parties.

The blockchain will ensure the data is secure and tamper-proof, so that you know what you're getting, and that you get what you pay for.

Sawtooth Lake creates a digital platform enabling physical traceability in a trustless world.

### Hyperledger Grid



[Hyperledger Grid](https://www.hyperledger.org/use/grid) is a domain-specific business blockchain technology for building supply chain solutions that include distributed ledger components; it's an ecosystem of technologies, frameworks, and libraries that work together, allowing application developers to chose which components are best for their industry or market model. It intends to:

* Provide reference implementations of supply chain-centric data types, data models, and smart contract-based business logic based on existing open standards and industry best practices
* Provide authentic, practical ways to combine components from the Hyperledger Stack into a single, effective business solution.

Hyperledger Grid was accepted in the Hyperledger Incubator as of December 2018, with Cargill, Intel and Bitwise as primary contributors to this initial stage. Its software is licensed under the Apache License Version 2.0.

Hyperledger Grid incorporates several GS1Standards concepts in an effort to put structure around static and dynamic data and increase visibility, standardization, consistency, credibility, neutrality and interoperability:

* Global Trade Item Number (GTIN) - this is a unique product identifier with a critical role in global commerce, composed of numbers that identify the company making the product, as well as numbers identifying the product. A product that has its own GTIN retains an identity regardless of where it is in the supply chain, and this is key for blockchain implementation.
* Global Location Numbers (GLN) - These are numbers that uniquely identify organizations and locations in the supply chain, and contribute to enhanced visibility in the supply chain.
* GS1 barcodes - These barcode labels must be captured in order to allow data to be shared among trading partners. They provide product specific information and allow real-time view of where the products have been and where they are going.
* Electronic Product Code Information Services (EPCIS) - This is similar to a standardized API, capturing and sharing information about the movement and status of products, logistic units, and other assets in the supply chain.

You can learn more about Hyperledger Grid from its website and [wiki](https://wiki.hyperledger.org/display/GRID/Hyperledger+Grid) pages, where more resources are provided as well.

## Chapter 4: Hyperledger Tools

The Hyperledger frameworks which we examined in the previous chapter are used to build blockchains and distributed ledgers. The Hyperledger tools, which we will look at next, are auxiliary softwares used for things like deploying and maintaining blockchains, examining the data on the ledgers, as well as tools to design, prototype, and extend blockchain networks.

### Learning Objectives

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

* Understand the role of Hyperledger tools.
* Get a high-level understanding of the Hyperledger tools (as of November 2020): Hyperledger Avalon, Hyperledger Cactus, Hyperledger Caliper, Hyperledger Cello, Hyperledger Explorer.

### Hyperledger Avalon



[Hyperledger Avalon](https://www.hyperledger.org/use/avalon) is a ledger independent implementation of the [Off-Chain Trusted Compute Specification](https://entethalliance.github.io/trusted-computing/spec.html) published by the Enterprise Ethereum Alliance (EEA). It joined the Hyperledger Incubator in October of 2019, bringing together sponsorship from Intel, iExec Blockchain Tech, Alibaba Cloud, Baidu, BGI, Chainlink, Consensys, EEA, Espeo, IBM, Kaleido, Microsoft, Banco Santander, Wipro, Oracle, and Monax. It aims to enable the secure movement of blockchain processing off the main chain to dedicated computing resources. Avalon is designed to help developers gain the benefits of computational trust and mitigate its drawbacks. It is released under the Apache License Version 2.0.

Hyperledger Avalon:

* Enables developers to accelerate throughput and improve data privacy
* The initial implementation of Hyperledger Avalon uses Intel Software Guard Extensions (SGX)
* Uses the Off-Chain Trusted Compute Specification as a starting point to apply a consistent and compatible approach to all supported blockchains.

You can learn more about Hyperledger Avalon from Eugene (Yevgeniy) Yarmosh's [An Introduction to Hyperledger Avalon](https://www.youtube.com/watch?v=I16EhP23HTg) presentation.

### Hyperledger Cactus



[Hyperledger Cactus](https://www.hyperledger.org/use/cactus) is an open source project jointly contributed by Accenture and Fujitsu; it joined the Hyperledger Greenhouse in May 2020. Formerly known as the Blockchain Integration Framework, this blockchain integration tool aims to provide decentralized, secure and adaptable integration between blockchain networks. Developers are currently working on refactoring the Hyperledger Cactus architecture to ensure it will enable plug-in based collaborative development, thus increasing the breadth of use cases and ledgers supported. Hyperledger Cactus is licensed under an Apache License Version 2.0.

To learn more about Hyperledger Cactus, you can watch Peter Somogyvari's[***Hyperledger Cactus - A Framework for Integrating Distributed Ledgers***](https://www.youtube.com/watch?v=IHy-5sbMrYs) presentation.

### Hyperledger Caliper



Welcome to the Hyperledger greenhouse, an open source consortium for developing business blockchain technologies hosted by the Linux Foundation.

Within the greenhouse, diverse global communities collaboratively develop open source projects that uniquely approach enterprise blockchain challenges.

These technologies can cross-pollinate and interoperate, just like how the community is driving the projects collaborate in an open and neutral environment.

Hyperledger Caliper is a blockchain benchmark tool in the Hyperledger greenhouse that measures the performance of various blockchain systems by using a set of predefined cases.

Most users feel concerned or at least curious about the performance of their blockchain solution.

However, until now, there has not been a commonly accepted blockchain benchmarking tool.

Caliper brings to market the first tool that uses a set of neutral and agreed upon rules to evaluate differing blockchain solutions.

In addition to a customizable test flow and workload, Caliper produces reports that contain performance indicators such as resource utilization, transaction latency, and transactions per second, or TPS.

Every blockchain system today offers its unique strengths.

Caliper allows users to understand the solutions that best meet their use cases.

Blockchain developers can also use Caliper as an internal tool to test the performance of different development versions, and since the performance of blockchain systems varies within different configurations, Caliper will be able to help users decide which configuration best suits their needs.

Get started with Hyperledger Caliper today by downloading the source code, accessing the documentation and joining our community from our website: hyperledger.org.

Currently in incubation***,***[***Hyperledger Caliper***](https://www.hyperledger.org/projects/caliper) was initially contributed in 2018 by developers from Huawei, Hyperchain, Oracle, Bitwise, Soramitsu, IBM and the Budapest University of Technology and Economics. It references the definitions, metrics and terminology defined by the Performance and Scalability Working Group.

Some of the project's key characteristics are:

* Unified blockchain benchmark framework
* Commonly accepted definition of performance indicators
* Commonly accepted benchmark cases.

As of November 2020, it supports the following blockchain solutions: Hyperledger Besu, Hyperledger Burrow, Ethereum, Hyperledger Fabric, FISCO BCOS, Hyperledger Iroha and Hyperledger Sawtooth.

Hyperledger Caliper is a blockchain benchmark tool, which allows users to measure the performance of a specific blockchain implementation with a set of predefined use cases.

### Hyperledger Cello



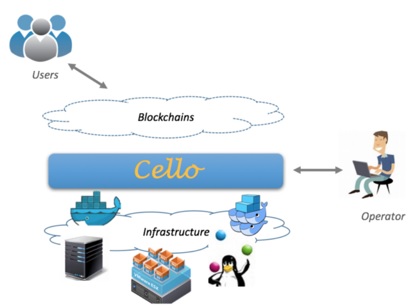
[Hyperledger Cello](https://www.hyperledger.org/projects/cello) is a blockchain module toolkit helping businesses use and manage blockchains in a more efficient way. Particularly for lean businesses and small enterprises, who want to reduce or eliminate the effort required in creating, managing, and terminating blockchains, Hyperledger Cello allows blockchains deployment to the cloud. Operators can create and manage such blockchains through a dashboard, and users (typically, chaincode developers) can obtain a blockchain instance immediately.

Currently in Incubation, *"Cello aims to bring the on-demand 'as-a-service' deployment model to the blockchain ecosystem"*, thus helping in furthering the development and deployment of Hyperledger's frameworks. Hyperledger Cello was initially contributed by IBM, with sponsors from Soramitsu, Huawei, and Intel (2017).

Application developers and system administrators using Cello can provision and maintain Hyperledger networks. For instance, you can create a group of distributed ledger networks in virtual clouds known as 'container clusters', and then, manage and monitor those networks with a configurable dashboard. Additionally, you can build a Blockchain-as-a-Service (BaaS) platform.

Some key features are:

* Deploy, manage and operate blockchains efficiently and automatically
* Support customized blockchain requests (support for Hyperledger Fabric)
* Support various infrastructures (baremetal, VM platforms, container cloud)
* Support advanced operational analytics for system status and ledger behavior



**Hyperledger Cello**  
(Source: <https://www.hyperledger.org/blog/2017/01/17/hyperledger-says-hello-to-cello>)

### Hyperledger Explorer



[**Hyperledger Explorer**](https://www.hyperledger.org/use/explorer) is a simple, but powerful open source tool for visualizing blockchain operations. It is the first tool to examine permissioned ledgers, allowing anyone to explore the distributed ledger projects being created by Hyperledger's members from the inside, without compromising their privacy. Currently in Incubation, the project was contributed by DTCC, Intel, and IBM in 2016.

Designed to create a user-friendly web application, Hyperledger Explorer can view, invoke, deploy, or query:

* Blocks
* Transactions and associated data
* Network information (name, status, list of nodes)
* Smart contracts (chain codes and transaction families)
* Other relevant information stored in the ledger.

The ability to visualize data is of critical importance, in order to extract business value from it. Hyperledger Explorer provides this much needed functionality. Key components include a web server, a web UI, web sockets, a database, a security repository, and a blockchain implementation.

Hyperledger Explorer supports Hyperledger Fabric and Hyperledger Iroha.

## Chapter 5: Hyperledger Libraries

In the previous chapter we looked at the Hyperledger tools, which are auxiliary software used for things like deploying and maintaining blockchains, examining the data on the ledgers, as well as tools to design, prototype, and extend blockchain networks. In this chapter we will take a look at the Hyperledger libraries for enterprise-grade blockchain deployments.

### Learning Objectives

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

* Understand the role of Hyperledger libraries.
* Get a high-level understanding of the Hyperledger libraries (as of November 2020): Hyperledger Aries, Hyperledger Quilt, Hyperledger Transact, and Hyperledger Ursa.

### Hyperledger Aries



[**Hyperledger Aries**](https://www.hyperledger.org/projects/aries) "provides a shared, reusable, and interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials. It is infrastructure for blockchain-rooted, peer-to-peer interactions; it's not a blockchain and it's not an application. This open source project joined the Hyperledger greenhouse in May 2019 and was initially contributed by developers from the Sovrin Foundation, the Government of British Columbia, and other Indy community developers.

Hyperledger Aries is related to both Hyperledger Indy and Hyperledger Ursa (we will talk about this project later in this chapter). This project aims "to change the client layers in Hyperledger Indy to be interoperable with other identity projects. The ultimate goal of Hyperledger Aries is to provide a dynamic set of capabilities to store and exchange data related to blockchain-based identity. These capabilities will range from the secured, secret storage of data such as private keys, up to the capability of globally accessible data that can be viewed and accessed by anyone. An example of such support is the creation of a secure storage solution similar to the wallet available in Hyperledger Indy today."

Hyperledger Aries developers aim to eventually have a scalable, searchable storage layer capable of storing other associated data necessary for identity maintenance, such as pictures, health records, or other personal information.

### Hyperledger Quilt



Welcome to the Hyperledger greenhouse, an open source consortium for developing business blockchain technologies hosted by the LinuxFoundation.

Within the greenhouse, diverse global communities collaboratively develop open source projects that uniquely approach enterprise blockchain challenges.

These technologies can cross pollinate and interoperate just like how the community's driving the projects collaborate in an open and neutral environment.

Hyperledger Quilt is a toolset in the Hyperledger greenhouse that offers interoperability between ledger systems by implementing the Interledger Protocol, or ILP, which is primarily used to transfer value across distributed and non-distributed ledgers.

Today, value transfers are relatively easy if the sender and recipient reside in the same country or own accounts in the same network.

However, since ledger systems are often siloed and disconnected, problems arise when transferring value to a different payment network.

As an enterprise-grade implementation of the ILP protocol, Quilt can facilitate interoperability between different networks and values by providing libraries and reference implementations of the core interledger components.

With ILP, money can be packetized, routed, and delivered over communication networks with automatic routing and a series of secure, multi-hop payments, connecting bank accounts to digital wallets and everything in between.

Long term, Quilt can become a ledger interoperability solution that enables more than just payment transactions, but a means to exchange any sort of asset across the many different blockchain networks that will exist.

Get started with Hyperledger Quilt today by downloading the source code, accessing the documentation, and joining our community from our website:

* hyperledger.org.
* [Hyperledger Quilt](https://www.hyperledger.org/projects/quilt) is an open source business blockchain tool that offers interoperability between ledger systems. It is a Java implementation of the Interledger protocol (ILP)  (which is primarily a payments protocol designed to transfer value across distributed ledgers and non-distributed ledgers). Among its key characteristics are:
* Provides a set of rules for enabling ledger interoperability with basic escrow semantics
* Furnishes a standard for ledger-independent address and data packet formats that enable connectors to route payments
* Supplies a framework for designing higher-level use case specific protocols.
* Currently in Incubation, Hyperledger Quilt was initially contributed by NTT Data and Ripple in 2017.

### Hyperledger Transact



[Hyperledger Transact](https://www.hyperledger.org/use/transact) is a transaction execution platform designed to be used as a library or as a component when implementing distributed ledger, including blockchains. Hyperledger framework-level projects and custom distributed ledgers can make use of Transact's advanced transaction execution and state management to simplify the transaction execution code required within their projects or to gain additional features. Transact provides an extensible approach to implementing new smart contract languages called smart contract engines.

Currently in Incubation, it was originally contributed by Bitwise, Cargill, Intel, IBM and Hacera in 2019. Some of the following features are already supported by Hyperledger Transact, or planned in the short-term:

* Serial and parallel transaction scheduling
* Pluggable state backend
* Transaction receipts
* Events that can be generated by smart contracts
* Support for Sabre and Seth, etc.

### Hyperledger Ursa



[Hyperledger Ursa](https://www.hyperledger.org/projects/ursa) is a shared cryptographic library that would enable people and projects to avoid duplicating existing cryptographic work and hopefully increase security in the process. Rather than having each Hyperledger project implement its own cryptographic protocols, it would be more desirable to collaborate on a shared library - this will simplify cross-platform interoperability and increase modularity for distributed ledger platforms.

In the long run, the goal is for Hyperledger Ursa to provide open source blockchain developers with reliable, secure, easy-to-use, and pluggable cryptographic implementations.

The project was proposed by Fujitsu, The Linux Foundation, Sovrin Foundation, Intel, DFINITY, State Street, IBM, Sai Infratel, and Bitwise, and is currently in incubation (since November 2018).

## Chapter 6: The Promise of Business Blockchain Technologies

This chapter is designed to help you evaluate whether blockchain tech, including the Hyperledger frameworks, are right for your business, and where best to implement this new technology. We will cover the ways different industries are using blockchain technologies today, and show you some common features of blockchains that can provide efficiencies in business.

The finance industry, in particular, put a lot of resources behind blockchain tech early on. They have created blockchains and distributed ledgers for transferring assets and recording trade agreements. Many types of transactions, such as private company stock sales, bonds, options, and cash transactions have all been recorded on permissioned blockchains.

Blockchain technologies are very good at recording state transitions. Just as the finance industry uses blockchain to record who owns an asset at any given moment in time, the legal industry has also implemented blockchain technologies to record property rights and the transfer of those rights. It will be interesting to see how the courts adapt to recording contractual agreements on both public and permissioned blockchains going forward.

Insurance companies act as a trusted intermediary, pooling funds from unaffiliated individuals. By holding these funds, they spread the risk of catastrophe amongst all clients. Clients of these insurance companies trust that, when something happens, the insurance company will pay them. Blockchain tech may be able to disrupt the insurance industry, as they may leverage the Hyperledger frameworks as a nexus of trust that controls claim payouts.

The healthcare industry has also found distributed ledger technology to be useful to record and share data, such as patient health records, or pharmacy information.

Several industries that deal with materials and product supply chains have began using blockchain and the Hyperledger frameworks for improved resource, sourcing, and allocation.

Let's take a look at different use cases for Hyperledger blockchain technologies and see what advantages they can bring to your business.

### Learning Objectives

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

* Examine several use cases where blockchain technology is actively used to solve real world business problems.
* Discover the factors to look at when evaluating if blockchain technology is right for a particular project.
* Decide when to use and when not to use blockchain technology.

### Business Blockchain Technologies Overview

Blockchain is a data structure with an automated way to enforce trust among participants. Consensus algorithms ensure that all participants agree on the data stored within the blockchain. Blockchain opens the door to disrupt any industry that relies on a central authority to confirm authenticity. It also allows independent, and even competing organizations, to share information to gain efficiencies across an industry.

In permissioned blockchains, a consortium of organizations are responsible for authenticating and controlling the participants in a blockchain. In public blockchains, no central authority or administration is required to exchange data. Blockchains can drive business innovation through controlled data-sharing networks for industry consortiums.

The promise of distributed ledger technologies (DLT) to simplify and automate key work functions has many industries taking notice. Businesses recognize the efficiency gains from transitioning from closed and proprietary solutions to standard open source capabilities, such as Hyperledger business blockchain technologies. Several common project features of blockchain applications are taking shape as the technology matures.

How exactly are businesses using these emerging technologies today? Next, we will explore the state of distributed ledger technologies in actual corporate settings, and how they compare against traditional tools.

### Hyperledger Advantages for Businesses (Brian Behlendorf)

Technologists are studying the Hyperledger protocol and applications.

What should business professionals know about the Hyperledger project?

Business professionals who should... when they see the word 'hyperledger', right, they should associate that with a set of principles that have to do with the creation of high-quality, trustworthy software, right?

First of all, they should associate it with open source development practices, they should know that any project that carries the term 'hyperledger', 'hyperledger foobar', 'hyperledger rhubarb', right, that these are projects that have been collaboratively built, that have been vetted by multiple developers working in concert on the technology, that it's as secure as we can make it, because the code is out there.

We try to hire folks to vet it, but we also... fundamentally, you shouldn't trust software that you can't see the source code to, right?

That brand association, that trademark should really come to be associated with open source, with security, as well as with a sense of process, like something that can't just show up one day and become a Hyperledger project.

The Technical Steering Committee has to approve any new proposed submission, and they have a pretty high bar.

Our goal, again, is not to be the GitHub of projects, even in the distributed technology, or distributed ledger, or smart contract space, but to really have a high quality portfolio of these different efforts.

Finally, they should realize that they can build their business on top of Hyperledger technologies, they can use it all day long, they don't owe anybody a fee, a license fee, a patent license, nothing, and, if they feel like it, if they want to contribute, there should be an easy glide path to having their technical teams get deeper into the code, become contributors, and even help set the direction for the technology.

### Business Interest in Hyperledger

When we first launched this course, in 2017, enterprise blockchain technologies were still in the initial stages of their production implementation. The concept of *blockchain* was at the time mostly associated with bitcoin and cryptocurrency. But the situation has significantly changed in the meantime, and while still considered revolutionary and in early stages, enterprise-grade blockchain technologies are now used in production, changing not only the way we do business, but also the way we envision doing business in the future, as more and more use cases and opportunities are created.

* Smart contracts eliminate the middleman and add accountability (used in various industry sectors, such as real estate, healthcare, government, music, etc.)
* Internet of Things (IoT)-based blockchain applications add a higher level of security,  and transparency (in industries like supply chain, healthcare, banking and financial services, automotive, cybersecurity, etc.). Hyperledger Fabric is at the forefront of this revolution.
* Identity security is a key area where enterprise blockchain technologies can make a difference, bringing, for example, a much-needed reduction in identity fraud and theft claims, cutting the red tape of government and local administration bureaucracy, and more. Hyperledger Indy, Hyperledger Fabric, etc. are just a couple of technology examples successfully used in production in this area.
* Blockchain adds data transparency and automation to supply management and logistics, building trust and enabling leaner, more cost-effective processes.

From smart companies, to smart cities, to smart energy management, to streamlining supply chains and financial services, from logistics to digital identities, across both public and private sectors, the opportunities provided by enterprise blockchain technologies are astounding. Talking about blockchain is now in the past; *it's now time to walk the talk*! And the sky is the limit it seems!

### Blockchain Use Case (Brian Behlendorf)

What is your favorite blockchain use case?

You know, what gets me up in the morning isn't so much making Wall Street, you know, a few milliseconds faster or...

I mean, to some degree, it's nice to be able to talk about, you know, bank payments taking five minutes, rather than three days, okay?

That's kind of a win! But, I'd say, the use cases that wake me up in the morning have more to do with positive social impact, alright?

Projects that, at the same time, is making a difference in fighting slave labor, say, fighting the conflict diamond problems in the diamond supply chain, or fighting the illegal fish catching and the slave labor practices that happen in the fishing industry, by providing better provenance tracking for the fish supply chain...

But, I'm also very much intrigued by identity projects out there, and the potential for distributed ledger applications to take something like India's Aadhar, which is their national ID system, and reinvent that as a decentralized privacy-protecting national ID system, rather than as a centralized, potentially privacy-invasive central ID system.

Lots of companies are starting to figure this out, lots of companies with large amounts of customers are starting to figure this out, and we certainly could do with fewer privacy breaches out there, and less surveillance capitalism, which, you look at all these businesses... many of them have business models based on learning too much about people.

I think through distributed ledger technology, ironically enough, we can actually come up with systems that make management of the distribution of personal data much easier to put in the hands of the individuals themselves.

And so, that's really what gets me excited.

There are numerous blockchain [case studies](https://www.hyperledger.org/resources/publications#case-studies) and [cross-industry projects showcased](https://www.hyperledger.org/resources/blockchain-showcase) on the Hyperledger website. Feel free to check them out to learn more about the business potential of blockchain technologies, and in particular, of Hyperledger technologies.

### Hyperledger Blockchains in Production

Over the past few years, there has been a lot of talk about blockchain and its potential in the enterprise landscape. Today, blockchain is no longer a hype: it has become a reality, and is transforming processes and how enterprises do business, across a wide range of industries.

Below is just a small sample of blockchain-based enterprise solution successfully being used in production:

* **Supply Chain**  
  IBM Food Trust, powered by Hyperledger Fabric, connects farmers, processors, distributors and retailers to create visibility and accountability in the food supply chain, by making the complete history and location of individual food items (along with accompanying information like certifications, test data, temperature data, etc.) available in seconds once uploaded onto the blockchain.  
    
  [Cambio Coffee, in partnership with ScanTrust](https://gateway.on24.com/wcc/gateway/linux/1101876/1832117/how-scantrust-built-end-to-end-product-traceability-with-hyperledger-sawtooth), developed a Hyperledger Sawtooth blockchain network to provide transparency and traceability of the coffee journey, from farmers to roasting, to packaging, and shipping. This approach increased customers' trust in the products and validate their provenance.
* **Airline Industry**  
  NIIT Technologies developed a new blockchain application, [Chain-m](https://www.niit-tech.com/news-events/news/niit-technologies-introduces-chain-m-blockchain-powered-solution-airlines-and-its), using Hyperledger Fabric. This new application aims to enhance passenger ticketing processes by adding increased transparency to the process, and improving record-keeping, security and agility, and ultimately, reducing operational costs.
* **Enterprise Operations Management**  
  JD.com, the largest retailer in China, has developed its own enterprise blockchain platform aimed at streamlining numerous operational procedures, such as tracking and tracing the movement of goods, charity donations, authenticity certification, property assessment, transaction settlements, digital copyrights, etc. [JD Blockchain Open Platform](https://jdcorporateblog.com/jd-launches-blockchain-open-platform/) uses Hyperledger Fabric.
* **Insurance Compliance Data**  
  The American Association of Insurance Services has developed [openIDL](https://www.aaisonline.com/web/guest/openidl" \t "_blank) (open Insurance Data Link), a system built on IBM Blockchain, thus powered by Hyperledger Fabric, which is designed to automate insurance regulatory reporting.
* **Decentralized Identities and Trusted Credentials**  
  In an attempt to streamline their business-oriented services, the [government of British Columbia started working on a project based on Hyperledger Indy](https://www.hyperledger.org/resources/publications/orgbook-case-study). [OrgBook BC](https://orgbook.gov.bc.ca/en/home" \t "_blank) is an online directory that can be used to quickly verify if an organization is legally registered to do business in British Columbia as a corporation. This is just the first step of a larger blockchain-based initiative aimed at streamlining government services.

Next, we will dive deeper into some of the industries that are using blockchain-based solutions, as well as specific use cases.

### Supply Chain Management

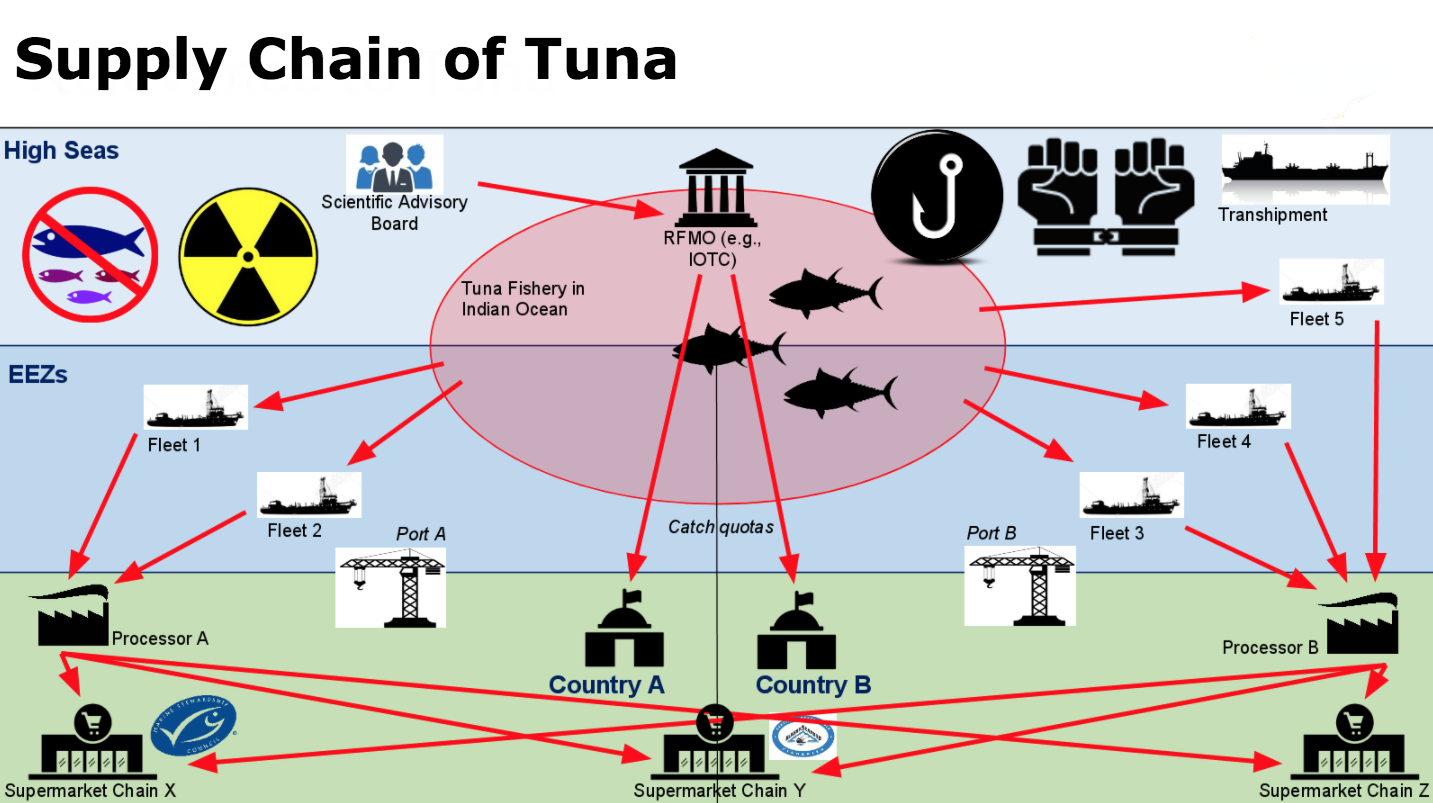
Supply chain management is an important piece of enterprise resource planning (ERP). Supply chain management is the oversight of funds, raw materials, components, and finished products, as they move from suppliers, to manufacturers, to wholesalers, to retailers, to consumers. This movement can occur both within one company, or among several companies. As assumptions change over time, the supply chain models can begin to show weak performance metrics. Good supply chain management will keep product quality consistent, and also prevent either understocking or overstocking of inventory.

Stocking the right amount of inventory over time is also known as supply demand synchronization, and is the key component in just-in-time lean manufacturing and distribution. Companies want to ensure that products are available when needed, but overstocking inventory is costly. Companies that overstock perishable goods must discard items. Companies that overstock non-perishable goods cannot use the money paid for those goods for other purposes until the inventory is used. Furthermore, if the price of a good drops while a company is storing excess inventory, then the company will lose money.

Currently, there are weak points in the supply chain management. These weak points occur where there are multiple ERP systems in use across organizations. Data doesn't flow well through the handshakes or interface points between systems. These weak points usually happen during transference of ownership, or change in status between two parties. Visibility is limited at the hand-off points of funds, raw materials, components, or finished products. This lack of transparency is often intentional, as companies don't want to expose their competitive advantages (e.g., an inexpensive supplier who delivers quality products on time). Additionally, a company could be cut out of a supply chain if members start transacting directly with that company’s suppliers.

Blockchains are being used to solve problems in supply chain management by eliminating the need for a trusted third party to certify raw materials, components, or finished products, as they travel through a supply chain. Every participant, or node, contains a copy of all transactions. This provides an audit trail of every transaction that has occurred in the system. A change would be validated or rejected by the nodes in the system. Because all participants have a copy of all past transactions in the network, any participant can detect if a product is not as advertised. Instead of examining raw materials, components, or finished products at several points in the supply chain, a record of the inspection would be available and bound to the item as it flows through the supply chain. Although a record of the transaction is public and tied to the movement of physical items across the network, specifics such as the quantity of goods, or the identity of the parties transacting, can be done pseudo-anonymously in a blockchain. Such a granular view of movement through supply chains improves resource allocation.

The trade finance industry can also leverage information visible in a supply chain blockchain. In its broadest sense, trade finance manages capital required for international trade. Trade financing has become the norm for cross border transactions, with the [World Trade Organization](https://www.wto.org/english/res_e/booksp_e/tradefinsme_e.pdf) estimating that "up to 80 percent of global trade is supported by some sort of financing or credit insurance" (2016). An exporter needs to mitigate the risk of non-payment, while an importer wants to mitigate the supply risk. The function of trade finance is to act as a third party to remove the payment risk and the supply risk, whilst providing the exporter with accelerated receivables, and the importer with extended credit. Institutions that provide capital during these trades can leverage the information visible in a supply chain blockchain to better evaluate companies for lending.



Source: Nishan Degnarain (used with permission)

### Supply Chain Case Study: Walmart

As one of the world's leading businesses in the supply chain industry, Walmart is constantly looking for ways to enhance transparency and traceability in the food system, and over the years has tried numerous solutions and approaches to solve this problem. Then, the hype of blockchain caught their attention. They looked into various blockchain technologies that could potentially be used to create a traceability system for their supply ecosystem, such as Ethereum, Burrow, Hyperledger Fabric, etc.

In partnership with IBM, they decided that Hyperledger Fabric was the best fit for their needs (enterprisegrade, permissioned, open source, vendor neutral, modular, plug-and-play). In October 2016, Walmart and IBM announced the two projects they were focusing on: one on tracing the origin of mangoes sold in US Walmart stores, and the other project was focusing on tracing pork sold in its China stores.

"The Hyperledger Fabric blockchain-based food traceability system built for the two products worked. For pork in China, it allowed uploading certificates of authenticity to the blockchain, bringing more trust to a system where that used to be a serious issue. And for mangoes in the US, the time needed to trace their provenance went from 7 days to… 2.2 seconds!" As a result, Walmart and IBM worked on expanding the system, both within and outside of Walmart; [IBM Food Trust](https://www.ibm.com/blockchain/solutions/food-trust), an ecosystem of producers, suppliers, manufacturers, retailers, etc., working together to create a smarter, safer and more sustainable global food system, was born.

Today, Walmart traces over 25 products from five different suppliers using the IBM Blockchain built on top of Hyperledger Fabric: from mangoes, strawberries and leafy greens, to meat and poultry, to dairy and almond milk, and even multi-ingredient products like packaged salads and baby foods. And it plans to expand the use of this system to include more products and categories in the near future.

You can learn more about Walmart's successful use of blockchain technologies from this article: [*How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric.*](https://www.hyperledger.org/resources/publications/walmart-case-study)

### Supply Chain Case Study: ScanTrust

Another great example of how blockchain technologies can be a great solution for transparency and traceability in the supply chain industry is that of Cambio coffee: if you buy a pack of Cambio coffee and scan the label with your smartphone, you will be able to see all the details of the coffee's journey, from harvest in Peru, to shipment, to roasting in Shanghai, and delivery to your home. Cambio Coffee is a direct trade organic coffee company that prides itself on building a direct link from coffee farmers to consumers, and the immutable records that are stored on the blockchain are proof that they stay true to their mission.

Cambio Coffee worked with ScanTrust to implement a traceability system built on top on Hyperledger Sawtooth. When ScanTrust decided to implement a blockchain solution to enhance trust, transparency and traceability in the supply chain, they wanted a reliable, proven, open source technology, supported by an active community, and they decided that Hyperledger Sawtooth was the best fit for what they needed, as it is also focused on IoT implementations.

“ScanTrust plans to use the Hyperledger Sawtooth-based solution for other projects. Besides enhancing traceability in the supply chain, the team sees other uses for the technology… A brand could create its own token to incentivize consumers to share data; or it could develop ways to allow consumers to tip the farmer who produced their coffee.”

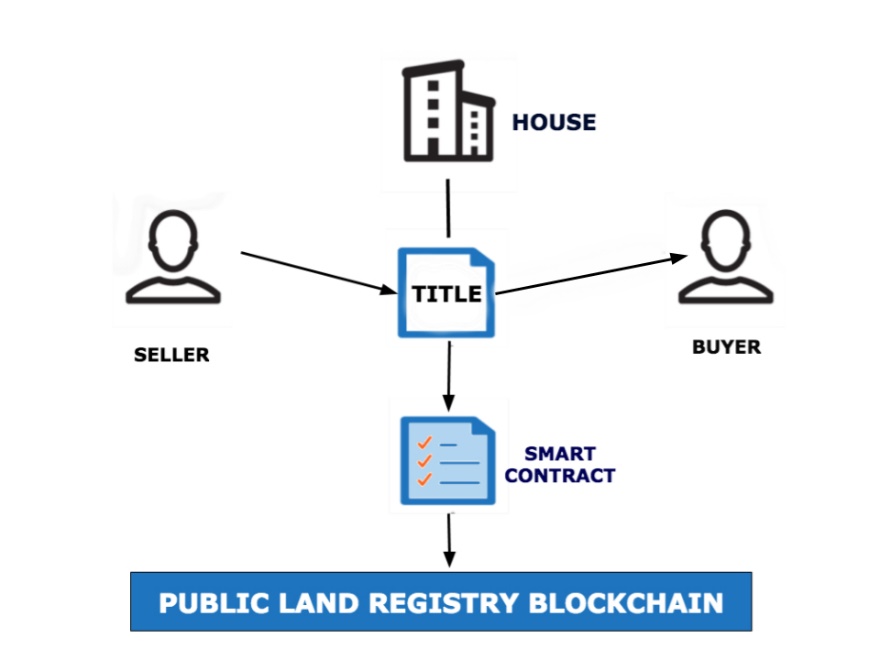
You can learn more about the this use case from the following article: [*How ScanTrust brought Transparency to the Supply Chain with Hyperledger Sawtooth*](https://www.hyperledger.org/resources/publications/scantrust-case-study).

### Property Rights

The legal industry has begun to examine how blockchain technologies can minimize disputes around property rights. Property rights are a division of law whereby the rights and responsibilities associated with owning an asset are established. Property ownership rights may include the right to use the asset, the right to profit from the asset, the right to exclude others from using the asset, or the right to transfer the asset to others. Property ownership responsibilities may include tax liability for the asset, maintenance and repair costs, or payment for injuries caused by unsafe or defective conditions of the asset.

Ownership for a particular asset may be transferred in whole, or in part. As a result, property rights or obligations attached to a particular asset may belong to several different entities at the same time. For example, if you purchase a plot of land, you have the right to use that land. However, the usage of the land is most likely limited by the government. The right to use the land may be taken away from you by foreclosure if you do not pay property taxes. Similarly, your right to use the land is limited to permitted uses per that areas’ zoning laws. It is unlikely that you will be allowed to operate a pesticide manufacturing plant in the middle of a residential neighborhood. If you lease out the plot of land, your right to use the property is transferred to the tenant, but you are still able to sell the plot of land to another landlord while the lease is active.

Companies may use blockchain technologies to record ownership rights and responsibilities. Specifically, governments have put land registry records on blockchain (Laura Shin, [forbes.com](https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#1c7a07944da3), 2016). Companies have also put intellectual property registration and ownership on blockchain ([poex.io](https://poex.io/)). Intellectual property includes copyright, trademark, and patents. To legally protect ownership rights in these, one registers their production, or invention, or otherwise proves when the work was established, and that they are the origin of the work.



Property Titles on a Blockchain via a Smart Contract

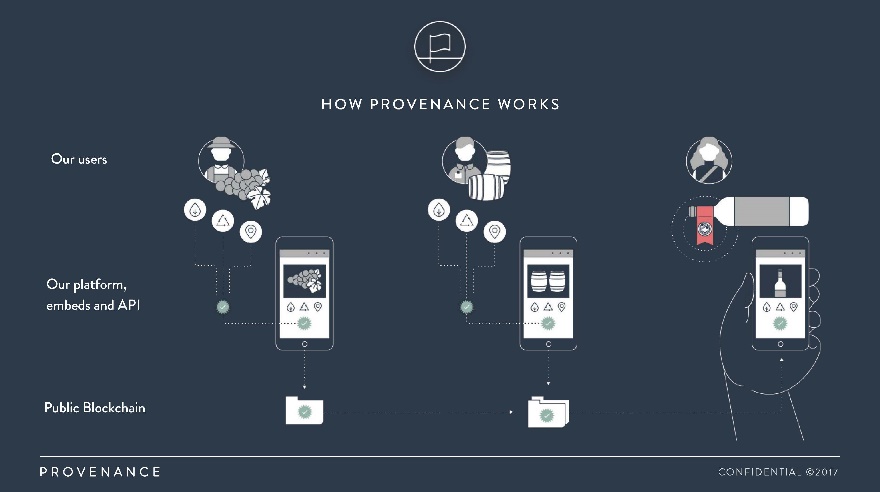
Companies with strong brand value in particular, such as the fashion industry and luxury good providers, are interested in more efficient ways to protect their intellectual property. When data is added to a blockchain, it can provide an immutable, secure, timestamped record for the creation of intellectual property, and any changes to the data can be easily detected. Blockchains establish this in a variety of ways.

A blockchain may record a hash of a document. As an example, photographers could place a hash of their unique digital photographs on the blockchain. The hash of a digital photograph will be constant so long as the photograph file has not been altered. Therefore, the blockchain can control and track the distribution of the photograph, detect the introduction of counterfeit images, and be used to resolve disputes as to who first introduced the image. By placing a hash of intellectual property documents on the blockchain, a party can publicly demonstrate data ownership, and prove the existence of certain documents at a given moment in time, without revealing the actual data. In addition to the hash, you may also choose to store the location of the file in the blockchain, which could be used for retrieval.

### Provenance

As the previous section on blockchains for supply chain management illustrated, blockchain data improves insight into products, as they move through their lifecycle. Large enterprises are not the only parties to benefit from this increased visibility. Consumers can also benefit from blockchain technology.

Provenance is a record of ownership used as a guide to authenticity or quality. Because of the overhead involved in traditional provenance records, they were only available for very large ticket items, such as works of art. With the efficiencies gained from blockchain technology, provenance records can be available for a wider range of goods. This improved information can aid consumers as they make purchasing decisions.



**How Provenance Works**(by [Project Provenance Ltd](https://www.provenance.org/), used with permission)

How do you, as a consumer, really know that you purchased an authentic item? Why is authenticity important? Some consumers want to make sure that fair trade and fair labor standards are upheld in the products they purchase. Others want to make sure that none of their products have been tested on animals. Still, others are concerned with the use of harmful chemicals during product manufacturing. Those consumers are willing to pay a premium to make sure that they are not funding operations that are not in line with their values. Counterfeit products, however, take advantage of the higher price point a brand that upholds strict standards can command. Their margins are increased over the authentic brand because they cut corners during production.

It turns out that counterfeit products are a global problem affecting several industries. For example, the European Union Intellectual Property Office (EUIPO), in collaboration with the International Telecommunication Union (ITU), estimates that $48 billion worth of smartphone sales were lost to phoney phones in 2015 (Karen Gilchrist, [cnbc.com](https://www.cnbc.com/2017/02/28/fake-smartphone-sales-cost-global-industry-48-billion.html), 2017). Also, "the Interprofessional Council of Bordeaux Wine estimates that 30,000 bottles of fake imported wine are sold per hour in China", whereby some estimate half of the wines retailing for more than $35 in China are counterfeit (Pamela Ambler, [forbes.com](https://www.forbes.com/sites/pamelaambler/2017/07/27/china-is-facing-an-epidemic-of-counterfeit-and-contraband-wine/#394d10b15843), 2017).

In order to be certain that your product is authentic, you would need either a record of all the transactions for the life of the item, or a trusted third party. Trusted third parties certify the authenticity or quality of an item. They function as a new data layer between data silos, and increase costs of transactions by charging for providing data and certifying products. Some examples of such trusted third parties are the National Organic Program (USDA Organic) for produce, Fair Trade USA for human worker conditions, or the Gemological Laboratory of America (GLA) for jewelry, diamonds, and gemstones. Blockchains can serve the function of these trusted third parties by uniquely identifying products, and certifying their authenticity. Alternatively, these trusted third parties can leverage blockchains by recording their audits and inspections on blockchains. This would reduce the overhead needed to certify products. For example, a manufacturer could prove that its sources also abide by the certification authorities’ standards if those sources are listed on blockchains as having passed all requirements. The timing of the source’s original certification and renewals could be viewed by any interested party.

As a consumer reading from a blockchain, you would be able to verify a product’s authenticity by seeing the full chain of custody for an item. Hyperledger frameworks allow consumers to view important data attached to the goods, without necessarily viewing exactly who conducted each transfer down the supply chain line. Therefore, the promise is that you will be assured that the product you are purchasing is an authentic product, without necessarily allowing the public to view your purchasing habits, all leveraging distributed ledger technology.

### Provenance Use Case: Circular

For years, consumers have been looking for ethically-sourced products, and a well-known example is that of diamonds provenance. A much less known conflict mineral is tantalum - a rare mineral used to make capacitors found in devices like smartphones and laptops. Rwanda is the world's largest supplier of tantalum; however, at times, tantalum is also smuggled in from Congo, where children or enslaved workers are used to mine it. As a result, there are many regulations passed by OECD (Organisation for Economic Cooperation and Development), US, and EU (US Dodd-Frank Act of 2010, EU Conflict Minerals law, etc.) aimed at improving traceability. Despite this regulations, there has not been a reliable way to prove the source of tantalum.

Blockchain technologies have been a game changer. Circulor, a UK-based company, has developed a system that traces the origin of tantalum, ensuring it is mined, transported, and processed according to approved regulations. This system is built on Hyperledger Fabric and delivers the first mine-to-manufacturer traceability of tantalum. How were they able to succeed? By creating a very tightly controlled system, that recorded the tantalum journey every step of the way: from mining in Rwanda, to refining in Macedonia, to manufacturing in USA, shipping from USA, final assembly in China, and the distribution to consumers.

The system went smoothly into production in the fall of 2018, and included, to start with, three mines in Rwanda and a refinery in Macedonia. And the plan is to bring more mines into the system. On top of that, Circulor aims to expand the system they built to cover other minerals and countries.

You can read more about tantalum traceability success story on the Hyperledger website: *[Circulor achieves first-ever mine-to-manufacturer traceability of a conflict mineral with Hyperledger Fabric](https://www.hyperledger.org/resources/publications/tantalum-case-study" \t "_blank)*.

### Finance

"Blockchain has huge potential to move the financial services industry away from messaged based models, slow reconciliation processes and inefficiency of fragmented data stores. With blockchain, financial services can move to a shared data construct, driving down costs, increasing efficiency and opening up entirely new business models".  
- David Treat, Accenture

The Bitcoin blockchain was created as a "peer-to-peer electronic cash system" ([Satoshi Nakamoto, Bitcoin](https://bitcoin.org/bitcoin.pdf)). Therefore, the first blockchain use case in existence was payments. However, Bitcoin proved to be quite slow to process payments, "somewhere in the region of 7 transactions per second", when compared to Visa, which "averages around 2,000 transactions per second, with peak capacity of perhaps 50,000 transactions per second" ([Guy Brandon, due.com](https://due.com/blog/can-the-blockchain-scale/), February 2017). Developers are actively working to increase the throughput capacity of Bitcoin and other blockchain payment systems ([lightning.network](https://lightning.network/" \t "_blank)). Payments, especially international payments, can be quite costly. Blockchain technologies plan to decrease the costs associated with payments, by allowing parties to interact directly, instead of transferring through an intermediary, such as a bank. In addition, having a record of all past payments is useful to auditors and regulators. Financial institutions have heavily researched blockchain payment systems because a universally recorded world state of payment information can decrease the number of payment disputes among institutions.

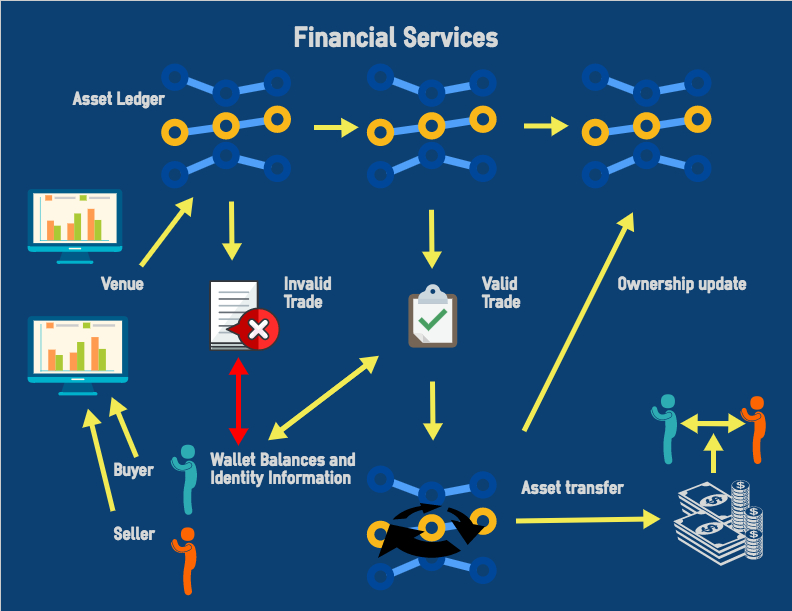
The finance industry, in particular, has shown early interest in blockchain technology. [R3](https://www.r3.com/about/), a fintech company that is a member of the Hyperledger consortium, has brought together more than 100 leading financial institutions to examine blockchain technology. The finance industry has already recorded business transaction agreements on blockchain. Currently, bonds, invoice financing, letter of credit transactions, and interest rate swaps governed by an ISDA master agreement have all been recorded on blockchain.

The financial industry would like to improve transaction settlement through blockchain technology by leveraging smart contract functionality for executing trades. Absent blockchain technology, a complex process known as the post-trade cycle is initiated once parties "execute" a trade. The post-trade cycle involves a series of steps to verify the terms of a trade, and to transfer assets involved in the trade in order to effectuate and settle the trade. Some trades are currently required by law to go through a separate central clearing organization. This organization steps in as the counterparty to each trade, creating two distinct contracts for each trade. These organizations are central securities depositories, whose role is to minimize the risk of trade default, and also to enforce rules against overexposure to certain types of trades.

Although every trade has its own lifecycle, generally, the following steps will occur:

* Parties execute a trade. Executing a trade occurs when parties agree on the details of a trade and are willing to enter into the deal.
* One party will draft an inception document, capturing all the terms of the trade, and will send it to the other party to get the trade confirmed.
* The recipient of the inception document will check the details of the trade and confirm the trade by signing and returning the document. Confirmation communication is done often by Fax, SWIFT, or Telex.
* The trade is allocated. For flexibility of profit and loss booking, parties will often allocate the trade to various sub-entities within their organization.
* Each trade will be stored by the party who was allocated the trade on an internal database. For ease of identification, the trade is assigned a unique Trade ID as a standard identifier.
* Post-Trade Changes are sometimes made by the parties. This can occur when:  
  - The trade can be amended with consent of both parties  
  - One party may assign its position in the trade to a different party  
  - A partial termination of the trade may be triggered if a change in the notional of the trade that is not pre-fixed according to the agreement occurs  
  - Termination of the deal before maturity of the trade may occur, which may entail a termination fee.
* Payment is made. These payments may be at the close of a trade, or at intermediate stages while a trade is still open. When the payments are made on an open contract, this is known as 'revaluation' and is done to minimize the risk of nonpayment by a counterparty whose position has weakened in the trade due to events that occurred after trade execution.
* Audit of the trade and associated payments is performed by the parties. If a dispute occurs, the parties must communicate and come to a resolution for such discrepancies. This is a manual and costly process.

Smart contracts may greatly improve the process of post-trade settlement, by reducing disputes and errors. Smart contracts will ensure that final settlement will happen when the execution of a trade occurs. With smart contract technology, a legal agreement can automatically execute clauses within it.



The image above shows the automation of back-office processes involved in trade confirmation and post-trade settlement via DLT. An asset ledger stores ownership and transactions. Smart contracts allow the asset ledger to handle collateral management and initiate payments per contract terms. Venues (e.g. exchanges, MTFs, bilateral voice conversations) still match trade requests with a counterparty, and provide price discovery. Querying information on the asset ledger may assist with price discovery. The asset ledger verifies the parties and asset ownership. It will then either accept, or reject the trade. If, for example, the seller does not own the asset in question, or the new trade would result in an illegal overexposure on the buyer side, the trade would be rejected. When a trade is valid and accepted onto the blockchain, the blockchain automates an immediate change in ownership, or a delayed, or contingent asset transfer. The changes in asset ownership or contract terms are securely recorded onto the asset ledger. The contract is programmed to execute automatically, exchanging payments and other assets per the terms agreed to by the parties.

It is still unclear whether courts will enforce blockchain contracts in the same way that they enforce traditional written contracts, with inked paper signatures. Therefore, the current best practice is to record trades on blockchain, alongside traditional legal documentation. The operative clauses in the traditional written contract are converted into smart contract templates to be placed on blockchain once a trade is confirmed. For example, a full ISDA master agreement document would be stored on blockchain, and tied to the smart contract governing the underlying swap or derivative trade. This leverages the predictable outcomes of a legal contract with the efficiencies that can be gained from distributed ledger technologies.

There are both advantages and disadvantages to controlling funds on blockchain. If funds aren’t under the control of the smart contract, then there is no way a payment can be guaranteed. If funds are controlled by the parties’ smart contract agreement, then those payments can indeed be guaranteed at the close of the trade. However, this also means that those funds cannot be used by the parties’ for anything else throughout the lifecycle of the smart contract. Today, a party may use the funds separate from the contract. This exposes the other party to the risk of nonpayment, but frees up capital for other purposes. The connection between risk and return is not a problem that blockchains can solve.

Conducting post-trade settlement in an automated way through smart contracts promises to introduce efficiencies, and reduce friction associated with trades. However, the industry has experienced some barriers to the adoption of blockchain technologies. Primarily, data privacy rules have come into conflict with the way standard blockchain protocols operate. Some regulations in the finance industry will not allow you to share information, or store it on a shared medium, even if it is encrypted. In addition, regulations covering securities professionals specify how ownership of certain assets must be recorded and properly transferred. Securities professionals include broker-dealers and investment advisers. These rules were written without the anticipation of blockchain technologies, and are at odds with the fully digital transference of assets over blockchain technologies. Either these regulations will need to adapt to blockchain technologies, or blockchain technologies will need to introduce new features conforming to existing regulations. The adoption of blockchain technologies for post-trade settlement will likely change the role of governments in the financial oversight. There will be less of a need to enforce individual trades and resolve settlement disputes, but the government may collect better data on existing trades by viewing and querying the blockchain. With this increased insight into the market, the government may or may not develop stronger standards for trades through smart contracts.

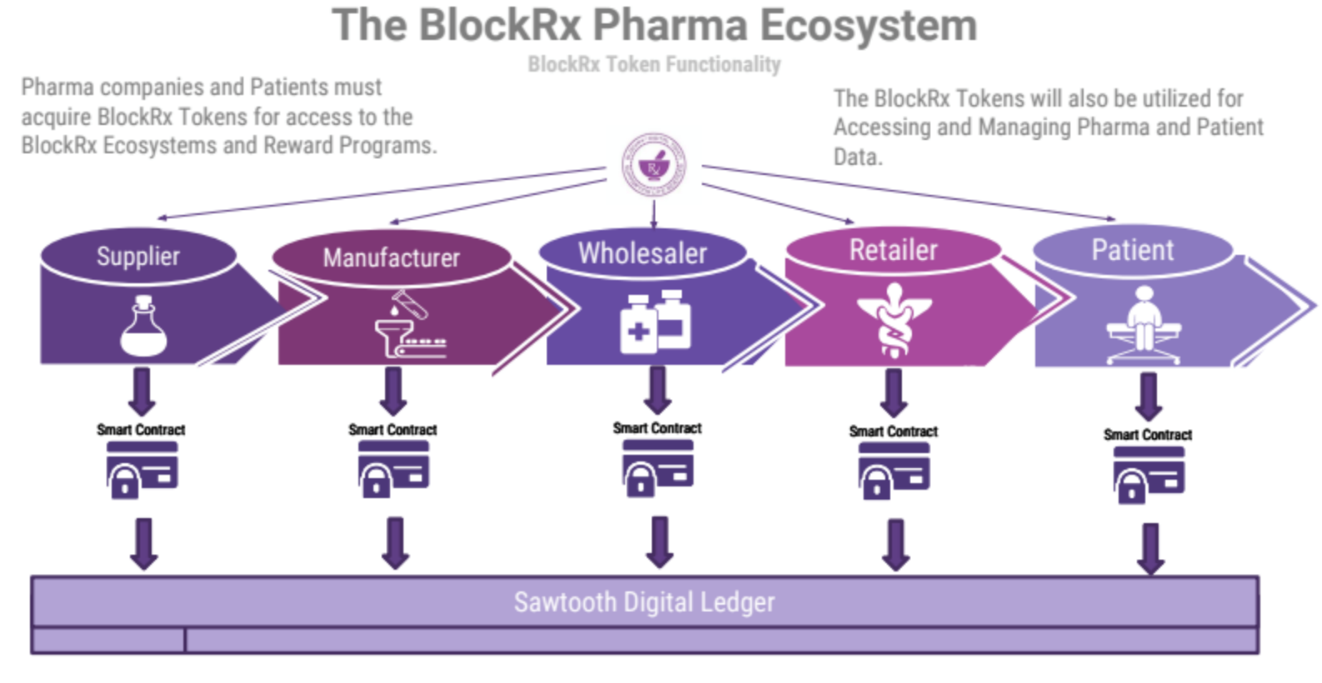
### Healthcare

A number of multi-party processes in the healthcare industry can leverage distributed ledger technology. By streamlining these multi-party processes, the healthcare industry can reduce the time and expense of collecting and verifying multiple pieces of information in order to deliver quality care to patients. Healthcare providers and insurance companies have begun to explore how blockchain can improve the delivery of patient care.

In 2015, the US spent 27.42% of the federal budget, or $1.05 trillion, on healthcare ([National Priorities Project](https://www.nationalpriorities.org/budget-basics/federal-budget-101/spending/)). Because these costs are so high, the US government, in particular, has invested resources into healthcare blockchain technology. The [Office of National Coordinator for Health Information Technology (ONC)](https://www.healthit.gov/) is responsible for health information technology. It has recognized a need for nationwide interoperability and standards for electronic health records, claims processing, and verification of provider credentials. To that end, it has sponsored many government blockchain initiatives in healthcare.

The healthcare industry has already placed medical insurance enrollment information on blockchain for verification, and plans to incorporate many other aspects of medical insurance claims processing on blockchain. One cost borne by health insurance providers is auditing care providers. Health insurance providers must verify whether a practitioner actually delivered the care that he or she was obliged to deliver to the patient. Health insurance providers must also audit the financial aspects incurred as part of this care, to ensure that care was paid, and the charges were accurate. Tying the care auditability with the payment auditability provides a key advantage to reducing the potential for fraud.

The healthcare industry has examined placing prescription drug fulfillment processes on blockchain since they involve gathering and checking information from many sources. Insurance benefits investigation eligibility checks are performed to see if insurance will pay. Prior authorization and step therapy requirements are checked to see if a patient is able to receive a particular drug, or if other drugs are preferred. Formulary checks, patients’ assistance checks, and pharmacy stock checks must all be performed. The healthcare industry has also used DLT to handle online identity management, by uploading verified pieces of a healthcare professional’s credentials for license verification.



By [The BlockRx Project](https://www.blockrx.com/), retrieved from the [Hyperledger Healthcare Working Group, August 22nd, 2017 Meeting](https://wiki-archive.hyperledger.org/doku.php?id=groups/healthcare/healthcare-wg-meetings)

Another area blockchain is used in healthcare is to protect data from cybercrime. Data breaches happen on a daily basis across all industries, and healthcare is no different. In fact, [1 in 4 data breaches](https://onlinenursing.duq.edu/blog/healthcares-blockchain-security-solution/) occur in the healthcare sector, affecting millions of people: more exactly, 1 in 13 patients in the U.S. are affected by breaches. Why is healthcare data so sought after by hackers? Because it's personal, permanent and detailed: from social security numbers, to address, to family history, to confidential medical history.

### Education

Blockchain solutions are being successfully implemented across various industries. As the technologies advance, more and more potential use cases arise. Education is one such area that could stand to benefit from distributed ledger technologies:

* Streamlining verification procedures for academic credentials, thus reducing fraudulent claims and bringing more transparency, ease of use, and speed to this process.
* Verifying e-portfolios of digital badges
* Securing and sharing student records
* Identity management
* Sharing security data (from security cameras and sensors, for example) across device networks
* Creating learning marketplaces
* Records management
* Increasing accountability and transparency for charitable school donations
* Streamlining the public assistance system for families and students.

You can learn more about the potential advantages of using blockchain solutions for education from the following article: [*20 Ways Blockchain Will Transform (Okay, May Improve) Education*](https://www.forbes.com/sites/tomvanderark/2018/08/20/26-ways-blockchain-will-transform-ok-may-improve-education/#6b6198ac4ac9).

### Education Case Study: Sony Global Education

We've all experienced the process of enrolling in higher education or applying for a skilled job - no two applications are the same, as each institution uses their own individual application and validation processes. Similarly, the credentials we must have when applying each require different validation process as well. Needless to say, this is a rather long and complicated process. Sony Global Education has identified in Japan the need to create a comprehensive, open and trusted system to record educational and training credentials of Japanese citizens. But this need is not limited to Japan alone - it spans worldwide. As such, Sony Global Education aims to create a system that will store this siloed data into one system, gathering people's academic and training credentials and then controlling access to this recorded data.

Sony Global Education decided to use Hyperledger Fabric, as it is a trusted, secure, open source, platform. The solution they designed was already tested successfully. Moreover, Sony Global Education is working with the Japanese Ministry of Internal Affairs and Communications to develop a next-generation system for managing digital transcripts based on their tested solution, aiming to secure the authenticity of transcripts and allow them to be safely shared within a trusted network.

You can learn more about this use case reading [*Sony Global Education Chooses Hyperledger Fabric for a Next-Generation Credentials Platform*](https://www.hyperledger.org/wp-content/uploads/2017/12/Hyperledger_CaseStudy_Sony.pdf).

### Smart Energy Management

We live in an increasingly connected and energy-dependent world. Balance between supply and demand is imperative to ensure electricity demand is met. However, the increasing demand in electricity adds increased pressure on conventional energy sources. For the most part, the existing electricity grid is coping with the existing demand; however, when unexpected events occur (weather-related, for example), the pressure exerted on this grid can reach dangerous, unsustainable levels. And with the advent of increased dependency on electricity in day-to-day life, time will come when conventional resources will no longer be sufficient. Drastic times require out-of-the-box solutions.

Enterprise-grade blockchain technologies are playing an increasingly important and innovative role in an increasing number of industry sectors, including the energy sector. In 2017, IBM partnered with TenneT, sonnen and Vandebron  to develop a [distributed database for managing the electricity grid](https://www-03.ibm.com/press/us/en/pressrelease/52243.wss) in the Netherlands and Germany:

* TenneT is focusing on finding new sustainable ways to cope with the increasing dependency on and demand for electricity. In their quest to maintain the supply-demand balance, TenneT is exploring the use of a Hyperledger Fabric-based permissioned blockchain network that will integrate renewable electricity sources (such as electric cars and household batteries) in the energy grid.
* TenneT and Vandebron are running a pilot project in the Netherlands to test this potential solution. "Vandebron will work with customers who own an electric vehicle to make the capacity of their car batteries available to help TenneT balance the grid. Vandebron will provide this service to its customers without compromising the availability of their car battery. The blockchain enables each car to participate by recording their availability and their action in response to signals from TenneT."
* TenneT and sonnen are running another pilot project in Germany, focusing on re-dispatch efforts to prevent regional overloads on the energy grid by integrating renewable energy sources into the electricity supply network. In Germany, this would be needed, for example, when wind energy produced in northern Germany cannot be transported to industrial centers in the southern part of the country. To solve this issue, a network of residential solar batteries aims to reduce the pressure of the distribution limitations. The blockchain network will allow the TenneT operator to see available, ready-to-activate residential solar batteries, and then record the batteries' input to the electricity grid.

If tests are successful, this [Hyperledger Fabric-based implementation](https://www.youtube.com/watch?v=IJ3U7wACSc8) could then be implemented worldwide, adding much needed flexibility and security in the energy management system.

### Smart Cities Use Case: Smart Dubai

Dubai is known for being a world-class business, cultural, and touristic destination. Dubai aims to become the world's first government fully powered by blockchain technologies by 2020. [Smart Dubai](https://www.smartdubai.ae/) is a city-wide effort to empower residents and visitors alike via digital transformation, an effort that relies on the partnership between the private sector and government entities. It aims "to make Dubai the happiest city on earth through technology innovation" by creating an efficient, blockchain-based city government, digitizing all of its services to add increased transparency, security, efficiency and reduce bureaucracy. Below we highlight just a few of the Smart Dubai initiatives:

* The Dubai Blockchain Strategy aims to enable the execution of all applicable government transactions through blockchain by 2020.
* The Decentralized Data Marketplace leverages blockchain technology to ensure the security and immutability of transactions, tokenization to hide sensitive information, etc.
* The [UAEPASS](https://www.smartdubai.ae/apps-services/details/uae-pass) is the national digital identity platform, giving UAE citizens, residents and visitors access to local and federal government services, as well as those of private companies, all on a single smart application, allowing them to authenticate and sign documents digitally.
* The [DubaiNow](https://www.smartdubai.ae/apps-services/details/dubai-now" \t "_blank) mobile application is a one-stop shop for smart services, unifying more than 55 key services from 22 government agencies. This application allows users to manage their bills, register their cars, renew licenses, track visa applications, obtain general information in real-time (from weather, to public transport, to health, etc.), and much more. This application also enables the Dubai government to implement various social responsibility-related activities: donations are collected and then distributed to a variety of beneficiaries, in collaboration with charities and government agencies. It also allows you to direct how money collected from fines you pay (e.g. traffic fines) are used, among other things.
* Paperless government by 2020 is another goal of the Smart Dubai initiative, allowing officials and citizens to save time and resources, and protect the environment as well. “Adopting Blockchain technology Dubai stands to unlock 5.5 billion dirhams in savings annually in document processing alone - equal to the one Burj Khalifa’s worth of value every year.”

Smart Dubai is embracing a multi-blockchain business model to deliver services, such as IBM's Hyperledger Fabric-based  and ConsenSys' private blockchain implementation based on Ethereum. In October 2018, Smart Dubai and IBM launched the [Dubai Blockchain Platform](https://www.smartdubai.ae/newsroom/news-details/2018/10/30/smart-dubai-and-ibm-to-offer-first-government-endorsed-blockchain-platform#listingPage=1), the first government-endorsed blockchain-as-a-service platform in the UAE.

Through its ground-breaking, innovative initiatives and forward thinking, Dubai is transforming the life of its residents and visitors alike, creating a high benchmark for other cities looking to leverage innovation and state-of-the-art technologies. And while Dubai has achieved great successes in the past few years, their mission will not stop in 2021. They already have a vision toward Dubai 2050.

"Smart technology has firmly established itself as the engine driving the cities of the future, transforming human communities and activities - from the most mundane of tasks to the most complex. We are constantly on the lookout for new opportunities to meet representatives from other like-minded organisations who share our vision for a smart, connected future that allows people to enjoy seamless city experiences." ([Khaleej Times](https://www.khaleejtimes.com/smart-dubai-empowering-tomorrow))

- Dr. Aisha Bint Butti Bin Bishr, Director General of the Smart Dubai Office

### Blockchain Best Practices for Enterprises

The use of distributed ledger technologies in production across various industries continues to expand and reach new horizons, as businesses explore new ways to incorporate blockchain in their day-to-day activities. However, in order to increase the success of blockchain business applications, some best practices must be considered:

* **Security for the long term**    
  While blockchain transactions are secure and cryptographically protected when it comes to the current technological advancements, we should always keep in mind that nothing is static, and technology continues to advance at an incredibly fast pace. What is secure today may not be so in the near future. Hackers and other bad actors are constantly focusing on breaking the cryptographic algorithms that protect blockchain data today.   
  *To avoid the potential security disruptions of tomorrow, a critical best practice is that users should never put personally identifiable information, or PII, on their blockchains.*
* **File storage on the blockchain**  
  Due to the way blockchains work to store data, replicating it on every other node or peer in the network, storage and compute costs can be incredibly high. *To avoid added storage costs, it is recommended that other storage and replication methods to be used - this includes cloud networks like AWS S3, GCP Filestore, etc.* This way, nodes and peers can have pointers or links to the data files kept outside of the blockchain network, instead of the actual data.
* **Permissioned blockchain for private data**  
  On public blockchains, anybody has access to the information stored on the network: they can add transactions and read the data that is in it. When it comes to permissioned blockchains, data can be stored, accessed and used only between partners that have access to it. *Permissioned blockchains, such as the Hyperledger technologies, are a great solution for businesses, as they want their data to remain private.*
* **Blockchain governance** **structure**  
  Most blockchain-related challenges are related to the governance model that is chosen. To keep things straightforward, you should define the governance structure upfront very early in the process, even before diving into blockchain: decide how new users/organizations are added to a blockchain network, how to determine if a user/organization should be removed from the blockchain network, include a mechanism that deals with and removes bad actors previously allowed in the network, etc. Keep in mind that things change over time, and as such, the governance procedures may change as well.
* **Performance and scalability requirements**  
  Blockchain architects must have a clear understanding of the requirements for their specific use cases, and they must ensure that their blockchains meet those requirements. Based on these requirements, decisions must be made early on with each deployment and use case in regards to what technologies to use.
* **Goals of blockchain business cases**  
  Not every project or solution is successful, unless it is carefully planned, designed and implemented. *A carefully thought out strategy must be designed and implemented for each project, to ensure that goals are achieved.*

Blockchain can be a great solution for numerous business use cases that rely on security, controlled access, accountability, transparency, and efficiency, spanning a wide range of industries, from finance to banking, supply chains, manufacturing, healthcare, telecom, etc. Having well laid plans, goals and best practices can all help enterprise IT leaders explore the growing blockchain ecosystem as they work to capture its strengths for their businesses.

### The Outlook of Blockchain for Business

The [2019 Technology Industry Innovation conducted by KPMG](https://assets.kpmg/content/dam/kpmg/us/pdf/2019/02/blockchain-tech-survey-2019-infographic.pdf) around the adoption of blockchain technologies suggests that 41 percent of businesses are likely to adopt and implement blockchain into their business operations in the next three years. Another important aspect revealed by this survey is that 48 percent of enterprises believe that blockchain will change the way they conduct and manage their business activities in the near future.

What areas are expecting significant disruptions due to increased adoption of blockchain technologies? The survey shows that IoT processes are expected to be impacted the most (27%), followed by processes involved in trading (22%),  reduced cybersecurity risk (20%), contracts (18%), etc. Industries that are believed to see the greatest blockchain adoption in the near future are financial services, industrial manufacturing and telecommunications.

What advantages would businesses have by adopting blockchain technologies? The KPMG survey outlines some of them:

* Improved business efficiencies
* Product/service differentiation
* Increased profitability
* Cost reductions
* New business insights from incremental data, etc.

Blockchain is viewed as one of the top 10 technologies that will transform businesses over the next three years, and beyond. The 2019 KPMG survey ranked blockchain at number 4, compared to 7 just a year ago. And, according to the Worldwide Semiannual Blockchain Spending Guide (March 2019) from [International Data Corporation](https://www.idc.com/getdoc.jsp?containerId=prUS44898819) (IDC), worldwide spending on blockchain-related solutions is expected to reach $2.9 billion in 2019 (an increase of over 88% from the previous year), and $12.4 billion by 2022.

Want to be at the forefront of the blockchain technological innovation? Start assessing your needs to see if blockchain would be a good solution for your business.

### What Enterprises Look for When Evaluating Whether or Not to Use Hyperledger (Brian Behlendorf)

What should an enterprise look for when evaluating whether or not to use Hyperledger?

I always try to start... suggest that people start with the business need, right, trying to look at what are you doing in your enterprise, and probably, it will mean what are you doing with your business partners, with your suppliers, with your customers, maybe even with your competitors, right?

What is it... what are some business processes, or some provenance tracking problems, or a registry somewhere that, you know, you're putting too much trust in a central org somewhere, where is there an opportunity to take a decentralized ledger approach, and a smart contract approach to solving those issues?

Start with the need, right?

In fact, one way to explore that is, you know, every industry has a consortium somewhere in that industry talking about technical standards, talking about common business processes, and those are often the right kinds of organizations to look at doing a proof of concept with, right?

Because they often have kind of this overarching kind of view of the industry, and they tend to be trusted by the participants in that industry.

Often, they could come up with what's the right kind of proof of concept, or maybe even a Minimum Viable Product kind of project, because there really is no blockchain of one, right?

It's really hard just to think about solving your own problems with a block, with a distributed ledger.

You really need to think about an industry-wide kind of approach, even from the earliest day.

Once you've identified like that kind of opportunity, you should start to ask yourself what are the characteristics of that need, is it from a transaction rate perspective, from a number of nodes, from how geographically distributed those nodes might be, and then, also ask yourself who are the developers that I'm expecting to be able to tap, to bring this technology to bear, and have they started to investigate distributed ledger technology, have they started to learn how Fabric works, how Sawtooth works...

I think that that's another important side of it.

As the business side of the house is trying to understand the use cases, you should really let your technology teams explore this technology, allow them to get their hands dirty, to go to a hackathon, to take this course, to start playing with these technologies to get a more intuitive sense for what they do, and what they can't do, right, what their limitations might be.

This is still very early days, and you still need to be smart about how do we apply these and how do we use them.

At some point, those two teams should meet up, right, and say "Here's what we think is really the MVP [Minimum Viable Product] or a proof of concept", and the other team should... that comes from the technology side of the house, should say "Okay, we understand how to build this, you know, if we, you know, shave these corners, we can do something in a week", right? and let's just see that, you know, cheap and dirty, what it looks like.

And then, over time, start to promulgate that amongst the other partners that you think you'd involve in a distributed ledger project.

### When to Use Blockchain

There are certain factors to consider when evaluating blockchain distributed ledger technology for your business. How many participants are in your system? What is the geographical distribution of the participants? What sort of performance requirements do you have? Defining the rules, risks, and responsibilities of each party in your blockchain system is useful as you consider transferring a database to a decentralized environment such as one of the Hyperledger frameworks. Blockchain is best suited for business applications where one or more of the following conditions apply:

* There is a need for a shared common database
* The parties involved with the process have conflicting incentives, or do not have trust among participants
* There are multiple parties involved or writers to a database
* There are currently trusted third parties involved in the process that facilitate interactions between multiple parties who must trust the third party. This could include escrow services, data feed providers, licensing authorities, or a notary public
* Cryptography is currently being used or should be used. Cryptography facilitates data confidentiality, data integrity, authentication, and non-repudiation
* Data for a business process is being entered into many different databases along the lifecycle of the process. It is important that this data is consistent across all entities, and/or digitization of such a process is desired
* There are uniform rules governing participants in the system
* Decision making of the parties is transparent, rather than confidential
* There is a need for an objective, immutable history or log of facts for parties’ reference
* Transaction frequency does not exceed 10,000 transactions per second.

### When Not to Use Blockchain

Blockchain technology is a powerful tool, but it is not always the right tool for the job at hand. If you are contemplating using blockchain technology, be sure to evaluate the problem fully. The following conditions are not currently well suited to blockchain-based solutions:

* The process involves confidential data
* The process stores a lot of static data, or the data is quite large
* Rules of transactions change frequently
* The use of external services to gather/store data.

Next, we will discuss in more detail the conditions that are not well suited to blockchain-based solutions.

### I. The Process Involves Confidential Data

The biggest advantage and challenge in deploying blockchains is the radical transparency which they provide. Methods are being developed to hide confidential data on the blockchain, while sharing it only to relevant parties. Regulations for data privacy often do not allow for blockchain solutions. A thorough review of the relevant privacy rules governing your business case should be examined to see whether blockchain is appropriate. For example, is leaking data in encrypted form allowed? What level of encryption is required when transmitting data?

### II. The Process Stores a Lot of Static Data/Data Is Quite Large

With blockchain technology, the entire database is stored across many nodes in a blockchain system. Because the replication factor of these systems is so high, they are best suited to databases that have many state changes, or store only the minimum necessary amount of information. If the data is relatively static, or if the files to be stored are quite large, a different technical solution may be more appropriate.

### III. Rules of Transactions Change Frequently

If the rules around how your business processes are conducted change frequently, or change in unexpected ways, then blockchain may not be well suited for your use case. The rules of transactions in blockchain are often pre-set, and smart contracts do not change execution paths once they have been initiated. Everything that takes place on a blockchain must be completely deterministic. Additionally, blockchains are append-only databases. A relational database may be more suitable if you need to make many changes to your data as the rules of your transactions change.

### IV. The Use of External Services to Gather/Store Data

A blockchain smart contract does not currently initiate the retrieval of external data. Instead, one or more trusted parties ("oracles") must create a transaction which embeds that data in the chain. This data is often gathered and stored in a traditional database by the oracle. Any interaction between a blockchain and the outside world is restricted to regular database operations.

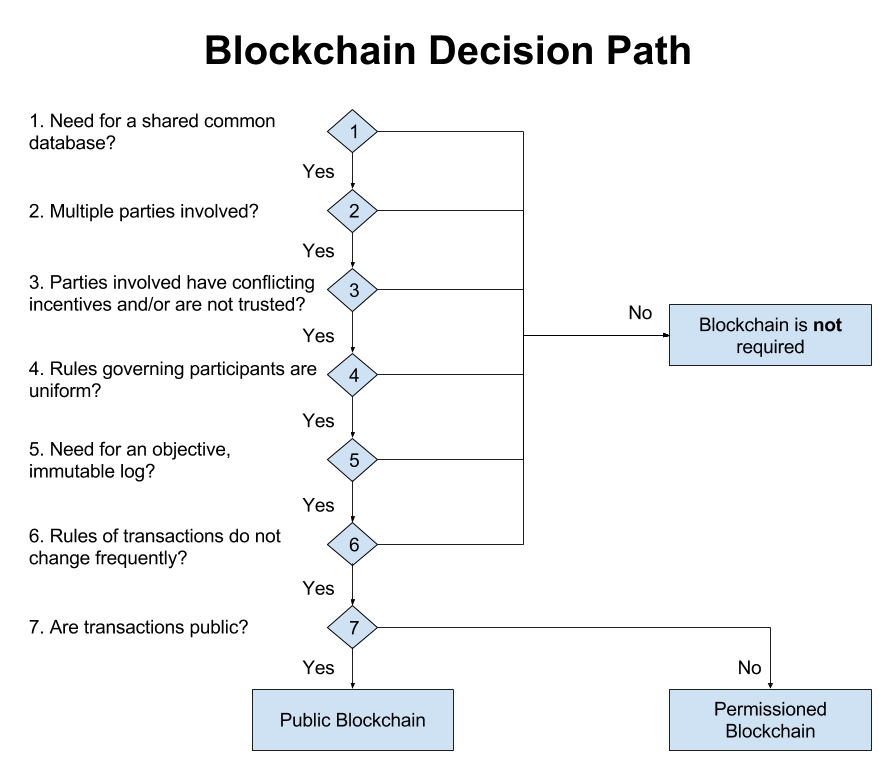
In other words, an oracle pushes data onto the blockchain, rather than a smart contract pulling it in. Once the oracle pushes the data, every node will have an identical copy of this data. This allows for the data to be safely used in a smart contract computation. While oracles allow for blockchain interface with external data, they undermine the goal of a decentralized system. Examine when such a trusted authority should be retained. When the trusted authority would or should be retained, efficiencies in the blockchain are not as high as in other applications.

### V. Simpler Alternatives

For some applications, other options are simply more efficient. When evaluating blockchain technology, consider whether regular file storage, a centralized database, or database replication with master/slave relationship between the original and copies is suitable. If those structures are suitable, then you can deploy your application with reduced complexity. Do you need a smart contract or are stored procedures written in an extension of SQL sufficient? Similarly, some applications can simply utilize cryptographic methods common in blockchains, without the database replication mechanisms of a blockchain.

### Blockchain Decision Path

The following diagram provides generalized, high-level decision points about when to use or not to use blockchain technology for your business.



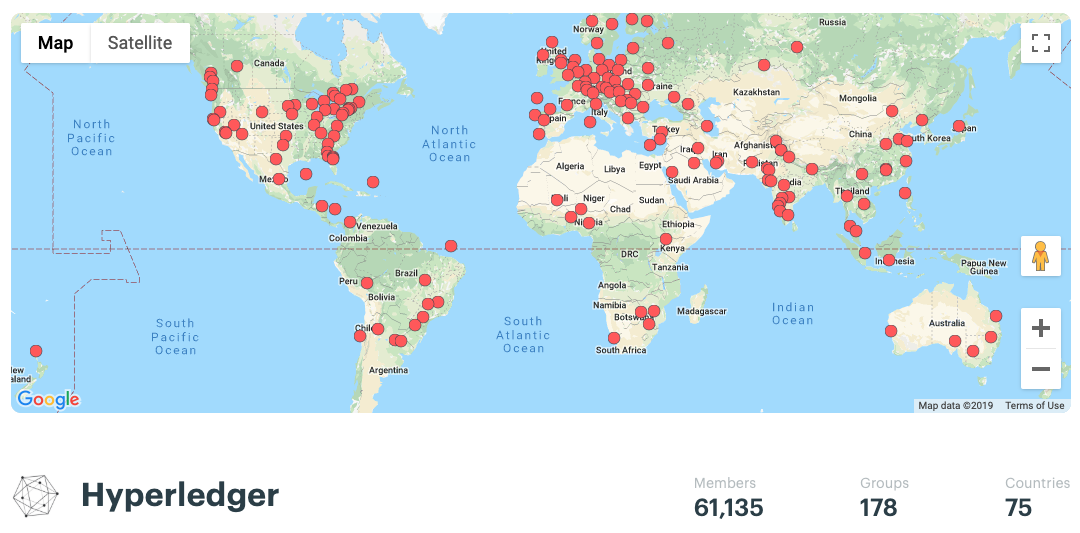
### Hyperledger Community

The development of the Hyperledger projects is led by a diverse group of technical, open source contributors. We are always looking for help to build an open source ecosystem of business blockchain technologies. If you are interested in contributing to and learning from the community, we welcome you to [join the Hyperledger effort](https://www.hyperledger.org/community).

### Joining the Hyperledger Community

You too can join the Hyperledger Community:

* **For developers**  
  Read the Hyperledger code on [GitHub](https://github.com/hyperledger/hyperledger). Join the Hyperledger discussion at [Rocket.Chat](https://chat.hyperledger.org/home" \t "_blank). Search for open bugs, or report a new one in the [Hyperledger’s bug database](https://jira.hyperledger.org/secure/Dashboard.jspa).
* **For business leaders**  
  For key updates from Hyperledger, join the [mailing list](https://lists.hyperledger.org/mailman/listinfo). Explore all Hyperledger [business solutions](https://www.hyperledger.org/projects).
* **For educators and community leaders**  
  You can start or join a [Hyperledger meetup](https://www.meetup.com/pro/hyperledger/). Development updates from Wiki can be found [here](https://wiki.hyperledger.org/).



**Hyperledger Global Meetups (as of 06/24/2019)**

### Hyperledger Working Groups

The Hyperledger Community’s working groups are open to the public. Developers and tech leaders can engage with any of the Hyperledger’s open community channels at this [page](https://wiki.hyperledger.org/display/HYP/Calendar+of+Public+Meetings).

Below, you can see an overview of Hyperledger’s working groups:

* [Architecture Working Group (AWG)](https://wiki.hyperledger.org/display/AWG/Architecture+Working+Group)  
  This is a technical workgroup focused on developing an architectural framework for Enterprise class distributed ledgers, towards convergence on a modular architecture.
* [Identity Working Group](https://wiki.hyperledger.org/display/IWG/Identity+Working+Group)  
  This group discusses, researches, and documents ways to capture, store, transmit and use identities on DLT, with a focus on projects under the Hyperledger umbrella.
* [Learning Materials Development Working Group](https://wiki.hyperledger.org/display/LMDWG/Learning+Materials+Development+Working+Group)  
  This group is focused on developing open source training material to educate people on Hyperledger and its projects.
* [Performance and Scale Working Group](https://wiki.hyperledger.org/display/PSWG/Performance+and+Scale+Working+Group)  
  This group discusses, researches, and identifies key metrics that relate to the performance and scalability of a blockchain and blockchain related technologies.
* [Smart Contracts Working Group](https://wiki.hyperledger.org/display/SCWG/Smart+Contracts+Working+Group)  
  This group focuses on giving an academic perspective to this research topic and also on practical ways to utilize them on different DLTs that are under the Hyperledger umbrella, and explores all potentials from deploying them in everyday software solution scenarios.
* [Technical Working Group China](https://wiki.hyperledger.org/display/TWGC/Technical+Working+Group+China)  
  This group acts as a bridge between the global Hyperledger community and the emerging technical user and contributor community in China.

### Learning Materials Development Working Group

The [*Hyperledger Learning Materials Development Working Group*](https://wiki.hyperledger.org/display/LMDWG/Learning+Materials+Development+Working+Group) is focused on developing training materials that aims to expand people's knowledge of Hyperledger and its projects. Members of this group collaborate with other Hyperledger working groups, Hyperledger team members, project maintainers, and volunteers from all over the world to identify training needs, identify strategies and solution to address those needs, and develop training material that targets both technical and non-technical audiences.

Among other things, members of this working group support the development of this MOOC by reviewing existing content and contributing new material, suggesting improvements, as well as providing assistance in the course forum when needed.

If you would like to contribute to Hyperledger projects, you don't have to be a technical guru to do so. There are many ways to help, and working on developing training materials is one of them. Anyone is welcome to join this group to learn more about how to get involved.

### Hyperledger Special Interest Groups (SIGs)

There are also a number of Special Interest Groups in the Hyperledger Community, focused on specific industries. You can learn more about these groups and their focus:

* [Healthcare SIG (HC-SIG)](https://wiki.hyperledger.org/display/HCSIG/Healthcare+SIG)  
  This group represents an international membership of healthcare and technology professionals united in advancing the state of the healthcare industry through the implementation of enterprise-grade technology solutions utilizing the Hyperledger greenhouse of business blockchain frameworks and tools.
* [Public Sector SIG](https://wiki.hyperledger.org/display/PSSIG/Public+Sector+SIG)  
  This group is focused on applying DLT in general, and Hyperledger technologies in particular, to the public sector uses and needs.
* [Social Impact SIG](https://wiki.hyperledger.org/display/SISIG/Social+Impact+SIG)  
  This group is primarily focused on serving as a platform for exchanging ideas and exploration of ways to use blockchain technology in the context of social good.
* [Telecom SIG](https://wiki.hyperledger.org/display/TCSIG/Telecom+SIG)  
  This group focuses on technical and business-level conversations about blockchain use cases in the Telecom industry.
* [Trade Finance SIG](https://wiki.hyperledger.org/display/TFSIG/Trade+Finance+SIG)  
  This group is focused on DLT and Hyperledger technologies applications to the trade finance uses and needs.

### Conclusions

This concludes the*LFS171x "Introduction to Hyperledger Technologies*" course! We have introduced you to the current Hyperledger frameworks and tools, and we have highlighted some of the business blockchain applications.

We hope this course inspires you and helps you continue your journey into the business blockchain technology world. Whether you are an engineer, entrepreneur, developer, educator, or business person, we look forward to seeing what you build, as well as hearing from you in the course forum.

Good luck to all of you in your future endeavors!

…the end.