Course introduction

Introduction to Blockchain

Introduction to Blockchain is the first course in the AWS Blockchain series. This course is intended for anyone that's interested in gaining a foundational understanding of blockchain technology and a better understanding of how Amazon Web Services (AWS) supports blockchain.

By completing this course, you should be able to:

Introduction to Blockchain

Introduction to Blockchain is the first course in the AWS Blockchain series. This course is intended for anyone that's interested in gaining a foundational understanding of blockchain technology and a better understanding of how Amazon Web Services (AWS) supports blockchain.

By completing this course, you should be able to:

- List blockchain core concepts.
- Compare and contrast blockchain and other similar technologies such as databases and ledgers.
- Explain the benefits of blockchain in solving business problems.
- State examples of blockchain technology applied in various industries.
- Recognize the challenges in establishing blockchain.
- Describe the basics concepts and functionality of Amazon Managed Blockchain.

This course provides a basic explanation of blockchain, discusses the technological evolution that lead to blockchain, and then discusses the benefits and core concepts that make blockchain work. It also covers things like the barriers to setting up a blockchain network, business use cases that benefit from blockchain, and briefly touches on Amazon Web Services Managed Blockchain solution.

To learn more, continue to the next lesson: Introduction to blockchain

Lesson 3 of 10

Introduction to blockchain

Blockchain is a globally recognized term among the IT community; however, it's not a globally understood technology. Many people think of blockchain and Bitcoin as synonymous. Blockchain, however, is much more than a cryptocurrency platform. Blockchain is a decentralized database that keeps a permanent record of all transactions. Once a record is written to a blockchain, it is unable to be altered. To better understand blockchain, it's important to be familiar with the concepts that lead up to blockchain.

At the end of this lesson, you should be able to:

At the end of this lesson, you should be able to:

- Recall an everyday example of blockchain technology that is currently in use.
- Understand what is meant by ledger, distributed ledger, and blockchain technology.

Everyday blockchain

The cryptocurrency Bitcoin is likely the first example of blockchain that you heard about. You may not have even know it was blockchain-based.

Bitcoin is a decentralized digital currency. That means it's not issued by a central bank. It also doesn't have a single entity controlling its value or distribution.

Bitcoin is designed to prevent counterfeiting or duplication of funds.

As blockchain's use has grown, additional cryptocurrencies have been created. The reason blockchain is so important to cryptocurrency is that it prevents currency from being duplicated. Someone can't simply go in and edit the amount of currency they have. They also can't spend the same currency

Everyday blockchain

The cryptocurrency Bitcoin is likely the first example of blockchain that you heard about. You may not have even know it was blockchain-based.

Bitcoin is a decentralized digital currency. That means it's not issued by a central bank. It also doesn't have a single entity controlling its value or distribution.

Bitcoin is designed to prevent counterfeiting or duplication of funds.

As blockchain's use has grown, additional cryptocurrencies have been created. The reason blockchain is so important to cryptocurrency is that it prevents currency from being duplicated. Someone can't simply go in and edit the amount of currency they have. They also can't spend the same currency twice—as soon as the currency is spent, it's transferred to the new holder and the old holder can't double-spend it.

Bitcoin represents a well-known example of blockchain technology in a practical application.

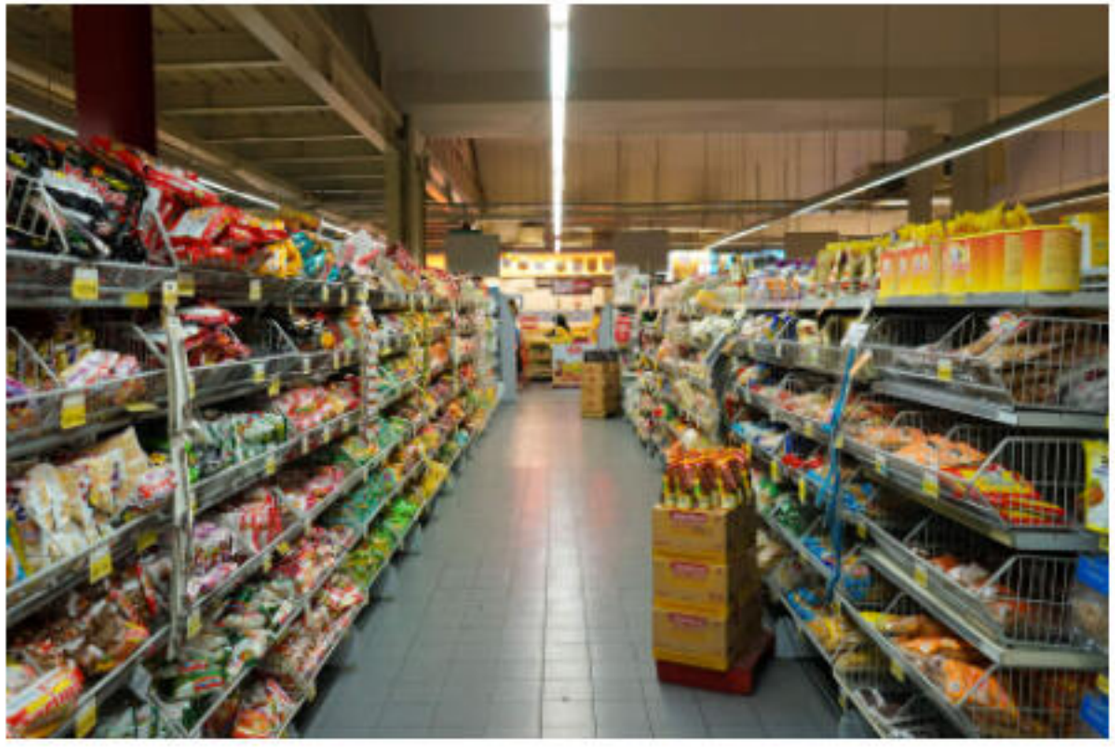
Having a complete, detailed transaction history for cryptocurrency is crucial for trust in cryptocurrency. Blockchain provides this complete, detailed history. What are some other use cases that might benefit from blockchain?

Shipping

A cargo ship being loaded with goods.

Major international shippers are starting to use blockchain technology to monitor shipments. Blockchain provides shippers with several valuable tools to maintain control of their customer's property. Every touch-point or interaction can be tracked and logged. Blockchain's consensus mechanisms ensure that all the data included is the data that was entered—nobody has manipulated the data after the fact. And finally, the record contains the entire history of a shipped item, from entering the shipping system through delivery.

Supply chain tracking



Grocery store full of product that could have it's entire path tracked using blockchain technology.

Grocers are starting to recognize that blockchain enables origin-to-destination tracking with detailed information every step of the journey. They can see the information at harvest, such as date, temperature, location, method, and so on. They can track the items from harvest all the way to checkout. They can monitor how long the item sat in a warehouse, how long it spent on a train or truck, and how long it's been sitting on their shelves. In the case of a foodborne illness, they can quickly isolate all the inventory from a specific plant and immediately know which of their customers purchased that inventory.

The path to blockchain

Now that you have an idea of some of blockchain's use cases, you can examine the path to blockchain, starting with ledgers.

Select the + symbol next to each category to learn more.

Ledgers +

Distributed Ledgers +

Blockchain +

Select the + symbol next to each category to learn more.

Ledgers

Oxford Learner's Dictionaries define a ledger as "a book or electronic document in which a bank, a business, etc. records the money it has paid and received."

Ledgers have been around in some form for over 5,000 years. Evidence exists of Mesopotamians keeping track of financial transactions on clay tablets. Ledgers have, obviously, come a long way since then.

The overall function of ledgers may not have changed much, but how they accomplish their function has changed quite a bit. Now, ledgers are frequently applications with a database behind them. A client application connects into the main database, reads current data, and sends updates. However, this is subject to tampering or data loss. With direct access to the source file, the file can be edited and swapped out, and the end user may never notice.

Distributed Ledgers

Distributed ledgers take the advantages of traditional or general ledgers and make them more resilient. Instead of having a single copy of the master data, a distributed ledger shares the full data set across several network participants (members); each member has a complete copy of the data.

This has various benefits. No single point has the master data file, so no single point can corrupt the master data file. If you lose one of the end points, the rest of the end points still maintain all the data. And when someone tries to make an update to the data in a distributed ledger, all the other end points are involved in the process of accepting or rejecting the update. In a distributed ledger, any updates must be agreed upon by the others—making it very hard to hack.

Blockchain

Blockchain is a distributed ledger that adds immutability. Immutability means that once something is written, it can't be edited or removed. With blockchain, data cannot be modified. The full history of data can be traced back to the start of the blockchain. Blockchain is a chain of transactions, contained in blocks, hence the name blockchain.

Every time a piece of information is changed, instead of updating the value and losing sight of what it used to be, blockchain simply adds a new block that holds the new data, while continuing to maintain all the old data as well.

Benefits of blockchain

You should now understand some of the basics of blockchain. You should also recognize some of the differences between blockchain, ledger, and distributed ledger. Now, you will examine some of the benefits that blockchain provides.

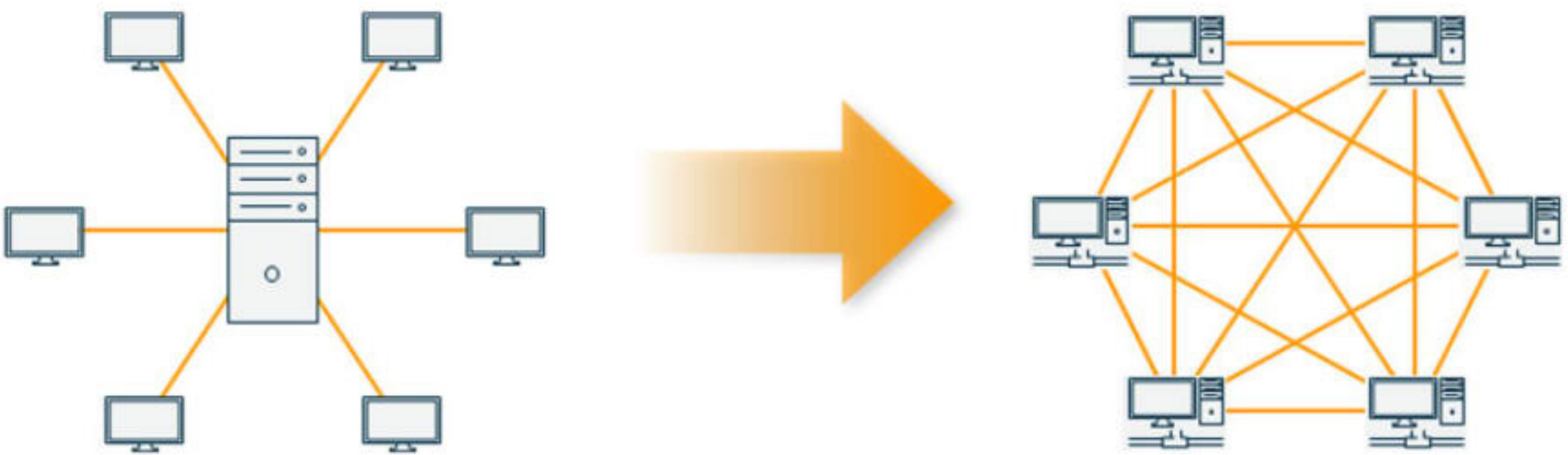
At the end of this lesson, you should be able to:

- Explain the concepts of decentralization, transparency, immutability, and auditability as they related to blockchain.

Increased trust, data security, and data integrity are some of the key benefits you can gain with blockchain. Decentralization, transparency, immutability, and auditability all support these benefits.

Decentralization

Decentralization means that each member of a blockchain has a complete copy of the data. Each member having a copy of the data protects against bad actors, improves disaster recovery, and promotes high availability.



When each member has a complete copy of the data, and updates to the data must be approved by the members, bad actors are stopped. If a illegitimate member or user attempts to delete the entire blockchain from a member, the other members retain the information, so no data is lost. If a bad actor tries to edit the historical data of one member, the other members will refuse to authenticate it. This denial prevents the false information from entering the blockchain.

Additionally, modern application development recognizes that monolithic architectures aren't always efficient. Putting all your trust in a large, single bucket increases the risk profile if anything happens to that bucket. In the same way, keeping all your data in a central, large, authoritative database or ledger increases risk of compromise or loss.

Each member has a complete copy of the data set. If a portion of the network goes down and takes down a member with it, the remaining members are able to validate and accept updates to the data structure. When the network is back up, that isolated member will be updated with the newest data set.

Transparency

Another piece of blockchain that increases trust is transparency. Transparency means that the information stored in the blockchain is visible to the members of the blockchain. Blockchain maintains a complete record of all transactions, and that record is available to every member, making blockchain a very transparent technology.

If we think of an agricultural example, at every step of the way, the people involved can see the whole path to date. So, the shipping company can see all the information about when and where the blueberries were harvested.

The distributor can see all of that, plus information on the shipping company:

- Which truck transported the blueberries

The distributor can see all of that, plus information on the shipping company:

- Which truck transported the blueberries
- Who the driver was
- How long the trip took
- What the truck temperature was

Additionally, the grocery store gets to see all that information as well, all the way back to when and where the berries were initially harvested. And because all the members have all the data, the farmer who initially grew the berries can see when they arrived at their destination and how they got there.

That level of transparency helps build trust, because everyone is able to see what is going on with their product.

That level of transparency helps build trust, because everyone is able to see what is going on with their product.

Some blockchain technologies, such as Hyperledger Fabric, provide data privacy as a native mechanism within the blockchain. With channels, you can create separate channels of the blockchain to share the data that makes sense to share, without losing any of the previous information. For example, if the distributor had contracts with multiple restaurants, grocery stores, and wholesalers, they could branch the data off to each group. Each customer would be able to track all the way back to the harvest, but the purchase price and volume could stay between the distributor and the buyer.

When you think of all the data available, and the fact that everyone can see what's in the block on a public blockchain, transparency really helps increase trust in the data. However, that trust in the data is only really possible because of immutability.

Immutability

Immutability simply means something cannot be edited or changed. You can update the information in a blockchain by adding data, which will be added in a new block. However, once a block is part of the chain, the information in that block can't be changed.

The immutability of blockchain is directly tied to its decentralization. Even if someone were able to edit the information in an already written block and try to push that information into the blockchain, it wouldn't work. As soon as the change was made on one member, and an attempt made to synchronize back up with the rest of the chain, the rest of the members would recognize a problem. Once the problem was recognized, the update would be blocked.

This immutability builds trust by letting everyone viewing the information on a blockchain know that the information hasn't been tampered with. With traditional databases, if the master database gets compromised, it can be difficult to prove that the data was tampered with and also to know, with certainty, what the correct data is. With blockchain, you can be sure that the data you're viewing was the originally written data and that nobody went in after the fact and modified it.

Auditability

Auditability is another benefit of using blockchain. Auditability speaks to how readily available and accessible something is to audit. Blockchain, relying on the other benefits already discussed, is a very auditable platform.

With blockchain's transparency, the auditor can investigate the blockchain and see all the transactions across time. They're able to know exactly what happened, when it happened, where it happened, and how it happened.

With blockchain's immutability, a complete audit log for every interaction is created. This can be shared with an auditor, who knows the data hasn't been compromised. Auditors can also compare the data between two members to validate the authenticity of the data.

Lesson summary

In this lesson, you learned about some of the key benefits of blockchain.

- Decentralization means that every member has a full copy of all the information, providing high availability, quick recovery, and protection from bad actors.
- Transparency helps build trust because everyone involved in the blockchain can see the history.
- Immutability works with transparency to further build trust. The inability of a blockchain to be retroactively edited means that the data is exactly what was entered initially.
- Auditability of blockchain leverages the other benefits. An auditor has a complete audit log for every interaction with the data in a blockchain. They can also compare the data from different members to verify the data's authenticity.

To learn more, continue to the next lesson: Blockchain core concepts

Blockchain core concepts

Now that you understand some of the key benefits of blockchain, it is a good time to discuss some of the core concepts that enable blockchain to work.

At the end of this lesson, you should be able to:

- Describe the basic concepts associated with blockchain, including blocks, cryptography, timestamping, peer-to-peer networking, blockchain types, smart contracts, and consensus mechanisms.

- Paraphrase the process flow that blockchain follows when it works, from initiation to settlement.

Blocks

Blocks are the basic unit of information in blockchain. Recall that a set of transactions results in a new block being created and added into the blockchain after the previous block.

A block itself has three primary components. The block is made up of the information for the current transaction, a cryptographic hash of the previous block, and a time stamp.

Select each tab to learn about each category.

TRANSACTION DATA | CRYPTOGRAPHIC HASH | TIMESTAMPING

The transaction data is the actual information relevant to the blockchain. The information contained will be largely dependent on the purpose of the transaction and the blockchain. Financial blockchains may see an addition of funds. Supply-chain blockchains may see an item change custody at a shipping point. Health information blockchains may see information related to a doctor visit. Regardless of the type of blockchain, all the blocks will also contain metadata about the transaction as well.

Select each tab to learn about each category.

TRANSACTION DATA | CRYPTOGRAPHIC HASH | TIMESTAMPING

A block also contains a cryptographic hash of the previous block in the blockchain. A cryptographic hash is a unique string of characters that can only be created using the information in the block and the cypher key. The hash is unique such that no other block, combined with the key, would produce the same hash. Additionally, if any of the data were changed in the block, the hash would also change. This process of creating a cryptographic hash of the previous block relates to blockchain's immutability.

Because the cryptographic hash is unique to the exact information that was in the previous block when the hash was created, any attempt to modify the information in the previous block would cause the hash to change. This reaction happens for every block in the blockchain.
For example, suppose that someone tries to modify the first block in a four-block blockchain. The fourth block has a cryptographic hash of the third block's data. The third block has a hash for the second. And the second block has a hash for the first. By modifying the data in the first block, the cryptographic hash in the second block would change. That data change in the second block would cause a change in the cryptographic hash in the third block. The data change in the third bock would alter the hash contained in the fourth block.

By using cryptographic hashes for the previous block as part of the dataset for a new block, blockchain makes it nearly impossible to make an undetectable change to data that's already written to the chain.

Select each tab to learn about each category.

TRANSACTION DATA | CRYPTOGRAPHIC HASH | TIMESTAMPING

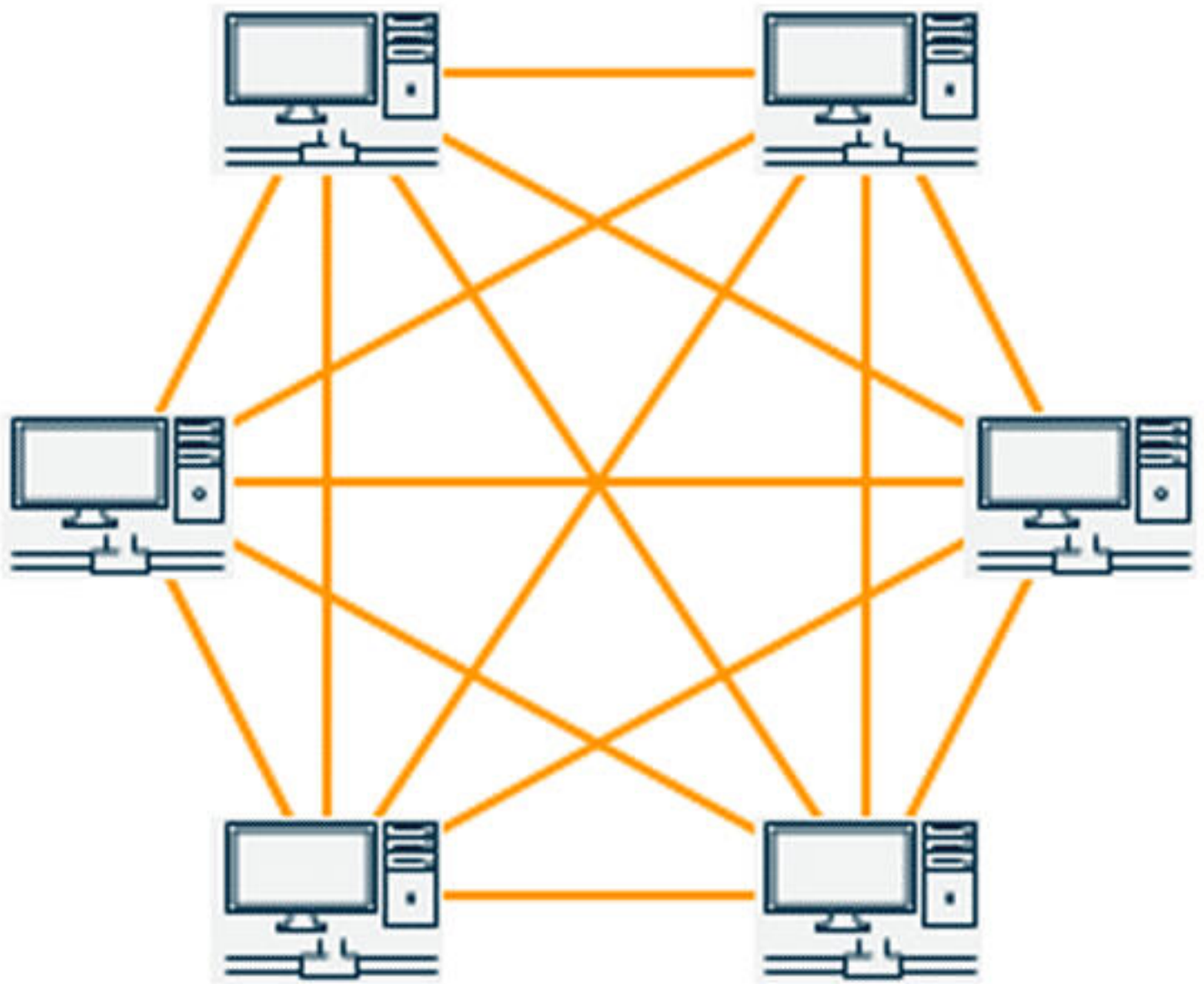
The third piece of information in a block on a blockchain is a timestamp. Timestamps serve two purposes. The obvious purpose of a timestamp is to know when a block was added to the blockchain. Due to the timestamp being part of a block, the cryptographic hash already discussed will vary based on the timestamp. This means that attempting to submit an edited block with a modified timestamp will run into the same problem with changing hashes, and will ultimately be rejected by the blockchain.

A second purpose of the timestamp is to show that the blocks are in chronological order of creation. This is important for auditability of the blockchain, because it ensures that any audit can validate the order information as attached to the blockchain.

Peer-to-peer network

Using a peer-to-peer network helps make blockchain fault tolerant, transparent, and distributed.

With the peer-to-peer network, each member of the blockchain is equal. Each member's blockchain data is equal. Each member can reach out to any other member for an update and pushes out updates to other members. Each member of the blockchain also has an equal vote on deciding if an update to the data on the blockchain should be accepted. All of the members having the same data means the data, while complete on any single member, is also distributed and decentralized across all members of the peer-to-peer network.



In a peer-to-peer network, all of the members talk to each other directly.

In a peer-to-peer network, all of the members talk to each other directly.

Peer-to-peer networking also means that a network disruption impacting some of the peers won't impact the entire blockchain. In a traditional primary-secondary relationship, the loss of the primary would cause a disruption. In a peer-to-peer network, because all members are equal, a network disruption doesn't prevent the blockchain from continuing to function. Once the disruption is resolved, the impacted members can reach out to any of the other members of the peer-to-peer network to get updated to the latest blockchain data set.

Consensus mechanisms

Blockchains immutability is directly related to consensus mechanisms. A consensus mechanism is a set of rules put in place by the blockchain that determines how all the members recognize a valid block addition.

Consensus mechanisms

Blockchains immutability is directly related to consensus mechanisms. A consensus mechanism is a set of rules put in place by the blockchain that determines how all the members recognize a valid block addition.

Consensus mechanisms are how each member of a blockchain knows that the information they are receiving is valid information. Without a consensus mechanism, anyone could submit an update to the blockchain and the chain would get updated.

Consensus mechanisms protect the blockchain network in several ways. As mentioned, consensus mechanisms let all the members know that an update is valid, and that the update was made by a member of the blockchain. Consensus mechanisms also set the standard for how members prove to the rest of the chain that an update is valid.

Finally, consensus mechanisms enable the distributed nature of the blockchain. Through the

Consensus mechanisms are how each member of a blockchain knows that the information they are receiving is valid information. Without a consensus mechanism, anyone could submit an update to the blockchain and the chain would get updated.

Consensus mechanisms protect the blockchain network in several ways. As mentioned, consensus mechanisms let all the members know that an update is valid, and that the update was made by a member of the blockchain. Consensus mechanisms also set the standard for how members prove to the rest of the chain that an update is valid.

Finally, consensus mechanisms enable the distributed nature of the blockchain. Through the consensus mechanisms, peers are able to share updates to the blockchain, and ensure that everyone on the peer-to-peer network is using the same data set.

There are multiple different consensus mechanisms out there, they work in different ways, and they have different trade-offs. Proof of work and proof of stake are two common consensus mechanisms that we'll cover in more detail.

Mechanism examples

Proof of Work and Proof of Stake are two common examples of consensus mechanisms. Both are commonly used in cryptocurrency applications, and have different trade-offs.

Select each tab to learn about each category.

PROOF OF WORK | PROOF OF STAKE

Proof of work is a consensus mechanism in which members solve mathematical puzzles. The first member to solve the puzzle is trusted and is able to create the next block on the blockchain. This consensus mechanism prioritizes the member that's put the most effort into solving a puzzle to determine who writes the next block. Though a proof-of-work blockchain gives each member an equal opportunity to create the next block, it can be very process intensive (and therefore energy intensive).

Mechanism examples

Proof of Work and Proof of Stake are two common examples of consensus mechanisms. Both are commonly used in cryptocurrency applications, and have different trade-offs.

Select each tab to learn about each category.

PROOF OF WORK | PROOF OF STAKE

In a proof of stake mechanism, the more cryptocurrency a member has, the greater trust is given to that member. With this increased trust comes an increased likelihood of being the member that creates the next block on the blockchain. Proof of stake is far less resource intensive than proof of work. However, proof of stake doesn't treat all members equally. Instead, it focuses on which members have the most coins.

Smart contracts

Another core concept of blockchain is a smart contract. A smart contract is a contract that executes without any additional action required by a third party. With a smart contract, you establish the terms and conditions of the contract. Once the terms and conditions of the contract are met on the blockchain, the contract automatically executes—without you needing to take any action.

For example, suppose a customer wants to make a large purchase. Traditionally, the customer would deposit money in an escrow account with a third party. The third party would hold the money until you fulfilled the customer order. At the point when the order is fulfilled, the escrow company would validate that the customer had their items. Then the escrow company would transfer the funds to you.

With a smart contract, the third party is removed from the equation. Blockchain would track the

transfer the funds to you.

With a smart contract, the third party is removed from the equation. Blockchain would track the shipment each step of the way. Once the shipment arrived with the customer, the ownership of the item would transfer to the customer and the funds would transfer to you. All this happens automatically, based on the smart contract you set up—no third party needed. This exchange also happens simultaneously. As soon as the contract is fulfilled, ownership of the item and funds are transferred. Until the contract is fulfilled, nothing is transferred. This avoids having currency or inventory hanging out in limbo waiting for the system to catch up and process a transaction.

Blockchain types

There are three main types of blockchains: permissionless, permissioned, and consortium. The type of blockchain will determine how widely the blockchain is shared and who has the ability to make updates to the blockchain.

Select the + symbol next to each category to learn more.

Permissionless

A permissionless blockchain, also known as a public blockchain, is an open blockchain. All the information on a permissionless blockchain is viewable by all members, and all members are equally empowered to make updates to the blockchain.

Because a permissionless blockchain is public, anyone can become a member of the blockchain, read the information, and contribute. A permissionless blockchain is great for broad, unrestricted collaboration. However, it has the least amount of control of who can see what information.

Permissioned

A permissioned, or private, blockchain is a blockchain in which membership is controlled by a central authority. Despite having a central authority that determines who is authorized to be a member of the blockchain and make updates, the decentralized principle of blockchain still applies.

A permissioned blockchain enables you to leverage the power of blockchain while also keeping relevant information protected from public view. A permissioned blockchain also enables you to control who is eligible to be a member of the blockchain.

Consortium

A consortium blockchain is a middle ground between permissionless and permissioned. A consortium blockchain still restricts access to the blockchain, but has a more distributed central authority. This allows a greater member set than a permissioned blockchain, while still protecting information from general public availability.

An example of a consortium blockchain might be if you partnered with two other companies. Each company would be able to control who, from its organization, are members of the blockchain. This leverages greater collaboration and sharing than if each company established its own private blockchain with no transparency to the other partners. However, even with the increased sharing, the consortium blockchain still keeps your and your partners' information restricted to only those that are part of the blockchain.

Lesson summary

In this lesson, you explored the benefits and relationships of blockchain and it's core concepts.

- You learned that consensus mechanisms enable members to know that a new block is valid. Consensus mechanisms also let members know how to create valid blocks to distribute across the blockchain.
- You also learned how the cryptographic hash greatly increases the immutability of blockchain and protects against editing of a previous block on the blockchain.

The lesson finished with a discussion on the different types of blockchains, and covered some of the benefits of public and private blockchains and how a consortium blockchain could bring benefits from both.

Blockchain frameworks

Now that you recognize some of the benefits of blockchain and understand some of the core concepts involved, it is time to learn about frameworks.

At the end of this lesson, you should be able to:

- Understand the basics of a blockchain framework.
- Recognize potential use cases for the Hyperledger Fabric and Ethereum frameworks.

What is a blockchain framework?

A blockchain framework is the set of standards on which a blockchain operates. Think of a framework as a piece of business software. Business software has a general purpose that it is designed for, a set of requirements to help it operate efficiently, and a set of guidelines for how to interact with it.

Blockchain frameworks function in a similar capacity. Frameworks provide a basic structure that a blockchain operates within. Like business software, frameworks have different purposes. Some frameworks are built specifically for cryptocurrency creation and tracking. Other frameworks are focused on collaboration and sharing of knowledge.

Blockchain frameworks also determine how your developers are able to interact with the blockchain. What languages are supported, how applications are built, and so on, are all determined by the framework.

The framework will also inform how information is shared and made available. Some frameworks have channels, so information can be shared only where it's needed. Others require that everything be fully public.

determined by the framework.

The framework will also inform how information is shared and made available. Some frameworks have channels, so information can be shared only where it's needed. Others require that everything be fully public.

It's important to understand the different frameworks and how to match a blockchain framework to your use case. Some key considerations when choosing a blockchain framework are:

- Your specific use case
- Available consensus mechanisms and their benefits and challenges
- Ease of use
- The developer community
- Licensing requirements
- Maturity of the blockchain framework

Ethereum

Ethereum is a permissionless, or public, cryptocurrency blockchain that provides a broad set of capabilities for using smart contracts, running applications, and executing code. Ethereum currently operates with a proof-of-work consensus mechanism. Ethereum 2.0 is intended to use a proof-of-stake consensus mechanism, reducing the compute intensity, but prioritizing members with more coins (or Ether).

Ethereum also has its own programming language (Solidity) that enables you to create applications within the Ethereum Virtual Machine (EVM). The EVM is a virtual machine in an Ethereum blockchain. Within the EVM, you can write, build, and run applications. You can even establish fees or charges, in Ether (Ethereum's cryptocurrency) for running an application.

You are able to charge for running an application in the EVM because Ethereum is a cryptocurrency blockchain that happens to be capable of running applications and executing smart contracts. Because of the cryptocurrency base, you can exchange currency when your application is run or when a smart contract is fulfilled.

Hyperledger Fabric

Hyperledger Fabric is a modular, permissioned (or private) blockchain framework focused on sharing information with the security and confidence of blockchain but maintaining privacy where needed. If you recall from the Benefits of Blockchain module, Hyperledger Fabric supports channels. With channels, you can control which information in a blockchain is visible to different peers.

For example, you can ensure that the shipping and tracking information for an order is available to everyone on the blockchain, while keeping the pricing information between you and the end customer only. You can create multiple channels to create the same effect for multiple customers, so everyone can see where products are shipping—but pricing information is kept confidential.

The modular focus of Hyperledger Fabric means that smart contracts and applications can often be easily repurposed or migrated from one area to another without having to rebuild or refactor the underlying code. So, if you have a smart contract that works with one customer, you don't have to rebuild the smart contract; you can simply replicate the smart contract and set it up for use with additional customers, saving development time and resources.

The modular focus of Hyperledger Fabric means that smart contracts and applications can often be easily repurposed or migrated from one area to another without having to rebuild or refactor the underlying code. So, if you have a smart contract that works with one customer, you don't have to rebuild the smart contract; you can simply replicate the smart contract and set it up for use with additional customers, saving development time and resources.

To build smart contracts, Hyperledger Fabric supports multiple programming languages, including Go, Java, and JavaScript. In fact, Hyperledger Fabric even supports Solidity (Ethereum's language) and the EVM.

Lesson summary

The blockchain framework is a software solution pack for a blockchain. It comes with commonly used functions, basic modules, repeatable code packets, and so on. It also possesses the standards to simplify the development, deployment, and maintenance of the blockchain solution.

The framework will determine which consensus mechanisms are available; whether the blockchain supports private, public, or consortium chains; and how the information in the blocks is shared across the blockchain network.

Challenges in establishing blockchain

As well as having a basic understanding of blockchain's functionality and benefits, it's also important to understand some of the challenges you might face in setting up your own blockchain.

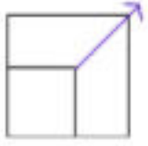
At the end of this lesson, you should be able to:

- Recognize the challenges in establishing blockchain.

Barriers to setting up blockchain

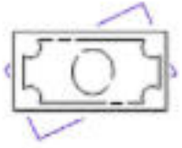
There are different barriers when setting up a blockchain network. Challenges that you should consider include setting up the actual network, ensuring your network is able to scale, managing costs, and keeping the network secure are all challenges you should consider.

Setup is hard



Hard to scale

Complicated to manage



Expensive

Setting up a blockchain network comes with several challenges.

Establishing the network

To establish a blockchain network, you need to decide on a blockchain framework and then configure the blockchain. Depending on the blockchain framework used, you may have to decide on your consensus mechanisms and get them in place, configure the network for private or public access, determine how new members join and leave the group, and so on. All this must be done while also ensuring that you have the compute power to get the blockchain off the ground and running.

After your blockchain is configured, you need to deploy. Setting up a test blockchain network that runs solely on your laptop may be relatively simple. However, fully deploying a blockchain network is more involved. Once the blockchain is configured, you need to finish configuring the network, including setting up VPNs, access points, and authentication. You also need to add members.

including setting up VPNs, access points, and authentication. You also need to add members.

The new members of the blockchain will need to:

- Provision and configure compute, storage, and networking hardware.
- Install software.
- Create and manage certificates.

With the deployment complete, you need to manage and maintain the network. Management and maintenance tasks vary depending on the network, but may include things like:

- Managing your certificates
- Inviting new members to join the network
- Tracking operational metrics such as usage of compute, memory, and storage resources

Scaling your network

When the blockchain network is up and running, you need to be sure it can continue to grow. Scaling blockchain comes in two varieties: scaling the number of members or scaling the processing power of the members. The ability to scale your blockchain is crucial to maintaining or even improving your transaction rate (the rate at which transactions on the blockchain are processed.

To scale the number of members on a blockchain, a mechanism needs to be in place to control how new members are added to or rejected from the blockchain. If it's a private blockchain, in addition to having a mechanism to add additional members, you also need to ensure you have enough compute capacity allocated for the new members.

To scale the processing power of a member, you need the ability to increase or decrease the number of nodes assigned to a member. By adding additional nodes, you are adding additional computing power to a member of the blockchain. Like scaling your number of members, if you're adding additional nodes, you need to have available compute power for the additional nodes.

Securing the blockchain network

Finally, you need the ability to secure the blockchain network.

On a public, or permission-less, blockchain, members can add themselves to the blockchain. Consensus mechanisms and voting help ensure that only valid information is written to the blockchain. However, anyone can become a member of the blockchain and then write to the blockchain, as long as they pass the consensus mechanisms.

On a private network, you need a way to control who has access to becoming a member as well as managing the private and public keys for the blockchain. If you have a consortium blockchain, you need to configure your network to not only control who you add as members, but also ensure that other participants in the blockchain have similar permissions, so they can add relevant members. All this must be accomplished while also keeping the network secure, avoiding unauthorized members from joining the blockchain, and preventing malicious parties from interacting with blockchain members.

members from joining the blockchain, and preventing malicious parties from interacting with blockchain members.

Managing blockchain costs

As your blockchain network grows, your associated costs are going to grow as well. Remember, providing a complete historical record of every transaction is one of the key benefits of blockchain. However, as each new block is added to the blockchain, the storage footprint of the blockchain will also increase. Similarly, depending on your consensus mechanism, each block may take more and more computing power to create and add to the blockchain.

Additionally, if you establish a private blockchain, you will also need a mechanism to share costs fairly with the other participants of the blockchain.

Pause and reflect...

fairly with the other participants of the blockchain.

Pause and reflect...

Take a moment to think about the challenges in establishing a blockchain network. What do you think will be your biggest challenge? Your biggest concern could be any of the following.

- Setting up the initial network
- Managing the addition and removal of members
- Being able to scale the network and members as needed
- Getting your security configuration correct
- or something else entirely

Lesson summary

Maintaining a blockchain network comes with different barriers to overcome, from the very first steps of choosing your blockchain framework, creating your first block, and establishing the network.

Once the network is established, you need to sort out how to handle scaling the network, both by adding members or adding additional compute power.

With the scalability of blockchain comes potentially increasing costs. Having a mechanism to fairly share the costs of maintaining a blockchain across participants can decrease the burden on a single entity and help distribute the burden better.

Finally, having a secure blockchain network means being able to control who is joining your private or consortium network. With all these concerns in mind, it is time to move on to the next module.

Solving your business problems using AWS services

Configuring and deploying a new blockchain can be a daunting task for anyone not already familiar with the process and technology. However, AWS makes standing up a blockchain simple with Amazon Managed Blockchain.

At the end of this lesson, you should be able to:

- Describe the basic concepts and functionality of Managed Blockchain.

Introduction to Managed Blockchain

Managed Blockchain puts the decentralization and immutability of blockchain at your fingertips. Managed Blockchain enables you to stand up a blockchain rapidly, using the reliability and scalability of the AWS Cloud. Managed Blockchain gives you the resilience, scalability, and cost optimization of the AWS Cloud while giving you full control over your blockchain application.

Managed Blockchain supports two popular blockchain frameworks:

- Hyperledger Fabric is a permissioned blockchain that is well suited for a situation where you need strict controls on privacy and security with a known group of members. Hyperledger Fabric also gives you the ability to create channels, sharing information only with the members who need to have visibility into the data.

- Ethereum is a permissionless blockchain that is well suited when a highly distributed blockchain with full transparency is needed. As a public blockchain, all members of the blockchain can see all data in the blocks.

Managed Blockchain makes both of these frameworks available to you in a fully-managed solution. That means you can focus on your blockchain and let AWS worry about maintaining the hardware, security, and networking needed to keep the blockchain up and running.

Amazon Managed Blockchain simplifies the tasks of: creating your network, inviting members, adding nodes, and deploy applications.

Managed Blockchain overview

Managed Blockchain provides solutions to each of the challenges encountered when trying to establish your own blockchain network.

Establishing the network

With Managed Blockchain, the network the blockchain is built on is the AWS Cloud. Establishing a blockchain network can be done in just a few steps from the AWS Management Console.

Managed Blockchain takes care of all the network configuration, resource provisioning, and software loading necessary for either Ethereum or Hyperledger Fabric.

Scalability

With Managed Blockchain, you can quickly scale out when needed by adding more members or adding more nodes to an existing member. When you create your blockchain, you set the voting threshold for new members to join the blockchain network. When a new member tries to join the network, the other members of the network will vote on the new member. If the votes exceed the threshold requirement, the new member will be allowed on the blockchain and becomes a contributing member.

Adding additional nodes to members associated with your AWS account is also easily accomplished. You can add nodes from the console, by using the AWS Command Line Interface (AWS CLI), or by interacting with the blockchain network using the API. By adding additional nodes to an existing member, you increase their ability to create and validate transactions. Managed Blockchain provides a variety of node types. This gives you the flexibility to choose compute or memory-focused nodes depending on your workload and need.

Securing the network

When it comes to making sure your blockchain network is secure, Managed Blockchain helps out in two ways.

First, your Managed Blockchain runs in the Amazon Virtual Private Cloud (Amazon VPC). By running in the Amazon VPC, your blockchain is protected by AWS infrastructure and services. Within the blockchain network, access and authorization for each resource is governed by processes defined within the network.

Outside the network—such as from a member's client applications and tools—Managed Blockchain uses AWS PrivateLink. AWS PrivateLink ensures that only network members can access required resources. In this way, each member has a private connection from a client in their VPC to the Managed Blockchain network.

And if you're deploying a Hyperledger Fabric blockchain, you'll need to establish a certificate authority. The Hyperledger Fabric certificate authority manages the identities of the members in your blockchain and determines their permissions. By running your blockchain with Managed Blockchain, you can leverage AWS Key Management Service (AWS KMS) to store the keys for the certificate authority. Using AWS KMS avoids having to set up your own security device to manage the keys for the certificate authority.

Alternatively, if your blockchain framework has different access and control features that you'd prefer to use, you can configure and use them within Managed Blockchain.

Managed Blockchain encrypts all data at rest on peer nodes using Managed Blockchain-owned encryption keys in the AWS KMS. This reduces the operational burden and complexity involved in protecting sensitive data. With encryption at rest, you can build security-sensitive blockchain applications that meet strict encryption compliance and regulatory requirements. Encryption at rest integrates with AWS KMS for managing the encryption key that is used to encrypt your tables. A Managed Blockchain-owned key is used to encrypt data at rest by default at no additional cost. No configuration is required.

Controlling costs

Establishing your own data center to run a blockchain network can be costly. You would also need to over-provision in order to support future growth, or you would be limited in your growth.

Managed Blockchain eliminates the operational overhead required to create the network and maintain your blockchain network. It manages your certificates and lets you easily invite new members to join the network. It also tracks operational metrics such as usage of compute, memory, and storage. Managed Blockchain can even replicate an immutable copy of your blockchain network activity into a database outside the network, enabling you to analyze network activity and gain insights into trends.

There is no up-front commitment with Managed Blockchain. For Hyperledger Fabric on Managed Blockchain, you simply pay an hourly charge (billed per second) for your network membership, peer nodes, and peer node storage, and you pay for data you write to the network. When you are finished with a Managed Blockchain network, you can easily leave the network or terminate it and stop paying. You only pay for the resources you use.

Lesson summary

Managed Blockchain solves many of the concerns or issues with setting up a blockchain network. Managed Blockchain is simple to set up, can scale at a moment's notice, and leverages AWS KMS to keep your network secure in the cloud.

Other applications of blockchain technology

At the beginning of this course, the Bitcoin example was used to provide a common starting point on which to build your foundational knowledge of blockchain.

Through this course, you've learned the basics of blockchain, including the terminology and concepts. You examined the barriers that can make standing up your own blockchain difficult. Amazon Managed Blockchain was briefly covered to highlight how a cloud provider with a blockchain platform can alleviate many of the barriers to establishing your own blockchain.

Now, it's time to branch away from the initial example of cryptocurrency and look at some other potential use cases for blockchain technology.

Other uses of blockchain

Blockchain's immutability, distributed nature, and transparency offer benefits that span far beyond cryptocurrency. From healthcare applications to government, and agriculture to finance, blockchain is just beginning to be tapped and isn't near its full potential.

Proof of Ownership

Documents/Contracts

Digital Security Trading

Enterprise Platforms

Mortgage Loans

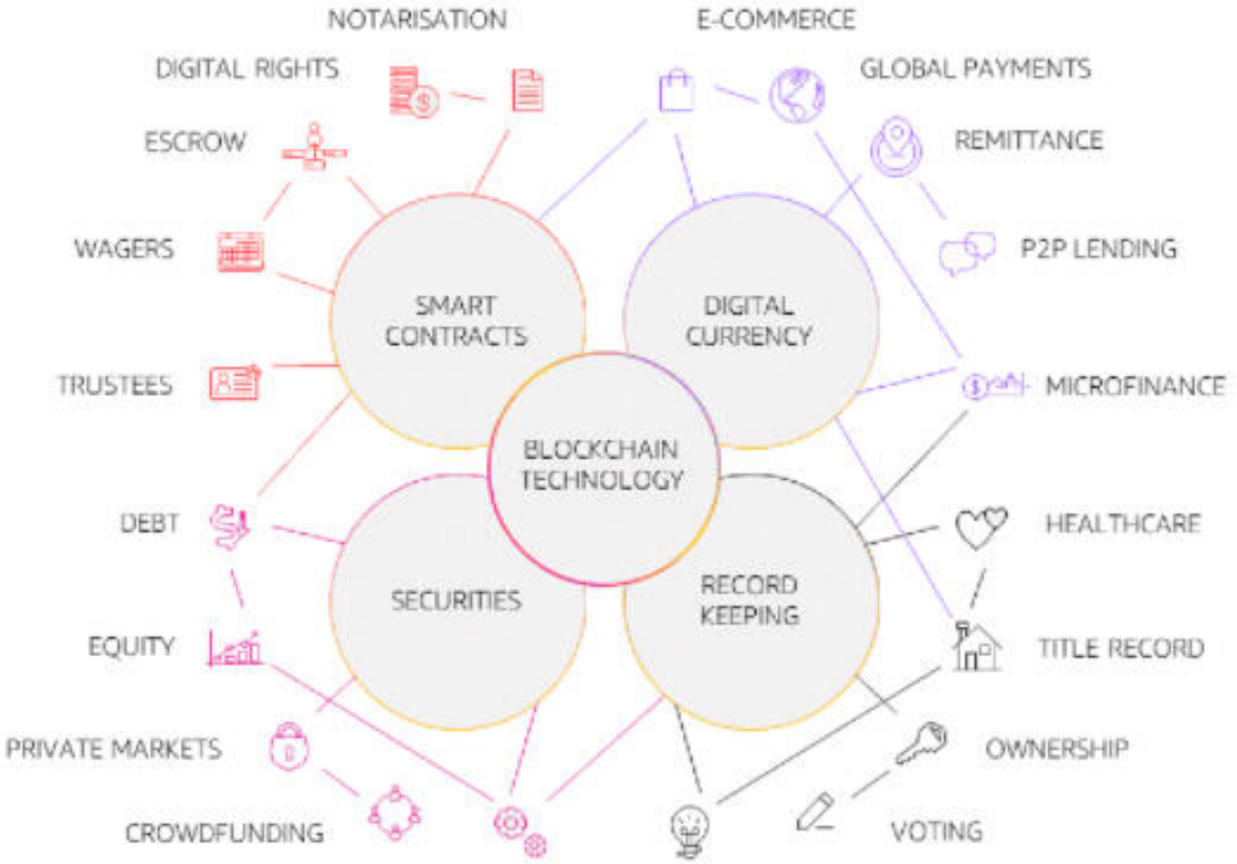
Voting Mechanisms

Patient Records

Corporate Governance

Financial

Insurance



Capital Markets

HCLS

Real Estate

Legal

Agriculture

Gaming

Transportation

M & E

Digital Advertising

Power/Utilities

Retail

Cloud

Research by firms such as Deloitte and McKinsey highlights that blockchain has applicability in all verticals, and is expected to increase and grow as familiarity with the technologies improves.

Keep this expected growth in mind as you read through the sample use cases, because regardless of the industry the use cases for blockchain are growing.

Healthcare

Blockchain in healthcare has multiple potential use scenarios. Consider patient care records. Creating a Hyperledger Fabric blockchain with channels would allow all providers to securely and confidently share patient information. Each office or hospital visit would be documented in an immutable archive. Each provider could see which notes were entered previously, when they were entered, and who entered them. The providers would also be able to review any previous updates to the health record. Knowing that nobody can delete information without a record of it, the provider and hospital also have an increased confidence in the completeness of the health record.

Healthcare

Blockchain in healthcare has multiple potential use scenarios. Consider patient care records. Creating a Hyperledger Fabric blockchain with channels would allow all providers to securely and confidently share patient information. Each office or hospital visit would be documented in an immutable archive. Each provider could see which notes were entered previously, when they were entered, and who entered them. The providers would also be able to review any previous updates to the health record. Knowing that nobody can delete information without a record of it, the provider and hospital also have an increased confidence in the completeness of the health record.

A Hyperledger Fabric blockchain has the capability to create channels. Because of this, deidentified information or general information such as blood type and vitals could be shared with all trusted members of the blockchain, while sensitive information could be kept in channels that protected the patient's privacy but kept providers informed.

A Hyperledger Fabric blockchain has the capability to create channels. Because of this, deidentified information or general information such as blood type and vitals could be shared with all trusted members of the blockchain, while sensitive information could be kept in channels that protected the patient's privacy but kept providers informed.

Or consider the impact on pharmaceuticals. With a blockchain solution, doctors and pharmacists would know exactly what a patient had been prescribed, how long they'd been on the medication, the last time the prescription was filled, and if the patient or a family member filled the prescription. Because of the immutability and transparency of blockchain, doctors and pharmacists wouldn't have to rely on patients remembering the myriad of drugs they may be on. They could check the blockchain and know right away if there was a potential conflict in the prescriptions.

Government

Government is an area with the largest potential for blockchain adoption and use. In the government sector, everything from voting to procurement, taxes to public health, has blockchain potential.

Currently, companies and individuals are expected to file their taxes and either make a payment or wait for a refund. However, it's a cumbersome system with multiple manual touchpoints that delay payments and refunds. With a blockchain-based system, smart contracts could automatically transfer payments or refunds between the government and the company or individual. Auditing of the tax information becomes simpler with blockchain's immutability and transparency. If you add in smart contracts, blockchain in government can also help expedite the processing of taxes or other government functions. Additionally, the risk of the information becoming corrupted, lost, or otherwise compromised is effectively removed with the decentralized and immutable nature of blockchain.

Currently, companies and individuals are expected to file their taxes and either make a payment or wait for a refund. However, it's a cumbersome system with multiple manual touchpoints that delay payments and refunds. With a blockchain-based system, smart contracts could automatically transfer payments or refunds between the government and the company or individual. Auditing of the tax information becomes simpler with blockchain's immutability and transparency. If you add in smart contracts, blockchain in government can also help expedite the processing of taxes or other government functions. Additionally, the risk of the information becoming corrupted, lost, or otherwise compromised is effectively removed with the decentralized and immutable nature of blockchain.

Property and land management is another potential area for government to leverage blockchain. Instead of having to conduct searches and dig through old files to determine the legal owner of a property, a blockchain solution would provide a log trail of current and past owners, as well as any other information that would typically be publicly available, including tax payments, assessments, transfers, and so on.

Agriculture

As discussed early in this training, agriculture is a natural industry for blockchain. The ability to track an item from the farm where it was harvested all the way to the final destination gives consumers greater confidence in the manner and method in which items are harvested.

With the use of smart contracts and channels (remember, channels are only available with Hyperledger Fabric), general information can be kept public while the details of individual negotiations can stay between the seller and purchaser for that contract. Payment can be transferred as soon as the shipment is received via smart contracts, removing the need for the payment to be held in escrow.

Finance and commerce

Finance and commerce is another segment with broad potential for the adoption of blockchain as the technology matures. The decentralization and immutability of blockchain make it an ideal match for finance and commerce transactions.

By leveraging smart contracts, finance companies could work with customers and other businesses to quickly transfer funds when assets have been delivered. The immutability and transparency of blockchain reduces the risk of fraud and provides a perfect record of all the events involved in a transaction.

In auctions or live trading of resource, stocks, or other commodities, the timestamp establishes who submitted a purchase or sale first. Those records could all be stored on the blockchain, with the transparency to enable auditing, the immutability to reassure all involved parties that the data is valid, and the decentralization to protect all the records from malicious actors who would try to corrupt the data.

Lesson summary

As blockchain evolves, its impact will cross all sectors. Some sectors are already getting involved in blockchain to see how they can expand the use beyond the initial focus on cryptocurrency. Blockchain's inherent nature—immutable, transparent, and decentralized—makes it well positioned to help solve business problems in an ever-changing e-commerce world.

To see how some of our customers are leveraging the power of Managed Blockchain, explore the Amazon Managed Blockchain Customers tab at https://aws.amazon.com/managed-blockchain/customers/?nc=sn&loc=7.