If you have been following banking, investing, or cryptocurrency over the last ten years, you may be familiar with “blockchain,” the record-keeping technology behind the Bitcoin network. And there’s a good chance that it only makes so much sense. In trying to learn more about blockchain, you've probably encountered a definition like this: “blockchain is a distributed, decentralized, public ledger."

The good news is that blockchain is actually easier to understand than that definition sounds.

What is Blockchain?

If this technology is so complex, why call it “blockchain?” At its most basic level, blockchain is literally just a chain of blocks, but not in the traditional sense of those words. When we say the words “block” and “chain” in this context, we are actually talking about digital information (the “block”) stored in a public database (the “chain”).

“Blocks” on the blockchain are made up of digital pieces of information. Specifically, they have three parts:

1. Blocks store information about transactions like the date, time, and dollar amount of your most recent purchase from Amazon. (NOTE: This Amazon example is for illustrative purchases; Amazon retail does not work on a blockchain principle as of this writing)
2. Blocks store information about who is participating in transactions. A block for your splurge purchase from Amazon would record your name along with Amazon.com, Inc. (AMZN). Instead of using your actual name, your purchase is recorded without any identifying information using a unique “digital signature,” sort of like a username.
3. Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a “hash” that allows us to tell it apart from every other block. Hashes are cryptographic codes created by special algorithms. Let’s say you made your splurge purchase on Amazon, but while it’s in transit, you decide you just can’t resist and need a second one. Even though the details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

While the block in the example above is being used to store a single purchase from Amazon, the reality is a little different. A single block on the Bitcoin blockchain can actually store around 1 MB of data.[1] Depending on the size of the transactions, that means a single block can house a few thousand transactions under one roof.

Volume 75%

1:08

What Is the Blockchain?

How Blockchain Works

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

1. A transaction must occur. Let's continue with the example of your impulsive Amazon purchase. After hastily clicking through multiple checkout prompt, you go against your better judgment and make a purchase. As we discussed above, in many cases a block will group together potentially thousands of transactions, so your Amazon purchase will be packaged in the block along with other users' transaction information as well.
2. That transaction must be verified. After making that purchase, your transaction must be verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone in charge of vetting new data entries. With blockchain, however, that job is left up to a network of computers. When you make your purchase from Amazon, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, dollar amount, and participants. (More on how this happens in a second.)
3. That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction's dollar amount, your digital signature, and Amazon's digital signature are all stored in a block. There, the transaction will likely join hundreds, or thousands, of others like it.
4. That block must be given a hash. Not unlike an angel earning its wings, once all of a block's transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.

When that new block is added to the blockchain, it becomes publicly available for anyone to view—even you. If you take a look at Bitcoin’s blockchain, you will see that you have access to transaction data, along with information about when (“Time”), where (“Height”), and by who (“Relayed By”) the block was added to the blockchain.

Is Blockchain Private?

Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network as nodes. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added, sort of like a Facebook News Feed that gives a live update whenever a new status is posted.

Each computer in the blockchain network has its own copy of the blockchain, which means that there are thousands, or in the case of Bitcoin, millions of copies of the same blockchain. Although each copy of the blockchain is identical, spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn’t a single, definitive account of events that can be manipulated. Instead, a hacker would need to manipulate every copy of the blockchain on the network. This is what is meant by blockchain being a "distributed" ledger.

Looking over the Bitcoin blockchain, however, you will notice that you do not have access to identifying information about the users making transactions. Although transactions on the blockchain are not completely anonymous, personal information about users is limited to their digital signature or username.

This raises an important question: if you cannot know who is adding blocks to the blockchain, how can you trust blockchain or the network of computers upholding it?

Is Blockchain Secure?

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the “end” of the blockchain. If you take a look at Bitcoin’s blockchain, you’ll see that each block has a position on the chain, called a “height.” As of August 2020, the block’s height had topped 646,132.[2]

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That’s because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker attempts to edit your transaction from Amazon so that you actually have to pay for your purchase twice. As soon as they edit the dollar amount of your transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on.

In order to change a single block, then, a hacker would need to change every single block after it on the blockchain. Recalculating all those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.

To address the issue of trust, blockchain networks have implemented tests for computers that want to join and add blocks to the chain. The tests, called "consensus models," require users to "prove" themselves before they can participate in a blockchain network. One of the most common examples employed by Bitcoin is called "proof of work."

In the proof of work system, computers must "prove" that they have done "work" by solving a complex computational math problem. If a computer solves one of these problems, they become eligible to add a block to the blockchain. But the process of adding blocks to the blockchain, what the cryptocurrency world calls "mining," is not easy. In fact, the odds of solving one of these problems on the Bitcoin network were about one in 17.56 trillion in August 2020.[2] To solve complex math problems at those odds, computers must run programs that cost them significant amounts of power and energy (read: money).

Proof of work does not make attacks by hackers impossible, but it does make them somewhat useless. If a hacker wanted to coordinate an attack on the blockchain, they would need to control more than 50% of all computing power on the blockchain so as to be able to overwhelm all other participants in the network. Given the tremendous size of the Bitcoin blockchain, a so-called 51% attack is almost certainly not worth the effort and more than likely impossible. (More about this below.)

Blockchain vs. Bitcoin

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. That concept can be difficult to wrap our heads around without seeing the technology in action, so let’s take a look at how the earliest application of blockchain technology actually works.

Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with.[3] But it wasn’t until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.[4]

The Bitcoin protocol is built on the blockchain. In an email announcing his research paper introducing the digital currency, Bitcoin’s pseudonymous creator Satoshi Nakamoto referred to it as “a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”[5]

Here’s how it works.

You have all these people, all over the world, who have bitcoin. There are likely many millions of people around the world who own at least a portion of a bitcoin. Let’s say one of those millions of people wants to spend their bitcoin on groceries. This is where the blockchain comes in.

When it comes to printed money, the use of printed currency is regulated and verified by a central authority, usually a bank or government—but Bitcoin is not controlled by anyone. Instead, transactions made in bitcoin are verified by a network of computers. This is what is meant by the Bitcoin network and blockchain being "decentralized."

When one person pays another for goods using bitcoin, computers on the Bitcoin network race to verify the transaction. In order to do so, users run a program on their computers and try to solve a complex mathematical problem, called a “hash.” When a computer solves the problem by “hashing” a block, its algorithmic work will have also verified the block’s transactions. As we described above, the completed transaction is publicly recorded and stored as a block on the blockchain, at which point it becomes unalterable. In the case of Bitcoin, and most other blockchains, computers that successfully verify blocks are rewarded for their labor with cryptocurrency. This is commonly referred to as "mining."

Although transactions are publicly recorded on the blockchain, user data is not—or, at least not in full. In order to conduct transactions on the Bitcoin network, participants must run a program called a “wallet.” Each wallet consists of two unique and distinct cryptographic keys: a public key and a private key. The public key is the location where transactions are deposited to and withdrawn from. This is also the key that appears on the blockchain ledger as the user's digital signature.

Even if a user receives a payment in bitcoins to their public key, they will not be able to withdraw them with the private counterpart. A user's public key is a shortened version of their private key, created through a complicated mathematical algorithm. However, due to the complexity of this equation, it is almost impossible to reverse the process and generate a private key from a public key. For this reason, blockchain technology is considered confidential.

Public and Private Key Basics

Here's the ELI5—"Explain it Like I'm 5"—version. You can think of a public key as a school locker and the private key as the locker combination. Teachers, students, and even your crush can insert letters and notes through the opening in your locker. However, the only person that can retrieve the contents of the mailbox is the one that has the unique key. It should be noted, however, that while school locker combinations are kept in the principal's office, there is no central database that keeps track of a blockchain network's private keys. If a user misplaces their private key, they will lose access to their bitcoin wallet, as was the case with this man who made national headlines in December of 2017.

A Single Public Chain

In the Bitcoin network, the blockchain is not only shared and maintained by a public network of users—but it is also agreed upon. When users join the network, their connected computer receives a copy of the blockchain that is updated whenever a new block of transactions is added. But what if, through human error or the efforts of a hacker, one user's copy of the blockchain manipulated to be different from every other copy of the blockchain?

The blockchain protocol discourages the existence of multiple blockchains through a process called "consensus." In the presence of multiple, differing copies of the blockchain, the consensus protocol will adopt the longest chain available. More users on a blockchain mean that blocks can be added to the end of the chain quicker. By that logic, the blockchain of record will always be the one that most users trust. The consensus protocol is one of blockchain technology's greatest strengths but also allows for one of its greatest weaknesses.

Theoretically, Hacker-Proof

Theoretically, it is possible for a hacker to take advantage of the majority rule in what is referred to as a 51% attack. Here's how it would happen. Let's say that there are five million computers on the Bitcoin network, a gross understatement for sure but an easy enough number to divide. In order to achieve a majority on the network, a hacker would need to control at least 2.5 million and one of those computers. In doing so, an attacker or group of attackers could interfere with the process of recording new transactions. They could send a transaction—and then reverse it, making it appear as though they still had the coin they just spent. This vulnerability, known as double-spending, is the digital equivalent of a perfect counterfeit and would enable users to spend their bitcoins twice.

Such an attack is extremely difficult to execute for a blockchain of Bitcoin's scale, as it would require an attacker to gain control of millions of computers. When Bitcoin was first founded in 2009 and its users numbered in the dozens, it would have been easier for an attacker to control a majority of computational power in the network. This defining characteristic of blockchain has been flagged as one weakness for fledgling cryptocurrencies.

User fear of 51% attacks can actually limit monopolies from forming on the blockchain. In "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money," New York Times journalist Nathaniel Popper writes of how a group of users, called "Bitfury," pooled thousands of high-powered computers together to gain a competitive edge on the blockchain. Their goal was to mine as many blocks as possible and earn bitcoin, which at the time were valued at approximately $700 each.

Harnessing Bitfury

By March 2014, however, Bitfury was positioned to exceed 50% of the blockchain network's total computational power. Instead of continuing to increase its hold over the network, the group elected to self-regulate itself and vowed never to go above 40%. Bitfury knew that if they chose to continue increasing their control over the network, bitcoin's value would fall as users sold off their coins in preparation for the possibility of a 51% attack. In other words, if users lose their faith in the blockchain network, the information on that network risks becoming completely worthless. Blockchain users, then, can only increase their computational power to a point before they begin to lose money.

Blockchain's Practical Application

Blocks on the blockchain store data about monetary transactions—we've got that out of the way. But it turns out that blockchain is actually a pretty reliable way of storing data about other types of transactions, as well. In fact, blockchain technology can be used to store data about property exchanges, stops in a supply chain, and even votes for a candidate.

Deloitte recently surveyed more than 1,400 companies across 14 regions about integrating blockchain into their operations. The survey found that 82% of respondents planned to hire staff with blockchain expertise in the next 12 months, and 39% already had a blockchain system in production today. In addition, 36% of companies said they would invest $5 million or more in blockchain in the coming year.[6] Here are some of the most popular applications of blockchain being explored today.

Bank Use

Perhaps no industry stands to benefit from integrating blockchain into its business operations more than banking. Financial institutions only operate during business hours, five days a week. That means if you try to deposit a check on Friday at 6 p.m., you likely will have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps.

By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes,[5] basically the time it takes to add a block to the blockchain, regardless of the time or day of the week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if banks are trading internationally), meaning that the money and shares are frozen for that time.

Given the size of the sums involved, even the few days that the money is in transit can carry significant costs and risks for banks. European bank Santander and its research partners put the potential savings at $15 billion to $20 billion a year.[7] Capgemini, a French consultancy, estimates that consumers could save up to $16 billion in banking and insurance fees each year through blockchain-based applications.[8]

Use in Cryptocurrency

Blockchain forms the bedrock for cryptocurrencies like Bitcoin. As we explored earlier, currencies like the U.S. dollar are regulated and verified by a central authority, usually a bank or government. Under the central authority system, a user's data and currency are technically at the whim of their bank or government. If a user's bank collapses or they live in a country with an unstable government, the value of their currency may be at risk. These are the worries out of which Bitcoin was borne.

By spreading its operations across a network of computers, blockchain allows Bitcoin and other cryptocurrencies to operate without the need for a central authority. This not only reduces risk but also eliminates many of the processing and transaction fees. It also gives those in countries with unstable currencies a more stable currency with more applications and a wider network of individuals and institutions they can do business with, both domestically and internationally (at least, this is the goal.)

Healthcare Uses

Health care providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy

Property Records Use

If you have ever spent time in your local Recorder's Office, you will know that the process of recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where is it manually entered into the county's central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index.

This process is not just costly and time-consuming—it is also riddled with human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanent.

Use in Smart Contracts

A smart contract is a computer code that can be built into the blockchain to facilitate, verify, or negotiate a contract agreement. Smart contracts operate under a set of conditions that users agree to. When those conditions are met, the terms of the agreement are automatically carried out.

Say, for example, I'm renting you my apartment using a smart contract. I agree to give you the door code to the apartment as soon as you pay me your security deposit. Both of us would send our portion of the deal to the smart contract, which would hold onto and automatically exchange my door code for your security deposit on the date of the rental. If I don't supply the door code by the rental date, the smart contract refunds your security deposit. This eliminates the fees that typically accompany using a notary or third-party mediator.

Supply Chain Use

Suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of their products, along with health and ethics labels like “Organic,” “Local,” and “Fair Trade.”

As reported by Forbes, the food industry is moving into the use of blockchain to increasingly track the path and safety of food throughout the farm-to-user journey.

Uses in Voting

Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia.[9] Each vote would be stored as a block on the blockchain, making them nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and provide officials with instant results.

Advantages and Disadvantages of Blockchain

For all its complexity, blockchain’s potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above.

Pros

- Improved accuracy by removing human involvement in verification
- Cost reductions by eliminating third-party verification
- Decentralization makes it harder to tamper with
- Transactions are secure, private and efficient
- Transparent technology

Cons

- Significant technology cost associated with mining bitcoin
- Low transactions per second
- History of use in illicit activities
- Susceptibility to being hacked

Here are the selling points of blockchain for businesses on the market today in more detail.

Accuracy of the Chain

Transactions on the blockchain network are approved by a network of thousands or millions of computers. This removes almost all human involvement in the verification process, resulting in less human error and a more accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain. In order for that error to spread to the rest of the blockchain, it would need to be made by at least 51% of the network's computers—a near impossibility.

Cost Reductions

Typically, consumers pay a bank to verify a transaction, a notary to sign a document, or a minister to perform a marriage. Blockchain eliminates the need for third-party verification and, with it, their associated costs. Business owners incur a small fee whenever they accept payments using credit cards, for example, because banks have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has virtually no transaction fees.

Decentralization

Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes more difficult to tamper with. If a copy of the blockchain fell into the hands of a hacker, only a single copy of the information, rather than the entire network, would be compromised.

Efficient Transactions

Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Whereas financial institutions operate during business hours, five days a week, blockchain is working 24 hours a day, seven days a week. Transactions can be completed in about ten minutes and can be considered secure after just a few hours. This is particularly useful for cross-border trades, which usually take much longer because of time-zone issues and the fact that all parties must confirm payment processing.

Private Transactions

Many blockchain networks operate as public databases, meaning that anyone with an internet connection can view a list of the network's transaction history. Although users can access details about transactions, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like bitcoin are anonymous, when in fact they are only confidential.

That is, when a user makes public transactions, their unique code called a public key, is recorded on the blockchain, rather than their personal information.

Although a person’s identity is still linked to their blockchain address, this prevents hackers from obtaining a user’s personal information, as can occur when a bank is hacked.

Secure Transactions

Once a transaction is recorded, its authenticity must be verified by the blockchain network. Thousands or even millions of computers on the blockchain rush to confirm that the details of the purchase are correct. After a computer has validated the transaction, it is added to the blockchain in the form of a block. Each block on the blockchain contains its own unique hash, along with the unique hash of the block before it. When the information on a block is edited in any way, that block’s hash code changes—however, the hash code on the block after it would not. This discrepancy makes it extremely difficult for information on the blockchain to be changed without notice.

Transparency

Even though personal information on the blockchain is kept private, the technology itself is almost always open source. That means that users on the blockchain network can modify the code as they see fit, so long as they have a majority of the network’s computational power backing them. Keeping data on the blockchain open source also makes tampering with data that much more difficult. With millions of computers on the blockchain network at any given time, for example, it is unlikely that anyone could make a change without being noticed.

Disadvantages of Blockchain

While there are significant upsides to the blockchain, there are also significant challenges to its adoption. The roadblocks to the application of blockchain technology today are not just technical. The real challenges are political and regulatory, for the most part, to say nothing of the thousands of hours (read: money) of custom software design and back-end programming required to integrate blockchain to current business networks. Here are some of the challenges standing in the way of widespread blockchain adoption.

Technology Cost

Although blockchain can save users money on transaction fees, the technology is far from free. The “proof of work” system that bitcoin uses to validate transactions, for example, consumes vast amounts of computational power. In the real world, the power from the millions of computers on the bitcoin network is close to what Denmark consumes annually. Assuming electricity costs of $0.03~$0.05 per kilowatt hour, mining costs exclusive of hardware expenses are about $5,000~$7,000 per coin.[10]

Despite the costs of mining bitcoin, users continue to drive up their electricity bills in order to validate transactions on the blockchain. That's because when miners add a block to the bitcoin blockchain, they are rewarded with enough bitcoin to make their time and energy worthwhile. When it comes to blockchains that do not use cryptocurrency, however, miners will need to be paid or otherwise incentivized to validate transactions.

Speed Inefficiency

Bitcoin is a perfect case study for the possible inefficiencies of blockchain. Bitcoin's "proof of work" system takes about ten minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS).[11] Although other cryptocurrencies such as Ethereum perform better than bitcoin, they are still limited by blockchain.[12] Legacy brand Visa, for context, can process 24,000 TPS.[13]

Illegal Activity

While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably Silk Road, an online "dark web" marketplace operating from February 2011 until October 2013 when it was shut down by the FBI.[14]

The website allowed users to browse the website without being tracked and make illegal purchases in bitcoins.[14] Current U.S. regulations require financial service providers to obtain information about their customers when they open an account, verify the identity of each customer, and confirm that customers do not appear on any list of known or suspected terrorist organizations.[15]

Central Bank Concerns

Several central banks, including the Federal Reserve,[16] the Bank of Canada[17] and the Bank of England,[18] have launched investigations into digital currencies. A June 2020 paper from the Federal Reserve Bank of Philadelphia said the creation of a central bank digital currency (CBDC) would put the Fed in direct competition with private banks. "Besides its potential role in eliminating physical cash, a CBDC will allow the central bank to engage in large-scale intermediation by competing with private financial institutions for deposits (and, likely, engaging in some for of lending of those deposits)," the paper said. "In other words, a CBDC amounts to giving consumers the possibility of holding a bank account with the central bank directly."[16]

Hack Susceptibility

Newer cryptocurrencies and blockchain networks are susceptible to 51% attacks. These attacks are extremely difficult to execute due to the computational power required to gain majority control of a blockchain network, but NYU computer science researcher Joseph Bonneau said that might change. In 2017, Bonneau presented a paper estimating that 51% attacks were likely to increase, as hackers can now simply rent computational power, rather than buying all of the equipment.[19] [20]

What's Next for Blockchain?

First proposed as a research project in 1991,[3] blockchain is comfortably settling into its late twenties. Like most millennials its age, blockchain has seen its fair share of public scrutiny over the last two decades, with businesses around the world speculating about what the technology is capable of and where it’s headed in the years to come.

With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself at age twenty-seven, in no small part because of bitcoin and cryptocurrency. As a buzzword on the tongue of every investor in the nation, blockchain stands to make business and government operations more accurate, efficient, and secure.

As we prepare to head into the third decade of blockchain, it’s no longer a question of "if" legacy companies will catch on to the technology—it's a question of "when."