Blockchain technology, sometimes referred to as **distributed ledger technology**, is one of the latest innovations in technology. It has applications in a whole host of fields including finance, law, economics, mathematics, philosophy, and computer science. This chapter covers the basics of this new and exciting technology.

The Blockchain

One of the pillars of modern technology is how data is stored. Due to the vast amounts of available data, it is important to store it in a way that will make it easily accessible later on. You might choose to store your personal budget in a spreadsheet with rows and columns, which makes it easy for you to navigate visually. Many companies with immense quantities of data store it in relational databases, which are similar to spreadsheets but are also easily navigable programmatically. A **blockchain** is just another way in which data can be stored.

Data stored in a blockchain is packaged into **blocks**, which are linked together to form a linear chain: the blockchain. The blockchain can be thought of as a book, where the book in its entirety represents the blockchain and each individual page represents an individual block. Blocks in the blockchain are numbered the same way as pages in a book are, starting from the first block, known as the **genesis block**, and continuing to the last. The page number, which here represents the position of the block in the blockchain is known as the **block height.** Pages in a book have uniform sizes and can thus contain a predetermined maximum number of words. Likewise, blocks in the blockchain have a uniform data storage capacity and can store a predetermined maximum amount of data.

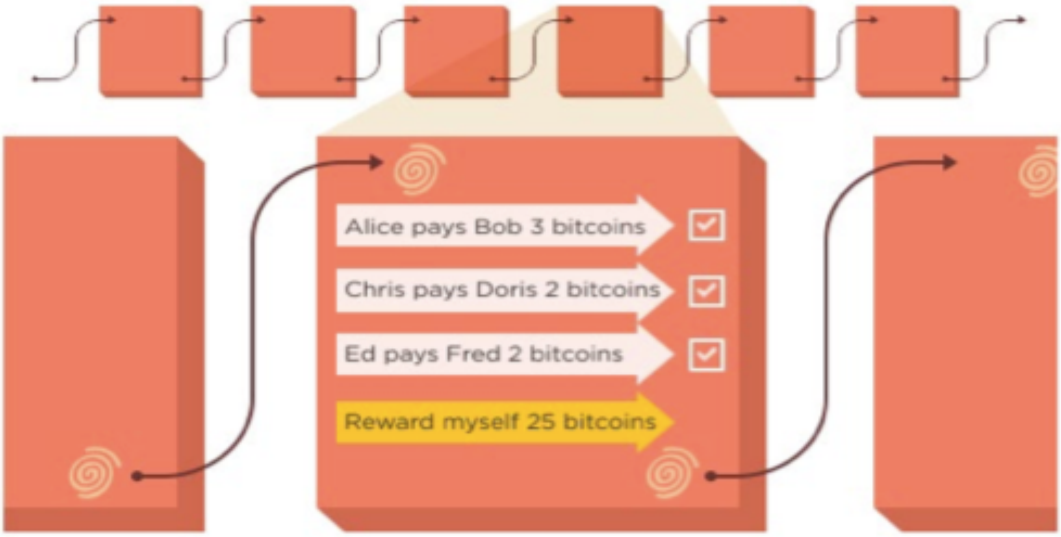
There are two things, broadly speaking, that readers of a book take for granted when flipping through its pages. Firstly, readers assume that every page that is supposed to be in the book is, indeed, in the book. If a student were to buy a history textbook in which the chapter, or even a couple pages, on World War II was missing, the student would be robbed of key information. In other words, we expect identical editions of books to contain identical information. This expectation applies to the blockchain as well. Each copy of a specific blockchain needs to contain all relevant blocks – and therefore all relevant data – in order to be **valid**. Otherwise, two parties sharing a blockchain to store data will have contradicting data sources. Secondly, we take it for granted that the order of the pages in a book is correct. A student attempting to understand the timeline of World War II, for instance, would be misguided if the pages on the conclusion of the war were, without logical reason, prior to the pages on the causes of the war. Since data often follows a logical order, it needs to be stored logically. This applies to the blocks in a blockchain too: a block that contains data on you spending Bitcoins cannot come before a block that contains data of you receiving Bitcoins – that would mean you're spending Bitcoins out of nowhere! Consequently, the order of blocks needs to remain intact for the blockchain to be **valid**.

What does it mean for a blockchain to be **valid**? The answer involves the very reason why the blockchain came about as a way of storing data. Storing data in a blockchain doesn't allow a company to store more data than it otherwise could store using a traditional database. Nor does storing data in a blockchain allow a company to navigate the data more efficiently than traditional databases do. So, why would someone store data in a blockchain? The advantage of storing data on the blockchain comes from its unique ability to allow multiple, independent parties to add data to a shared data storage. For this reason, the blockchain is sometimes referred to as a **distributed database**. For instance, ten private companies maintaining vaccination records could store them on a blockchain in order to share the data, ensuring that no client gets the same vaccination twice. A blockchain is **valid** when at least a majority of the companies involved agree that the blockchain is storing the data appropriately. You'll find out exactly what this means later in the chapter.

However, why can't these companies just share a central database stored on a server owned by one of the companies? They surely can, and this was the primary solution before the blockchain was invented. Yet, the central database solution has the major disadvantage of having a single point of failure. What if the company in charge of the servers shuts them down unexpectedly? What if the company doesn't properly back the database up and suddenly loses all the data? What if the company decides it wants to shut another company out of the system and unilaterally revokes their access? In other words, the central database solution requires all parties to trust a single, central authority. If the data is stored on the blockchain, on the other hand, there is no need for a single, central authority to maintain a server with the central database. Instead, each of the ten companies maintains a copy of the data and independently verifies the legitimacy of any new vaccination record that is added. This lack of a central entity that needs to be trusted for data to be collectively stored and retrieved is known as **decentralization**. Each individual or institution participating in a blockchain is known as a **node**.

What Does a Block Look Like?

Blocks are the fundamental pillars of the blockchain. They store all information and are linked together to form the blockchain. Each block in the blockchain is represented by a **digital fingerprint**, which is unique to the block and can be used to unambiguously identify the block in the blockchain. A digital fingerprint works very similarly to a human fingerprint. Humans can be unambiguously identified with their fingerprints, meaning that if someone leaves their fingerprints at a crime scene, investigators can use the fingerprints to match them against fingerprints previously collected in a database. However, the person cannot be identified from the fingerprints alone: a fingerprint database needs to contain a mapping between fingerprints and other forms of identification, such as people's names and photos of their faces. Digital fingerprints of blocks work in the same way: nothing about the data in a block can be deduced from the block's digital fingerprint, but a block can be unambiguously identified in the blockchain using its digital fingerprint. This is useful when, for instance, checking whether one copy of the blockchain is missing any blocks.


Alice pays Bob 3 bitcoins
Chris pays Doris 2 bitcoins
Ed pays Fred 2 bitcoins
Reward myself 25 bitcoins

https://bitsonblocks.net/2015/09/14/inside-bitcoins-blockchain/

Other than its own digital fingerprint and any included data, each block also contains the digital fingerprint of the block immediately before it. A blockchain is a linear data structure, which means that each block is **appended** to one block and has at most one block that is, in turn, appended to it. The blocks are chained together by storing references to the digital fingerprints of the block to which they are appended, which also makes it easy to maintain and validate the correct order of the blocks.

A digital fingerprint is simply a 64 character-long hexadecimal number. Below is an example of a digital fingerprint:

0f978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

The **hexadecimal numeral system**, unlike the decimal system humans conventionally use, contains digits with 16 values (0-f) rather than 10 values (0-9). The hexadecimal system is used because it allows for more numbers to be represented using fewer characters than the decimal system. This is good for data storage efficiency. For instance, the largest possible number that can be represented in the hexadecimal system using only 3 digits is *fff*. In the decimal system, this number would be 4095, which is significantly larger than 999, the largest possible 3-digit number in the decimal system.

The Science of Mining

Mining is perhaps the most elusive concept in blockchain technology. Let’s begin by understanding the need that mining fills. Recall the example of ten private companies using a blockchain to share a database of their clients’ vaccination records. There was no central authority, no single company in charge of maintaining the database and ensuring that all the data in it is correctly stored and accurate. Instead, each of the ten companies individually vetted all incoming data and maintained a local copy of the blockchain. How do the companies agree on what data to add and what to throw away if there is no central authority to stipulate this? The ten companies involved in the blockchain need to come to a **consensus**, or agreement, on what data to add. Mining is a process by which this consensus is reached between multiple nodes that was pioneered in Bitcoin, the first widely used application of blockchain technology. The process of mining in Bitcoin will be explained later in this chapter, but a core part of the mining process in all blockchains is the creation of blocks' digital fingerprints.

The creation of digital fingerprints involves cryptography, which relies heavily on mathematics. A digital fingerprint is created by running the block data through a **hash function.** A hash function takes any input data, usually text, applies a mathematical algorithm to the data, and outputs a value that uniquely represents the input data. Digital fingerprints for Bitcoin blocks are created by running the block data through the SHA256 algorithm, a hash function designed by the United States National Security Agency (NSA). SHA256 takes any arbitrarily sized data as input, manipulates that data, and outputs a 64 characters-long hexadecimal number, known as the **hash**. Regardless of the size of the inputted data, the output is always 64 characters long. Any change in the input data will produce a new, unique hash and the same hash cannot, in practice, be produced by two different inputs. This makes it very easy to detect if a block's data has been tampered with. Thus, the hash of a block's data, colloquially referred to as the block's **digital fingerprint**, is used as a block identifier. Below are a few examples of digital fingerprints generated from arbitrary input data:

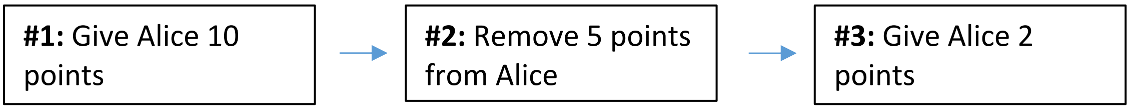
Input Data	**Digital Fingerprint: SHA256 Hash**	**Notes**
a	ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb	One character produces a 64 characters-long hash.
blockchain	ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1	An entire word produces an equally long hash.
blockchains	99cf6497afaa87b8ce79a4a5f4ca90a579773d6770650f0819179309ed846190	One small change in the word produces a completely new hash.
The favorite number of the fox was 44.	f70d31700c3c122331538f9b389a10217e0bd1cc0694b67a5c7b4f02c17b6198	Regardless of the input data's length, the hash is 64 characters-long.

You might have heard that mining is a **computationally intensive process**. However, generating a hash from any input data, such as the above, takes a fraction of a second and can be done without using too much of a computer's resources. Generating a hash, in other words, is *not* a computationally intensive process in and of itself. What makes mining computationally intensive is that a specific type of hash needs to be generated from the input data in order to create a valid digital fingerprint for a block. In the Bitcoin blockchain, for instance, this entails generating a hash from the block data whose numerical value is smaller than a given **target value**. More information about the mining process can be found in the Bitcoin section of this chapter.

The term "**miner**" is used to denote the parties involved in the mining process. However, the term "miner" does little to clarify the purpose of their job. The primary purpose of miners is to maintain the validity of a blockchain in lieu of a central authority. As stated above, miners undergo a computationally intensive process in order to find the digital fingerprints of new blocks. This process is a substitute for a central authority that stipulates which blocks are valid and contain data that should be appended to the blockchain. Exactly how this process achieves this goal differs from blockchain to blockchain, but the most popular method is found in the Bitcoin blockchain, which is detailed later in this chapter. Miners aren't individuals sitting at their desks iterating through hashes: a miner is a piece of software running on a (very powerful) computer that automatically iterates through millions, billions, even trillions of hashes per second. These computers are owned by independent individuals or companies who usually receive a reward for running their mining software. In Bitcoin, for instance, miners create and receive new Bitcoins every time they find a valid digital fingerprint for a new block. As a result, they are generating new coins and making money by performing their job as miners. However, not all blockchains let miners generate new coins when new blocks are found, and some blockchains have no rewards for miners at all. In such cases, miners are instead referred to as **validators**.

Immutability of the Blockchain

The blockchain is sometimes referred to as a **ledger** because of the way data modifications are recorded. Think of how you would change a value, such as the balance of a user, in a spreadsheet or traditional database. You would most probably overwrite the cell or data field and replace the old value with the new value. This method of modifying data is not possible on the blockchain. Instead of overwriting the data in a block, you would append a new block to the blockchain that modifies that data. As a result, just like a ledger, the blockchain keeps track of every data change ever made. This integral property of the blockchain is known as **immutability**. Note that this is different from saying that a blockchain cannot grow: on the contrary, blockchains are immutable precisely because the only way they permit changes to the data they hold is through the addition of new blocks, that is, through growth. The Bitcoin blockchain grows at an approximate rate of one block every 10 minutes, but once a block is validated and appended to the blockchain, it should, in theory, remain unchanged forever. Below is an example of the process:



#1: Give Alice 10 points

#2: Remove 5 points from Alice

#3: Give Alice 2 points

If we consider the above to be the current state of a blockchain that has a block height of 3, then Alice, currently, has 7 points. Note that instead of simply updating the first block with Alice's current point total, we added a new block each time her point total changed. Hence, the blockchain serves as a ledger containing a transaction history, or the history of data manipulation. Due to its immutable nature, the blockchain is sometimes referred to as an **immutable ledger.**

Both the data in the blocks as well as the order of the blocks, known as the **block order,** are immutable. In the example above, the order might seem irrelevant as addition is commutative, but blockchains are usually governed by complex rules that require immutable ordering. Consider, for instance, that a rule governing the blockchain above is that no user is allowed to have more than 10 points. If the order were somehow disrupted, and block #2 and block #3 swapped places, Alice would have 12 points in the now-second block, which would render that block erroneous. This erroneous block, known as an **invalid block**, would render the entire blockchain invalid. Consequently, both the block order and block data should, in theory, not be changed in a blockchain.

Decentralization

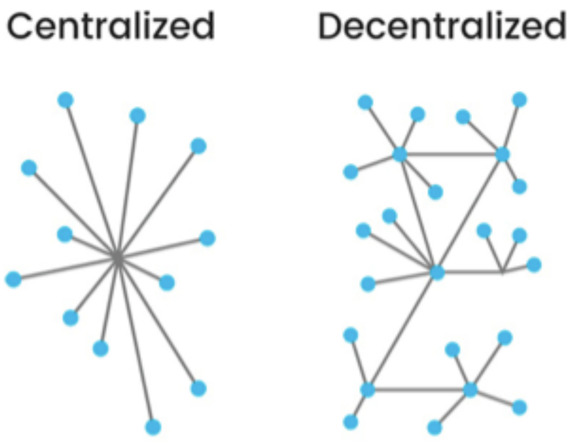
As mentioned earlier, the blockchain is an appealing way of storing data because it allows multiple, independent parties to share a database in the absence of a central authority. This means that there is no master copy of the data, no central authority that decides what data can or should be added, and no single point of failure. This type of network is known as a **decentralized network** because it lacks a central hub. This type of network is at odds with how most of society is structured. Take currencies, such as the US Dollar, for example: it is backed by a central government, controlled by a central bank, and transacted via banks who act as centralized intermediaries. When we use the US Dollar, we trust these centralized institutions to act with integrity and fulfill the duties they promise to fulfill. As soon as a central bank fails in its duties, the currency collapses. This happened, for instance, when Zimbabwe's monetary policy caused hyperinflation in 2008, and the Zimbabwean dollar lost all of its practical value. On the other hand, a currency that runs on the blockchain, like Bitcoin, has no central government or central bank controlling its functions. Instead, blockchain technology is used to distribute these roles, traditionally centralized, among miners who collectively maintain the network. In other words, blockchain technology allows for a **trustless network** to exist, whereby you don't have to trust anyone while still being certain of the integrity of the system.

While there are many benefits associated with decentralized networks that are built on top of blockchain technology, the implications of an absence of a central authority need to be kept in mind. If you accidentally send your Bitcoins to the wrong person or feel that you have been scammed, there is no central authority you can turn to in order to have your Bitcoins returned. Likewise, there is no bank that can vouch for the safety of your funds or aid you in major money transfers. A decentralized network removes the safety nets that central authorities provide in centralized networks and leaves individuals to fend for themselves. This is an important consideration to keep in mind when engaging in decentralized networks, especially those that involve high risk. Currently, the most popular decentralized network built on a blockchain is Bitcoin.

Bitcoin: The Genesis of Blockchain Technology

Bitcoin is a **cryptocurrency**, a form of digital money, that uses the blockchain to function as decentralized money. Bitcoin, along with most cryptocurrencies, is, therefore, an application of blockchain technology – currently the most popular application. Bitcoin is the oldest cryptocurrency and currently has a market cap of hundreds of billions of dollars. In fact, blockchain technology arose from the creation of Bitcoin: the inventor of Bitcoin, an anonymous individual or group of people publishing under the alias **Satoshi Nakamoto**, invented blockchain technology to serve as the transaction ledger for Bitcoin. Before this invention, digital currencies were either centrally controlled or could be very easily manipulated and destroyed. Only after Bitcoin's creation did people realize the potential of blockchain technology in other domains.

Bitcoin was invented in 2008 when Satoshi Nakamoto published a whitepaper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System." A year later, in 2009, Nakamoto published the first piece of Bitcoin code. The code was released as **opensource**, meaning that anyone could read it and suggest improvements to it, which resulted in a community-driven effort among programmers to constantly improve the Bitcoin code. Nakamoto's publications were made on an online forum for peer-to-peer technology enthusiasts. **Peer-to-peer technology** is a type of technology that is intended to run without the need for a centralized authority or server. Fiat currencies, such as the US Dollar, are not peer-to-peer networks, because banks act as central authorities and oversee all transactions, the storage, and the creation of money. As discussed earlier, Bitcoin is a peer-to-peer network without a central authority that dictates the validity of transactions or maintains the power to shut the system down. No individual or institution can manipulate or exert control over Bitcoin. As such, Bitcoin is a **decentralized network**.



https://www.eyerys.com/sites/default/files/blockchain.png

The key invention that Nakamoto made in Bitcoin was the **proof-of-work algorithm**, which lays the foundation for how Bitcoin as a network achieves consensus or, in other words, agrees upon which transactions are valid and which are not. This is sometimes referred to as the **mining process**. In fiat currencies, this is not a problem, because banks centrally stipulate validity: if you try to send someone money that you do not have or if you try to spend your money twice, your bank will prevent you from doing so. Therefore, when using a fiat currency, you trust banks as central authorities to make correct decisions about transaction validity. In Bitcoin, however, **trust is decentralized**, meaning you can trust no one in the network yet still be certain that no invalid transaction, such as someone stealing your Bitcoin, will take place. To attain this, Nakamoto invented proof-of-work as a mechanism through which **distributed consensus** is reached, whereby the Bitcoin network agrees on a set of rules that dictates transaction validity. These rules are rooted in mathematics, specifically in cryptography.

To understand Bitcoin's distributed consensus, it is important to understand some basic demographics of the Bitcoin network. The users of the Bitcoin network are loosely divided into two groups. The first, larger group are the regular users who send and receive Bitcoins; the second, smaller group are the **miners** whose job it is to validate transactions and group them into blocks, which are then appended to the Bitcoin blockchain. In theory, anyone can become a miner and thereby contribute to Bitcoin's distributed consensus.

Miners have tangible incentives to continue performing their job of mining new blocks. Each time a miner successfully mines a new block, he reaps the **block reward**. The block reward is a pre-determined amount of Bitcoins that are created in the new block and sent directly to the miner. This, special, type of transaction is known as the **coinbase transaction**. Currently, 12.5 Bitcoins are created in every new block and sent directly to the miner. The block reward halves every 210,000 blocks. On top of the block reward, the miner of the block receives all **transaction fees** that are contained within the block. Every Bitcoin transaction contains a transaction fee, which is designated and paid by the user sending Bitcoins. The higher a designated transaction fee, the quicker the transaction will be confirmed on the Bitcoin blockchain because of the greater incentive for miners to include it in their blocks.

Below is a walkthrough of the process of how Bitcoin as a currency can work without a central bank or government.

How Bitcoin Works

Step 1: A new transaction is created

Alice wants to send 5 Bitcoins to Bob for a new car she purchased. Normally, if Alice used a fiat currency such as the US Dollar, her bank would transfer the funds to Bob's bank. Alice's bank would remove the money from her account, and the money would appear in Bob's bank account. With Bitcoin, however, there are no banks, and so the process of transferring Bitcoins is very different. Let's walk through how it happens.

To begin, each Bitcoin user has a **private key** which needs to remain personal and secret. The private key is used to sign all transactions made by the user. This is an important part of

Bitcoin because, in the absence of banks, it serves as the mechanism through which a user exerts control over their money. Each user uses their private key to verify their ownership of their Bitcoins when sending them. In other words, this private key is used to unlock the user's Bitcoins. If the private key is lost or stolen, the user loses access to his or her Bitcoins.

The **private key** is a random 64 characters-long hexadecimal number (note that this is different from the digital fingerprint of a block). There is no central database that stores all existing private keys and you could, in theory, generate a new private key by rolling a 16-face die 64 times and recording the numbers you get on each roll. If you are concerned that someone might create the same private key as the one you are already using – don't worry! There are 2^{256} private keys available, which is more than the number of atoms in our universe. The probability of someone randomly generating a private key that is identical to yours is lower than that of you walking outside right now and dying because a piano fell on your head.

A **public key** is generated from the private key using elliptic curve cryptography, an advanced approach to cryptography. This public key is then hashed and encoded to create a unique **Bitcoin address** for each user. The Bitcoin address is meant to be public as it is the address to which you receive Bitcoins. In our example, Bob would have to give Alice his Bitcoin address.

Private Key	e9873d79c6d87dc0fb6a5778633389f4453213303da61f20bd67fc233aa33262
Bitcoin Address	1BoatSLRHtKNngkdXEeobR76b53LETtpyT

Alice verifies ownership of her 5 Bitcoins by using her private key to create a **cryptographic signature** of the Bitcoin transaction. This cryptographic signature serves as proof that Alice did indeed send 5 Bitcoins that were hers to Bob. Any miner can verify that Alice did indeed sign the transaction by using Alice's public key to verify the transaction data. Hence, Alice never needs to share her private key.

Once Alice signs the transaction, her **Bitcoin client** (the piece of software Alice uses to handle Bitcoin payments) broadcasts the Bitcoin transaction, containing information that it is meant for Bob, to the Bitcoin miners through a **gossip protocol**.

Step 2: Miners verify the transaction

Each miner verifies this transaction upon receiving it by, among other things, checking whether Alice indeed has 5 Bitcoins to spend. This is done by traversing across the Bitcoin blockchain and subtracting all the Bitcoins that Alice has spent from those that she has received. Recall that the blockchain is an immutable ledger of all transactions that have ever taken place. This means that if a miner starts with the first block and reads data from every single block until the latest block, he or she is able to calculate Alice's balance.

Step 3: The transaction is waiting to be mined

Once the miners validate the transaction, it is stored in each miner's **memory pool**, which is a local data storage that holds all valid transactions that are waiting to be packaged into blocks and added to the Bitcoin blockchain. Note that when a transaction is in the memory pool it is not in the Bitcoin blockchain, that is to say, it is not yet a confirmed Bitcoin transaction. The transactions sitting in the memory pool are waiting to be mined into blocks and appended to the blockchain.

Step 4: The transaction is packaged into a block, mined and appended to the blockchain

How are transactions taken from the memory pool, mined into blocks, and appended to the blockchain? At this stage, the Bitcoin proof-of-work algorithm comes into play.

Imagine a game where Player A thinks of a number between 1 and 10. Player B's task is to guess the number, but he can only guess one number per try. Assuming that Player A thinks of his number randomly, there is no deterministic methodology that Player B can employ to figure out the number. Simply, he has to guess. This type of guessing is known as **brute force** guessing. If Player C, then, joins the game but with two guesses per try, he is statistically expected to guess the number quicker than Player B. This is because brute force guessing can be made more efficient with an increased frequency of guesses.

Miners engage in a similar brute force guessing game when attempting to find the digital fingerprint of a block that is valid. To begin the process, the miner selects an arbitrary amount of transactions from the memory pool. The miner then appends some required data, such as the current **timestamp**, and runs everything through the SHA256 hashing algorithm. The resulting hash is the **block hash**, also referred to as the block's digital fingerprint. This process of selecting transactions and hashing them to create a block is known as **mining**. How does the miner know if he found a valid block hash? If the numerical value of the block hash is lower than the current **target** value, the block is deemed valid and can be appended to the Bitcoin blockchain. An intuitive way of comparing the hexadecimal values of SHA256 hashes to the target is by looking at the leading zeros: the more zeros at the start of the hash, the lower its value.

Example target value	000000000000000000365a170000000000000000000000000000000000000000
Invalid block hash	000f6497afaa87b8ce79a4a5f4ca90a579773d6770650f0819179309ed846190
Valid block hash	0000000000000000000000000000a4a5f4ca90a579773d6770650f0819179309

Statistically, more often than not, the miner will find a hash that is greater than the target and therefore generate an invalid block that cannot be appended to the Bitcoin blockchain. To generate a new block hash, the miner can either change the permutation of the transactions in the block, select a new set of transactions from the memory pool or – and this is the preferred option – add a random number to the data in the block, known as a **nonce**. Recall that the smallest change in input data will produce a new hash, so the miner can iterate through different nonce values to produce radically different hashes.

Miners iterate at a **hash rate** of trillions of hashes per second, often using specialized hardware, in a competition to be the one that finds the next valid block hash. The faster a miner can iterate through hashes, just like Player C had more guesses per try, the more likely he or she is to find a valid digital hash. This computationally intensive process is known as proof-of-work because once a miner finds a hash, it serves as proof of the work he put in to mine the next block.

Once a miner finds a valid block hash, the block is broadcasted to the Bitcoin network, and other miners verify and append it to their version of the Bitcoin blockchain.

Step 5: The other miners verify the block containing the transaction

Although mining a block is a computationally intensive process, verifying that a block is valid is a simple job. Once the other miners receive the mined block, all they have to do to validate it is to run it through the SHA256 algorithm once. If the block hash value is below the target, the miners accept the block as valid and append it to their local copy of the blockchain. The block has now been **confirmed**.

Once a block is appended to the blockchain, it is almost impossible to remove or change the block. The deeper a block is in the blockchain, measured by the number of blocks that come after it, the harder it is to remove or change that block. Recall that blocks contain links to previous blocks, thus, in order to re-mine a block (a technical way of describing the process of changing a block’s contents) that is 5 blocks deep, an attacker would not only have to re-mine that block, but also the 4 blocks that come after it, and any new block that has been added to the blockchain during this time. It is, in practice, impossible for a single miner to have the electrical output to produce a hash rate high enough to perform such an attack.

Therefore, the deeper a block is in the blockchain, the more immutable it is, and the more Alice and Bob can be certain that their transaction has been securely approved. The deeper a block is in the blockchain, the more **confirmations** it is said to have. Hence, a block that is 5 blocks deep is said to have 5 confirmations. A transaction is considered securely final after **6 confirmations**.

The entire process outlined above demonstrates the simple rules that are followed by thousands of independent miners to asynchronously achieve consensus about the state of the Bitcoin blockchain. The **state of the Bitcoin blockchain** is a technical way of saying the number of Bitcoins that each user holds. The process is asynchronous because there is never a point in time when an election or ruling takes place that stipulates a consensus on the state of the blockchain. Instead, the proof-of-work algorithm is intended to act as a lottery of which miner gets to produce the next block and consequently extend the blockchain. As such, no central authority, such as a bank, needs to be trusted in this decentralized network.

The Price of Bitcoin

The **price of Bitcoin** is dictated by supply and demand. At any given point in time, the value of Bitcoin is the value at which it was traded in the latest transaction. For example, if Alice sends half of a Bitcoin to Bob for $500, then the price of one Bitcoin at that given point in time is $1,000. Bitcoins can be bought on online **exchanges**, such as Coinbase or Bitstamp. Most exchanges determine the price of Bitcoin by aggregating the prices of the latest transactions.

Since there is no central bank that controls the value of Bitcoin through monetary policy, Bitcoin has thus far suffered from high **price volatility**. Many critics of Bitcoin argue that price instability prevents mainstream adoption of Bitcoin as a medium of exchange and renders Bitcoin a speculative instrument instead. Proponents of Bitcoin argue that price volatility will decrease as Bitcoin usage rises. If more merchants begin accepting Bitcoin payments, fewer users will seek to convert their Bitcoins back to fiat currency. This will lower speculation levels and begin stabilizing the price. Currently, however, Bitcoin and many other cryptocurrencies face high price instability.

Storing and Losing Bitcoins

Users store Bitcoins in pieces of software known as **wallets**. Despite the name, wallets do not actually store your Bitcoins; rather, they scan the Bitcoin blockchain to calculate how many Bitcoins you have access to with your private keys. The wallet software also takes care of generating private keys and creating corresponding public keys and addresses for Bitcoin users.

There are two ways in which your Bitcoins can be **stolen**. The first method involves the thief getting access to your private keys. Once the thief gains access to the private keys, he can use them to transfer all Bitcoins associated with the private keys to himself. The second method involves a hacker hacking into the servers of an exchange where Bitcoins are traded. Most exchanges store the private keys to the Bitcoins that are currently being traded in a database. If the hacker gains access to this database, he or she can transfer any Bitcoins associated with the private keys to himself or herself.

The Bitcoin network itself is vulnerable to attacks, primarily to attacks launched by malicious miners. The most prominent of such attacks is known as the **51% attack**. Recall that consensus in the Bitcoin network is distributed, whereby simple rules are followed by many independent miners to produce new blocks. If a miner decides to disobey the rules and begins mining otherwise invalid blocks, the Bitcoin network will simply disregard it, unless the dissenting miner comprises a **majority**. A majority, in this case, is measured in hash rate, meaning that if a miner, or a group of colluding miners, controls more than 51% of the power to produce new blocks, they can dictate what blocks get produced. In such a scenario, the malicious miners can undo transactions and spend their Bitcoins more than once. As a result, the decentralization of the Bitcoin network is undermined. Due to the vast amount of miners, it is very difficult to conduct a 51% attack on Bitcoin because of the sheer amount of energy, primarily electricity, required as input to conduct such an attack. An attacker would need the electrical output of all of Austria to conduct such an attack. To date, there has not been a known instance of a 51% attack on the Bitcoin network.

What has happened, however, is that a minority of miners have disagreed with some of the rules that govern Bitcoin and decided to change them. When a group of miners disagrees with the rules that are followed in the distributed consensus of the Bitcoin network, they may choose to no longer participate in that network as miners. This is known as a **fork** because the dissenting miners split away from the Bitcoin blockchain and begin working on their own blockchain, which entails the creation of a new cryptocurrency. The most popular Bitcoin fork happened on August 1, 2017, when the cryptocurrency Bitcoin Cash was created. The miners who split away from the Bitcoin network to create Bitcoin Cash disagreed, among other things, with the Bitcoin consensus rule that stipulates that valid blocks have a maximum size of 1MB. The miners wanted to increase the block size in order to increase the number of transactions that can be validated in one block. The block size of Bitcoin Cash blocks was increased to 8MB.

The Times Ahead

Many skillful developers constantly work on improving the Bitcoin code. Currently, most efforts are geared towards improving the speed and efficiency of Bitcoin transactions. A new technology known as the **lightning network** is being developed, which will allow very small transactions to be sent instantaneously across the network. There is also a lot of work being put into spreading awareness and adoption of Bitcoin. While Bitcoin's price volatility is rampant, it is lower than that of the Venezuelan bolivar, the national currency of Venezuela. This has resulted in individuals converting their savings into Bitcoin as it is easier to access than the US Dollar. Moreover, several merchants in Venezuela have begun accepting payments in Bitcoin. The more central institutions fail in maintaining national currencies, the more can we expect Bitcoin adoption to rise.

The World of Blockchains

Cryptocurrencies have thus far been the most popular blockchain application, which is mainly due to the fact that blockchains are a great way of keeping track of digital asset ownership. Since the creation of Bitcoin, countless new cryptocurrencies have spawned, some more legitimate than others. Each new cryptocurrency exists on its own blockchain with its own network of users and miners. While new cryptocurrencies bring varying degrees of new innovations to the table, most are, at least conceptually, based on Bitcoin. For instance, the cryptocurrency Monero was created to allow private transactions by obfuscating transaction data stored in the blockchain. Dash, another cryptocurrency, was created to reduce Bitcoin's transaction costs and increase transaction speeds. Each of these cryptocurrencies exists on separate blockchains and requires specialized software to be used. There are currently thousands of cryptocurrencies; however, not all cryptocurrencies actually provide what they promise. Most cryptocurrencies don't gain enough traction to survive or are outed as frauds.

Ethereum

The most notable post-Bitcoin cryptocurrency is Ether, which is built on the **Ethereum** blockchain. The reason why, unlike Bitcoin, the Ethereum blockchain is referred to as an ecosystem is because Ethereum provides more than just a cryptocurrency. In Ethereum, users can upload pieces of code that will run on the blockchain. This is useful because it allows any programmable job – not just monetary transactions – to be recorded, validated, and executed in a decentralized manner. The same way Bitcoin erased the central authority of financial institutions in currency, Ethereum can erase the central authority of any institution.

Let’s look at an example. Imagine the job of a contract lawyer in making and enforcing a legal agreement between two parties. Among the most pertinent tasks of the lawyer is to oversee the integrity of the contract, ensure the contract goes unchanged after signing and execute the contract agreement once the criteria are met. Sound like the lawyer is a central authority and a single point of failure? He is indeed. If the lawyer is corrupted or makes a mistake, the contract can be manipulated. In other words, both parties involved in signing the contract trust the lawyer to perform his job veraciously: it is a centralized network.

If the contract were instead written in code and uploaded onto the Ethereum blockchain, it would be enforced programmatically by each miner on the Ethereum network. This doesn’t mean that the miners would warp into the real world and force a party to abide by the contract. They do, however, provide a provable record of what, according to the contract, should be done. Hence, the same way Bitcoin intends to replace banks as financial intermediaries, so does Ethereum intend to replace contract-enforcing bodies as intermediaries in agreements. These programs that run on the Ethereum blockchain are known as **smart contracts**. When multiple smart contracts interact to form a more complex program, it is referred to as a **decentralized application** or **dApp.** Decentralized applications don’t have to be fancy: they can be a simple set of rules such as “breed a new kitty when 0.5 Ether is received.” This is actually an example of a rule in one of the most popular Ethereum dApps: a game called Cryptokitties.

Initial Coin Offerings

Initial Coin Offerings (ICOs) have been the cause of a lot of hype and controversy in the world of blockchains. Think of an ICO as something similar to an unregulated Initial Public Offering (IPO). Instead of selling shares, however, a company that wants to do an ICO will sell **tokens.** There are two types of tokens that can be sold in an ICO: **utility tokens** and **security tokens.** Utility tokens are the more popular type as they fall outside of most legal regulation. When you purchase a utility token, you aren’t buying a share in the company but a discounted coin that can be used to interact with the company’s dApp when it launches. On the Ethereum platform, for instance, Ether is used to pay miners to mine transactions in smart contracts, so Ether can be regarded as both a utility token and a cryptocurrency. Owning a security token, on the other hand, entitles you to certain ownership rights of the company. These tokens are less popular in ICOs as they are regulated by legislative bodies. ICOs are wholly unregulated, meaning a company can determine how many tokens it wants to sell, autonomously set the price of a token, and sell it to virtually anyone.

In mid-2014, a year before the Ethereum platform launched, 60 million Ether coins were sold to investors in a presale that would become the first of many ICOs launched on the Ethereum platform. However, ICOs can take place on any blockchain platform. In 2017 alone, companies raised a whopping $3.25 billion through ICOs. As an investor in ICOs, it is of crucial importance to do your due diligence before purchasing any tokens. Due to the lack of regulation, there is nothing stopping a company from disappearing and not meeting anything on its roadmap after it makes money from selling its tokens in an ICO. There have been many ICO scams in the past, and it remains a difficult job to safely navigate the ICO landscape.

Blockchain Beyond Cryptocurrencies

Another popular application of blockchain technology lies in **decentralized supply chains** and **decentralized property transfers**. Both of these applications make use of the blockchain's ability to provide individuals with ownership over digital assets or digital representations of physical assets. For instance, a smart contract can be used to handle real estate transactions with minimal involvement of a broker while the blockchain keeps track of who owns what property. Similarly, a supply chain can be made more efficient by representing a good on the blockchain and requiring each supplier to cryptographically sign when and where they processed the good. Thus, it is possible to efficiently track the movement of a good through a supply chain all the way to its source and identify any faulty suppliers. There also exist ambitions to fully decentralize certain supply chains, which would entail a retailer purchasing a good directly from the producer of that good. The energy sector is a particularly salient industry for this type of decentralization as, for instance, homeowners with solar panels on their roofs could sell excess energy to their neighbors. Some of these blockchains, if operated by private companies who exert control over who gets to be a node or a miner, are known as **private blockchains** because participation in the distributed consensus is limited to a private party. While private blockchains have a limited ability to achieve full decentralization, they can nonetheless be used to distribute authority and trust among multiple actors.

The Future of Blockchain

Blockchain technology allows us to create decentralized and trustless networks that connect people and companies in novel ways. Blockchains can be used to create networks without central authorities and increase the security of supply chains while cutting administration costs. The direction of blockchain technology is perhaps most eloquently embodied in a message left by Satoshi Nakamoto in the first Bitcoin block:

The Times 03/Jan/2009 Chancellor on Brink of Second Bailout of Banks

The message, citing the headline of a The Times issue, is a sharp criticism of the blind trust we sometimes place in centralized institutions. When these institutions fail in their roles, it is often the average users who pay the price, just like citizens end up paying the bailout of a failing bank. Blockchain technology allows us to build fully functioning networks without the need for central authorities to act as single points of failure.