#### 

| * Chapter 9: An introduction to the technical side of Bitcoin   + 9.0 Introduction     - **Activity** - watch “How Bitcoin Works Under the Hood”   + 9.1 Public and Private Keys: Security through Cryptography     - 9.1.1 Cryptography Public/Private Keys     - 9.1.2 Hashing Explanation     - **Activity** - Generate SHA 256 Hash   + 9.2 The UTXO Model   + 9.3 Bitcoin Nodes and Miners     - 9.3.1 What is a Bitcoin Node and how do I set one up?     - **Activity** - Watch video on Bitcoin Nodes     - 9.3.2 What is a Bitcoin Miner and how does mining work?   + 9.4 What is the Mempool     - **Activity** - Mempool   + 9.5 How Bitcoin transactions work from start to finish     - **Activity** - Bitcoin Transactions in Action |
| --- |

#### 

#### 

#### 

# Chapter 9: An introduction to the technical side of Bitcoin

"Bitcoin is not "unregulated". It is regulated by algorithm instead of being regulated

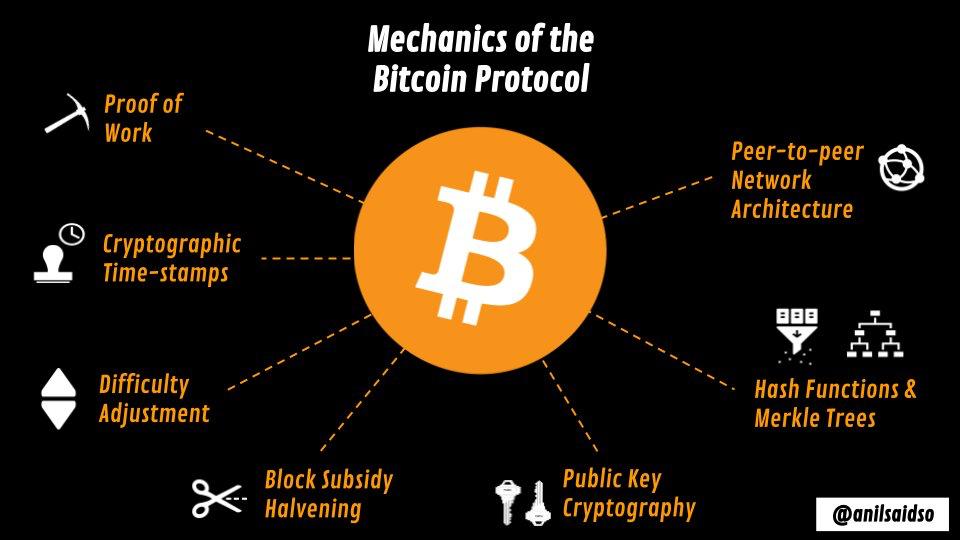
by government bureaucracies. Un-corrupted."

Andreas M. Antonopoulos

## 9.0 Introduction

In this chapter, we will take a closer look at the technology that enables The Bitcoin Network to operate in a fully decentralized way. We will explain in simple terms what happens when you send a Bitcoin transaction, how those transactions are processed, and what miners and nodes do in the Bitcoin Network.

* + - [Image from Chapter 9 Images Folder]



We are going to cover some challenging and technical concepts in this chapter. One thing that is important to remember, is that many people don’t understand how the internet works, yet they are able to use it every day to send emails, contact friends on social media, and even pay their bills. Learning the technical side of how Bitcoin works is a long journey that not everyone may want to take, even if they decide to use it as money. While we do encourage you to keep learning about the technical aspects of Bitcoin, we will keep this chapter focused on basic key concepts.

| [ORANGE NOTE BOX]  If you want a deeper technical understanding of how Bitcoin works, we have included resources in the back of this workbook. You can also register on our website for the Bitcoin Diploma - Technical Edition to be notified when that more technical course is ready. |
| --- |

Let’s jump in by watching a video that shows how the Bitcoin Network works.

**Activity** - Watch “How Bitcoin Works under the Hood” [[QR-CODE](https://www.youtube.com/watch?v=Lx9zgZCMqXE)]

As you saw in the video the Bitcoin Network is simply a ledger or record of transactions that is stored on multiple computers called nodes. The Bitcoin ledger is pseudonymous, meaning it doesn't have personal details, only transaction and address information. The ledger shows every bitcoin and its movements since the network started on January 3rd, 2009.

Next we’ll take a closer look at the technology that makes this system possible…

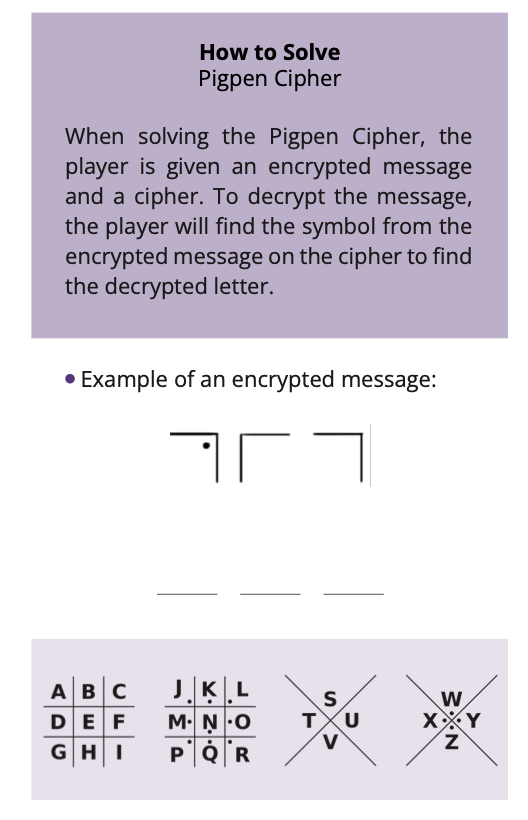
## 

## 9.1 Public and Private Keys: Security through Cryptography

“What Bitcoin gives us is a hard promise: the program will execute exactly as specified.”

Andreas Antonopoulos

**9.1.1 Cryptography Public/Private Keys**

Cryptography is a way of keeping information secret by disguising it in code.

[Images from BD 2023 page 86-88]

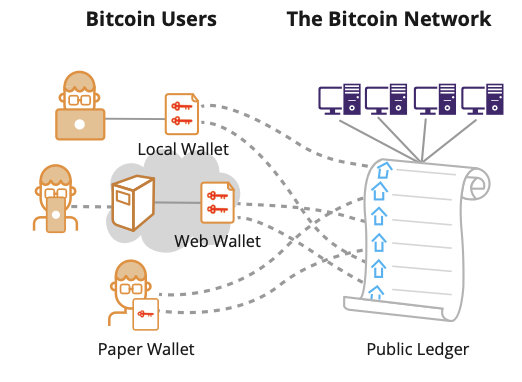
Encryption is the process of taking information and transforming it in a special code, making it unreadable to anyone that does not have the correct decryption method. This is similar to locking a safe, where only the person with the correct key or combination can open it.

Decryption, on the other hand, is the process of taking the encrypted information and making it readable again, like unlocking the safe and being able to read the information inside.

For instance, let’s say John wants to send Arel a secret message that isn’t meant for anyone else to read. They agree to use the Pigpen Cipher encryption method to disguise the message before sending it. Only those with the cipher can decrypt the message, making it unreadable to anyone else. Though this method is not considered secure today, it does illustrate the principle of private-key cryptography to send messages.

So, how does cryptography work in Bitcoin transactions?

In traditional private-key cryptography, John and Arel would have to first share a secret key, like a password or the Pigpen Cipher. John would then use this key to encrypt his message before sending it to Arel. Arel, who also knows the secret key, would then use the same key to decrypt the message and read it.

However, if someone else is in possession of the key and intercepts the message, he could encrypt it and read the message.

[Image from BD 2023 page 26-37]

Public key cryptography, the type that is being used in bitcoin transactions, has solved this problem. With public key cryptography John and Arel don’t need to share the password or encryption method with each other. Instead, they each have two different keys: a **public key** (which is safe to share with anyone) and a **private key** (which should be kept private).

In this case, when John wants to send a message to Arel, he can use Arel’s **public key** to encrypt his own message before sending it to Arel. When Arel receives the message, only he is able to decrypt it with his **private key**. Anybody else, even if they intercept the message, would not be able to read the message. Chances are also much lower to steal the key, because even John and Arel don’t need to share the key with each other.

So the main advantage of public key cryptography over private key cryptography is that it allows for secure communication without the need for the sender and receiver to first share a secret key (or another encryption method like Pigpen Cipher), which could be intercepted by a third party.

In Bitcoin, public key cryptography is not being used to send encrypted messages. Instead, it is being used to create unique **digital signatures** that make Bitcoin transactions immutable. A **digital signature** is a way to prove the authenticity of a Bitcoin transaction, in some way similar to when you write your signature on a physical document.

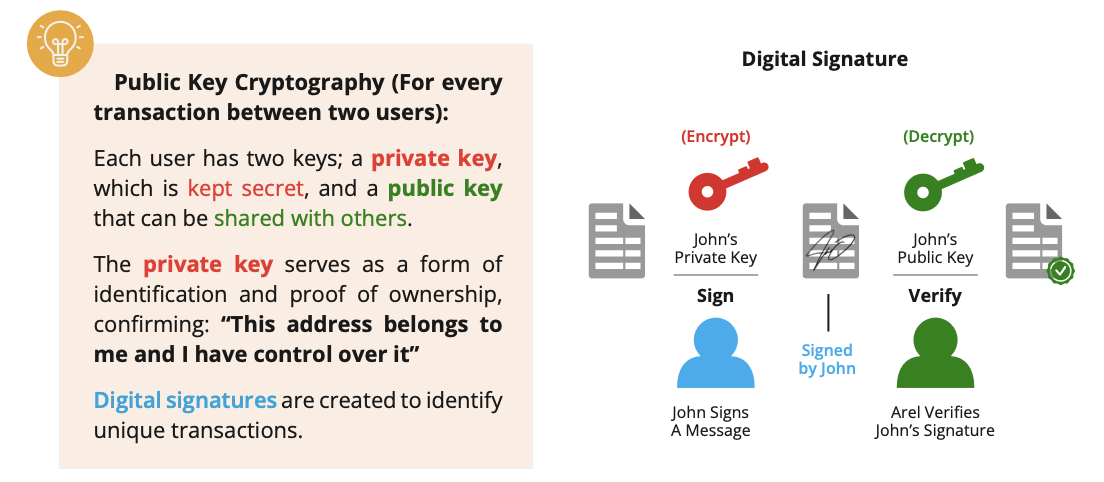
[Image from BD 2023 page 26-37]

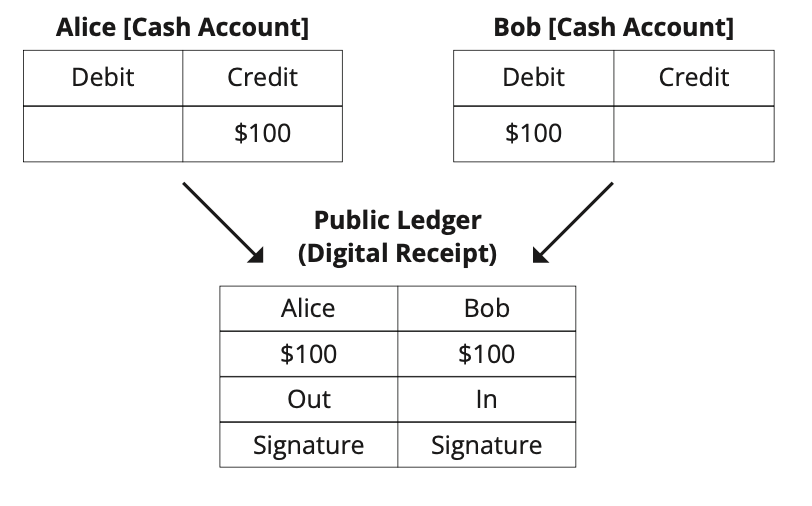
[TEXT BOX]

Public Key Cryptography (For transactions between two users):  
  
Each user has two keys, a private key, which is *kept secret*, and a public key which can be *shared with others.*

The private key serves as a form of identification and proof of ownership, confirming “this address belongs to me and I have control over it”.   
  
Digital signatures are created to identify unique transactions.

[END TEXT BOX]



[Image from BD 2023 page 26-37]

* Bitcoin transactions involve transferring a certain amount of bitcoin directly to another person’s account.
* Encryption is being used to make sure that only the real holder of the bitcoin has the control to send their money to someone else. It makes sure that the property is guarded from malicious actors.
* As an additional measure of protection, each transaction that you send in bitcoin automatically gets a **UNIQUE signature**. This **unique signature** is empowered by tamper proof technology that helps the network verify that the real owner of the bitcoin has sent the bitcoin, and not someone else.

[Image from BD 2023 page 26-37]

In simple terms how this works in a real Bitcoin transaction:

1. Creating the Transaction: A user initiates a bitcoin transaction by specifying details such as the recipient's address and the amount of bitcoin to be sent.
2. Digital Signature Generation: The sender generates a unique **digital signature** using their **private key**. This signature is a unique cryptographic code that verifies the authenticity of the transaction.
3. Broadcasting the Transaction: The signed transaction is broadcasted to the Bitcoin network, indicating the intent to transfer ownership of bitcoin from the sender to the recipient.
4. Verification on the Network: Nodes on the Bitcoin network receive the transaction and use the **public key** of the recipient to decrypt and verify the integrity of the transaction. Simultaneously, they use the sender's **public key** to verify the **digital signature**.
5. Confirmation on the Bitcoin network: If the verification is successful, the transaction will be added to the ledger, which serves as a secure, transparent record of all transactions. Once confirmed, the ownership of the bitcoin is officially transferred from the sender to the recipient.

In summary, the digital signature, created with the sender's private key, serves as cryptographic proof of authenticity and ownership, allowing Bitcoin’s decentralized network to validate and record the transaction on the ledger.

**9.1.2 Hashing Explanation**

Please don’t be intimidated by the technical terms and mathematical concepts ahead. We understand that not everyone is crazy about math, but you might surprise yourself and see that even the most complex ideas can be grasped with a little bit of effort.

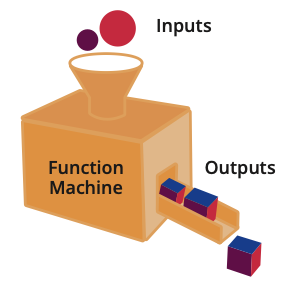
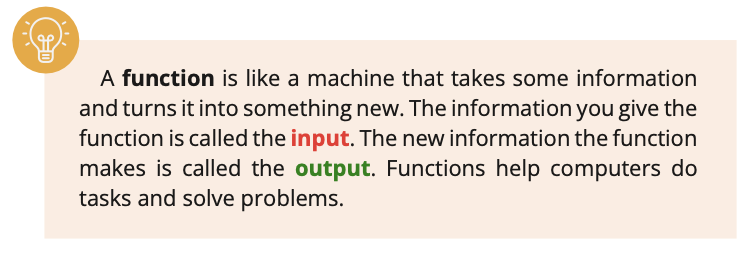
What is a function?

[Image from BD 2023 page 124-128]

[TEXT BOX]

A **function** is like a machine that takes some information and turns it into something new. The information you give the function is called the **input**. The new information the function creates is called an **output**. Functions help computers do tasks and solve problems.

[END TEXT BOX]



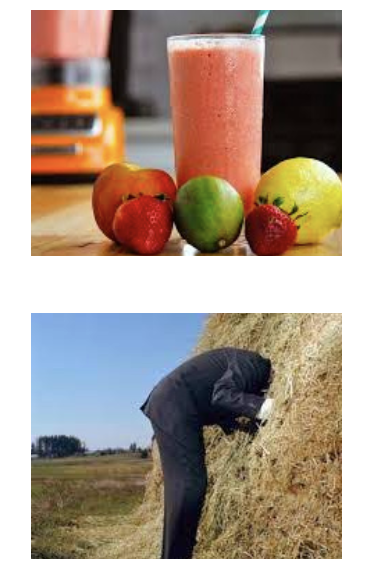
[Image from BD 2023 page 124-128]

Think of it like a recipe for making a salad. The recipe (or function) tells you what ingredients to use and how to mix them together to make the salad. You can put different ingredients in, but the recipe will always give you the salad as the output. Functions can be used to help make things easier and more efficient.

This recipe therefore is a function that takes the ingredients as the **input** and generates the tossed salad as the **output**.

In Bitcoin, functions are utilized to execute transactions. We already know that transactions in bitcoin are essentially transfers of value (money) from one address to another. To perform a transaction, a number of cryptographic functions are used to validate the transaction and update the state of Bitcoin’s ledger.

The functions used in a Bitcoin transaction include verifying the authenticity of the transaction inputs, checking that the sender has sufficient funds, and updating the balances of the relevant addresses. Once a transaction is verified and added to a block in the ledger, it becomes part of the permanent record of all transactions on the network.

[Image from BD 2023 page 124-128]

What is a one-way function?

A one-way function uses a set of instructions to process the information and turns it into something new, like a smoothie recipe turns ingredients into a new drink. But, just as you can’t un-blend a smoothie to get the original ingredients back, you can’t reverse the one-way function to get the original information back.

[Image from BD 2023 page 124-128]

Public-key cryptography, of which the **public key** is a part of, relies on the use of one-way functions, which make it difficult to determine the **private key** from the **public key**. In theory, it is not exactly “impossible” to find the private key from the **public key**, but it is extremely difficult to do so, and it would take an inordinate amount of time and computational power to accomplish this task.

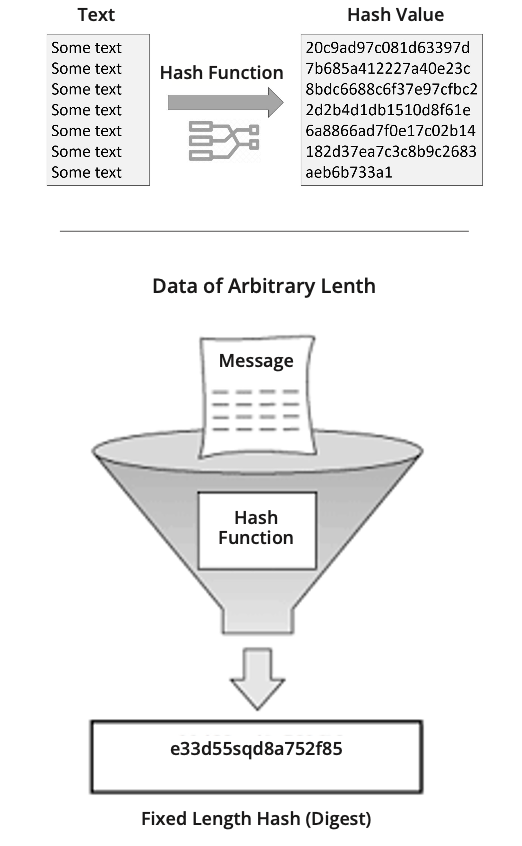
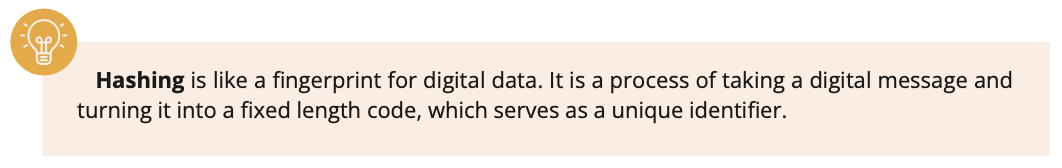
Finding a **private key** from a **public key** in Bitcoin is like trying to find a needle in a haystack as large as a football field. The needle represents the **private key** and the haystack represents all the possible **private keys**.

In the same way, one-way functions are designed to be irreversible and cannot be decrypted.

[Image from BD 2023 page 124-128]

What is a hash function?

[TEXT BOX]



Hashing is like a fingerprint for digital data. It is a process of taking a digital message and turning it into a fixed length code, which serves as a unique identifier.

[END TEXT BOX]

Just like a fingerprint can identify a person, a hash can identify a digital message. Hashes are used in many applications, including Bitcoin transactions.

How hashing is used in Bitcoin transactions

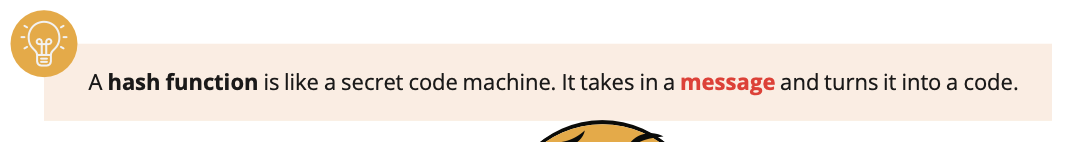
In Bitcoin, every transaction is hashed before it is added to a block in the ledger. The hash acts as a signature for the transaction, verifying that the transaction is valid and has not been tampered with. If someone tries to change even a single letter in the transaction, the hash will be completely different, alerting others to the change.

The role of hashing in providing security

Hashing is essential to the security of the Bitcoin Network. By using hashes to identify transactions, the network can detect any attempt to change or manipulate a transaction. This helps to prevent fraud and ensure that all transactions are recorded accurately on the ledger.

A hash function is a type of one-way function that takes an **input** (referred to as the “message” or “data”) and converts it into a numerical representation referred to as a “hash.” The **output** hash is unique to the **input** data, so even a small change in the input data results in a completely different hash.

[TEXT BOX]



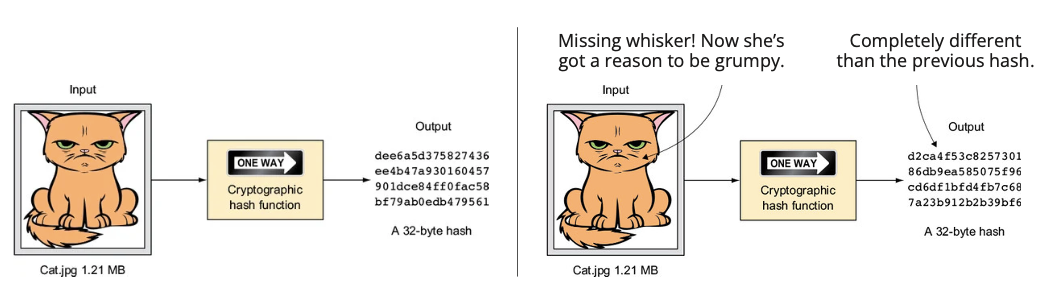
A **hash function** is like a secret code machine. It takes in a **message** and turns it into a code.

[END TEXT BOX]

[Image from BD 2023 page 124-128]

The code always looks the same for the same message. If you change the message even a little, the code will be completely different. This helps computers remember things and check if anything has been changed.

**Activity** - Generate SHA 256 Hash →



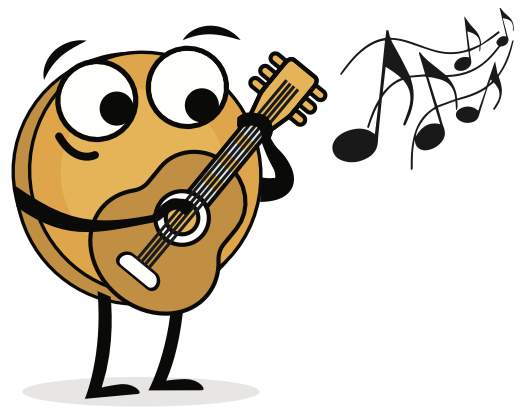
The **output**, or hash, is always the same length, no matter how long the original information was.

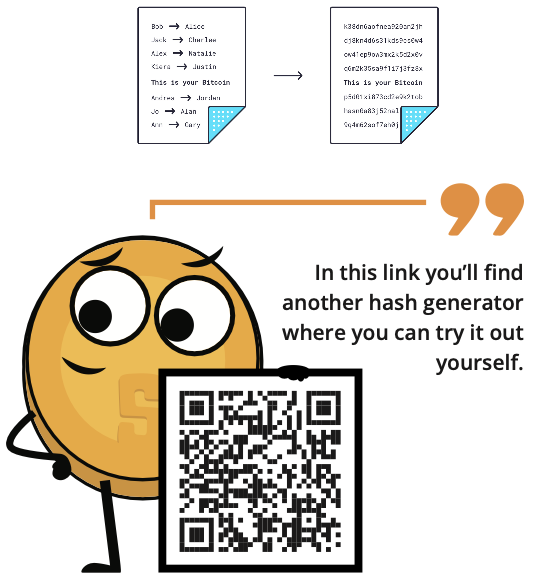
Bitcoin uses a few specific types of hash **function** called **SHA-256** and **RIPEMD160**.

A few examples below:

* Notice that a small change in the second input changes the output completely when compared to the first one.
* The third input is a huge file yet the output is still the same fixed length as the other two.



[Image from BD 2023 page 124-128]

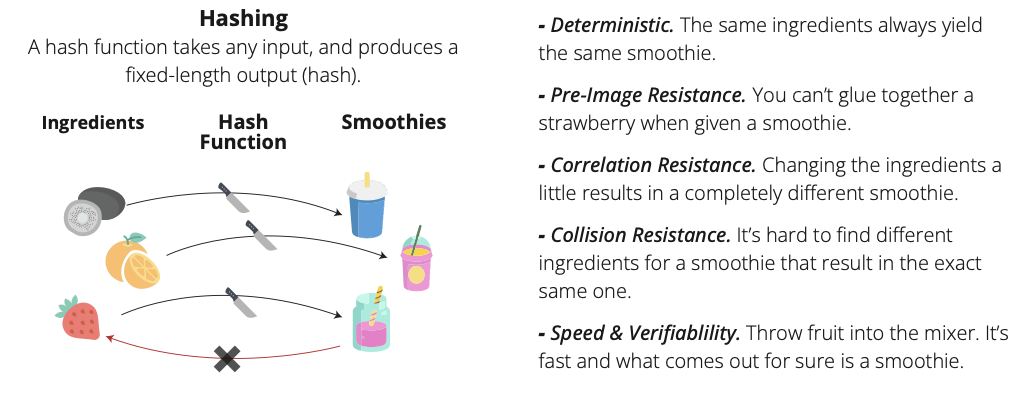
Hashing can also be thought of as a musical score that captures the essence of a piece of music. Just as a musical score is a unique representation of a tune, a hash value is a unique representation of a piece of data. By comparing the score of a piece of music with the actual performance, a musician can determine if the performance is accurate. Similarly, by comparing the hash value of received data with the original hash value, one can determine if the data has been altered during transmission.

Just as a slight deviation in a musical performance can cause it to sound different, even the slightest change to the original data will result in a different hash value. This makes hashing a powerful tool for ensuring the integrity and authenticity of a bitcoin transaction.

[Image from BD 2023 page 124-128]

The process of encoding the **public key** through hashing is used to improve the security of information by converting it into a fixed-length, unreadable format. Bitcoin uses the SHA-256 and Ripemd-160 algorithms to produce public addresses. The resulting output serves as a unique identifier for the **public key** and helps to ensure the integrity and security of transactions stored in the ledger. By encrypting the information in this way, it becomes more difficult for unauthorized individuals to access and manipulate the data.

[Image from BD 2023 page 124-128]



## 9.2 The UTXO Model

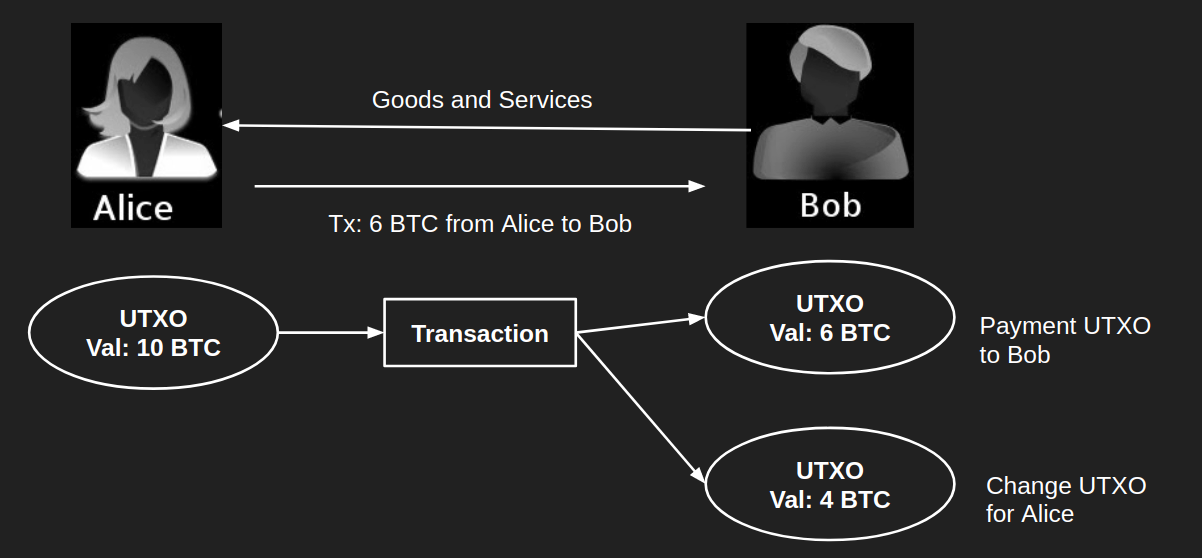
| ORANGE IDEA BOX  UTXO means Unspent Transaction Output |
| --- |

What are UTXOs?

In Bitcoin, transactions work like breaking a bigger piece of gold into smaller pieces and sending these smaller pieces both to others and to yourself.

You can think of UTXOs as different sizes and pieces of bitcoin, or differently denominated bills in your wallet. When you spend a UTXO, it is recreated into a new UTXO for the receiver, and whatever is left over is sent back to you in a different new UTXO known as “the change UTXO”. This is much like using a $10 bill to buy two cups of coffee for $6. The coffee shop keeps the $6 piece and returns you $4 in change.

[Image from Chapter 9 Images Folder]



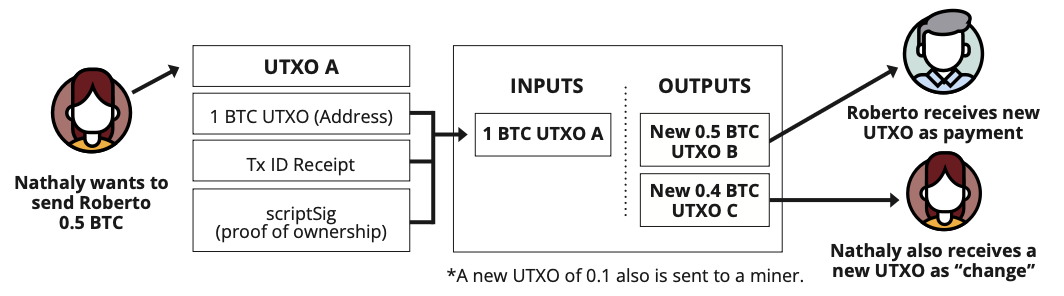
When sending bitcoin, you always send the entire amount of one (or more) of your UTXOs in your Bitcoin wallet. What happens? You send a piece to the recipient, and you receive the remaining amount back as change to one of your new Bitcoin addresses. The change you receive back is called an unspent transaction output, or UTXO, and can be used as an input for a new future transaction.

The balance of your Bitcoin wallet is the sum of all your different UTXOs. So, the sum of your UTXOs is the sum of the amount of bitcoin you own.

| ORANGE IDEA BOX  It is important to note that you should not make others aware of your UTXO’s, because when someone knows your UTXOs they can track your bitcoin transactions in the network, and ultimately will know how much money you own. |
| --- |

In conclusion, each time you make a transaction, you use one or more of your existing UTXOs to spend bitcoin, and new UTXOs are being created (for both you as the recipient).

[Image from BD 2023 page 122]

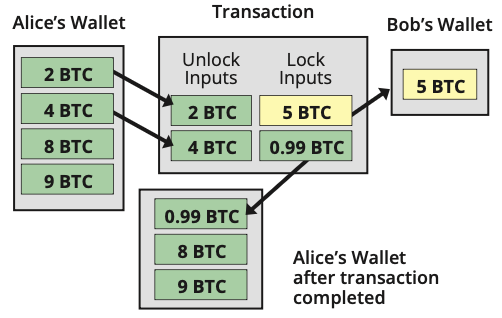


When a transaction is made, the amount of bitcoin that is sent is divided into multiple outputs, each of which is associated with a new Bitcoin address (a new UTXO).

When sending bitcoin to someone, you will use one or more UTXOs as the source of the funds (input). These UTXOs will be combined, if necessary, to create new outputs that belong to both the recipient of the transaction and yourself. These new outputs, or UTXOs, will then become the recipient’s property and your property. These UTXOs can then be used as the source of funds in other future transactions. This chain of UTXOs creates a transparent and traceable history of all bitcoin transactions on Bitcoin’s ledger, starting from the very first block (January 3rd, 2009).

An example to illustrate how this works: if you want to send 2 bitcoin but you only have a UTXO worth 5 bitcoin, the difference of 3 bitcoin is sent back to you as “change.” This change is a new UTXO for you, and you can spend that new UTXO in a future transaction.

[Image from BD 2023 page 122]

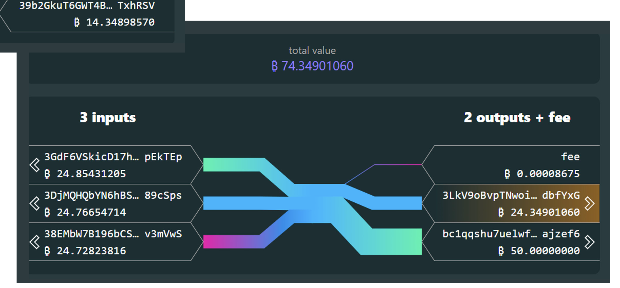
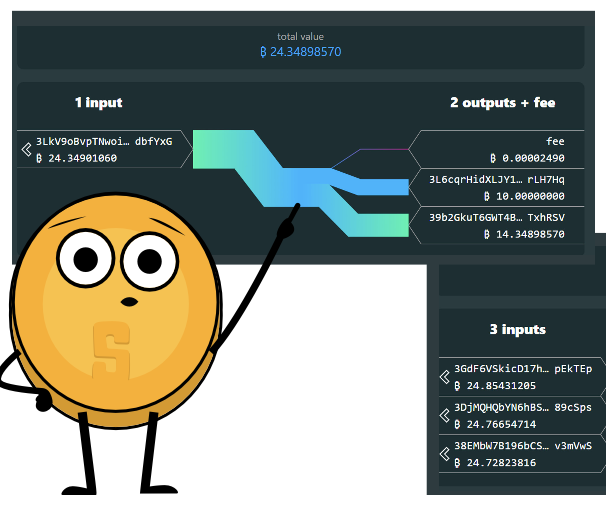
Another example:

1. Alice wants to send Bob 5 bitcoin.
2. She combines 6 bitcoin from two of her UTXOs.
3. From these UTXOs, she sends 5 bitcoin to Bob, gets 0.99 bitcoin as change back to herself, and needs to pay a 0.01 transaction fee.
4. After confirmation, the transaction is added to Bitcoin’s ledger, updating all the nodes that have a copy of the ledger.

Say Alice attempts to use one of her already spent outputs to make another transaction, it would automatically be rejected by the nodes. This is because the nodes maintain a copy of Bitcoin’s ledger (and all its transactions), so they can easily check the balance of Alice’s UTXOs, and verify that the transaction is not valid.

Below is an actual screenshot of a real transaction where there is only one input. However, the starting balance could, in another case, be the sum of multiple UTXOs (multiple inputs). What observations can you make when you look at the two transactions below? Do the inputs match the outputs? Can you describe the details of the transaction? Is there a connection between the two screenshots? And which transaction occurred first?

[Image from BD 2023 page 123]



## 9.3 A closer look at Bitcoin Nodes and Miners

In this section we’re going to take a more detailed look at two very important parts (and participants) of the Bitcoin Network which were first introduced in Chapter 6. We’ll look at:

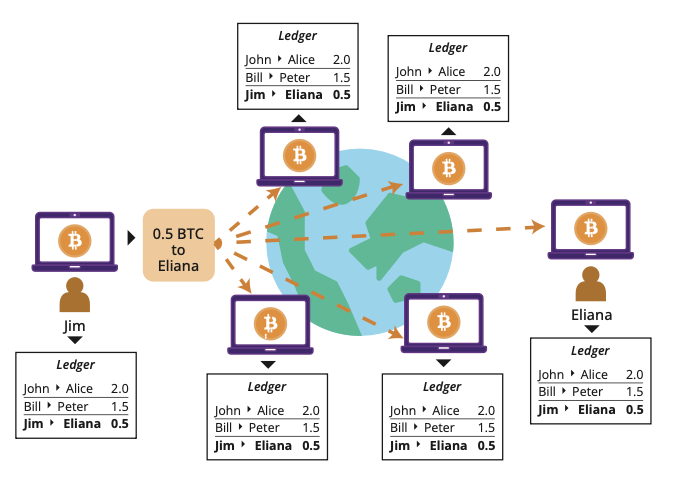
1. Bitcoin Nodes: Gatekeepers of Validation whose main job is to keep a copy of Bitcoin’s ledger, make sure that all transactions are valid, and that everyone follows the same rules.

By spreading out this job among many people worldwide, Bitcoin stays strong against potential problems. These Nodes help keep the system trustworthy and true to its decentralized idea, where no one person or group has too much power.

1. Bitcoin Miners: Architects of Security which use powerful computers and electricity to check and confirm transactions, making sure everything is secure. This work helps make the ledger, or blockchain, resistant to any bad actors trying to mess things up.

Together, Bitcoin Nodes and Miners work as a team to maintain a decentralized, secure, and strong system—a new way of handling money that people all around the world can rely on. Let's explore these roles in more detail to understand how they contribute to the innovative Bitcoin system.

**9.3.1 What is a Bitcoin Node and how do I set one up?**[Image from BD 2023 page 93]

A Bitcoin Node may sound technical but it is just a piece of software which runs a copy of the Bitcoin ledger. When you run your own Bitcoin Node, you gain a voice in shaping the rules of the Bitcoin network. 

Imagine this: if a group of people attempts to change how Bitcoin functions, say by altering the total supply of Bitcoin, you have a say. You can choose not to change your node to the new system, which is like voting to enforce the rules of the network that you support.

Let’s imagine a Bitcoin Node as a digital traffic cop with some essential tasks:

1. Gatekeepers of Validation: A Bitcoin Node keeps a digital copy of the blockchain, which is like a shared ledger of all bitcoin transactions. Many nodes around the world hold this same record.
2. Communication Hub: Nodes connect with each other, creating a vast communication network. They share information, especially transactions waiting to be added to the blockchain, stored in a digital waiting room called “the mempool."
3. Quality Checker: Every addition to the blockchain undergoes scrutiny. Nodes ensure that transactions are valid, rejecting any that don't meet the rules of the Bitcoin network.
4. Blockchain Informant: Other software, like wallets, can ask a node for information about the blockchain, such as bitcoin balances. Nodes serve as information hubs.
5. New Node Welcomer: When a new node wants to join, existing nodes generously provide a copy of the blockchain. The new node independently checks the validity of each transaction, emphasizing a trustless system.

**Activity** - Watch video on Bitcoin Nodes: <https://youtu.be/xc_TxlByxeY>

One of the options to run your own node is to download the Bitcoin Core software, and to give it some time to download the entire blockchain. Once ready, you can leave it on and approximately every 10 minutes, new blocks with transactions arrive. Your node checks their validity, adding them to your local copy of the blockchain.

| [RESOURCE QR CODE LINK] Resource: Bitcoin Core Software - <https://bitcoincore.org/en/download/> |
| --- |

Running a node provides sovereignty and independence. You don't rely on others; it's your own traffic cop. Unlike your Bitcoin wallet, which lacks a copy of the blockchain, a node ensures self-sufficiency. Instead of trusting others about your bitcoin holdings (and the state of the Bitcoin network), your wallet communicates with your personal node, making your digital experience more secure and trustworthy.

**9.3.2 What is a Bitcoin Miner and how does mining work?**

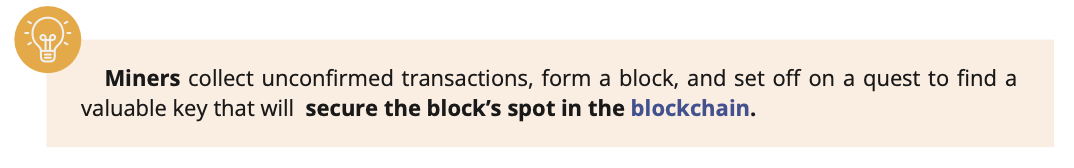
“The purpose of mining is not the creation of new bitcoin. That’s the incentive system.

Mining is the mechanism by which Bitcoin’s security is decentralized.”

Andreas M. Antonopoulos

Think of miners as digital bookkeepers. Just like companies pay accountants to maintain their financial records, miners get paid in bitcoin for verifying and adding transactions to the blockchain, ensuring the network is secure and running smoothly. This task requires serious computational power and specialized equipment.

[TEXT BOX]



**Miners** collect unconfirmed transactions, form a block, and expend energy to look for a valuable key that will **add and secure the block’s spot in the blockchain.**

[END TEXT BOX]

Miners are in a race to add the next block to the blockchain. The sought-after prize is a “valid block hash,” cleverly hidden among billions of others, and only a specific key assigned by the network can unlock it.

Picture a massive haystack filled with millions of keys, each representing a unique block hash. The network has chosen one specific key to unlock a valuable reward. Miners rummage through the haystack, testing each key in the lock, but only one lucky miner will discover the perfect match.

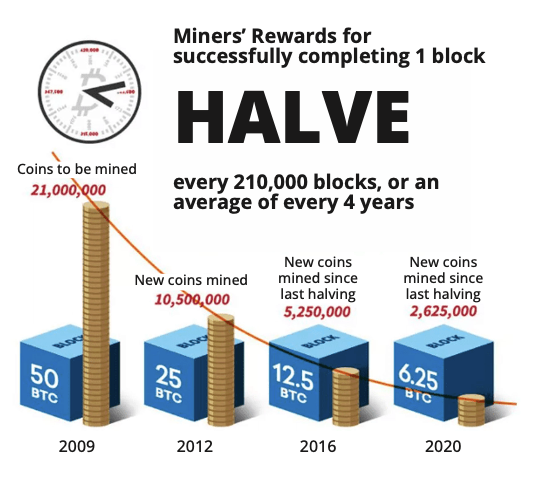
Once a miner finds the correct block hash, they share it with the network along with their created block of new transactions. Other miners verify the solution to make sure it’s the right fit. If everything checks out, the block is added to the blockchain, creating a secure and public ledger.

Miners earn rewards for their efforts in two ways:

1. Block rewards
2. Transaction fees

Block rewards are new bitcoin released into circulation with each block added to the blockchain. Transaction fees are small bitcoin payments users make to have their transactions processed faster and prioritized by the miner. Miners can pick which transactions to include in the block they mine, usually giving preference to those with higher transaction fees.

[Image from BD 2023 page 139]

Bitcoin halvings

A Bitcoin halving is an essential part of the Bitcoin universe that helps maintain its scarcity and value over time. As you know, there is a fixed supply of 21,000,000 bitcoins in total. This supply isn’t fully available from the day Bitcoin launched. Instead, this supply enters the Bitcoin universe in a step-by-step fashion.

Satoshi Nakamoto cleverly designed a block reward system to distribute new bitcoins without a central authority. In Bitcoin’s early days, miners got a sweet 50 bitcoin reward for each block they mined, motivating them to invest in powerful equipment and electricity for their mining operations.

To keep the network stable and manage new bitcoin supply, the block reward is halved about every 210,000 blocks. This event, called “the halving”, decreases the number of new bitcoin entering circulation and continues to motivate miners to protect the network and uphold its decentralization. Historically, halving events have led to significant price increases in the Bitcoin market due to the reduced supply of new bitcoins making their way into circulation.

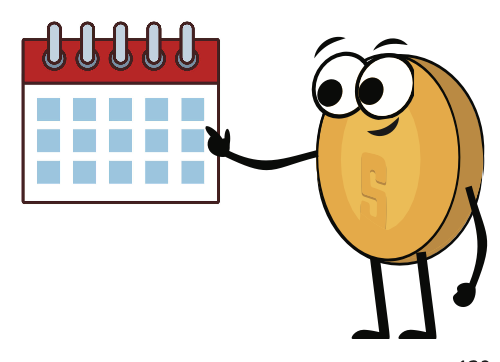
[TEXT BOX]



**Circulating Supply** refers to the total amount of a currency. With Bitcoin, the total circulating supply is the number of coins that have been mined and are in circulation at any given time, excluding any coins that are lost forever.

[END TEXT BOX]

[Image from BD 2023 page 139]

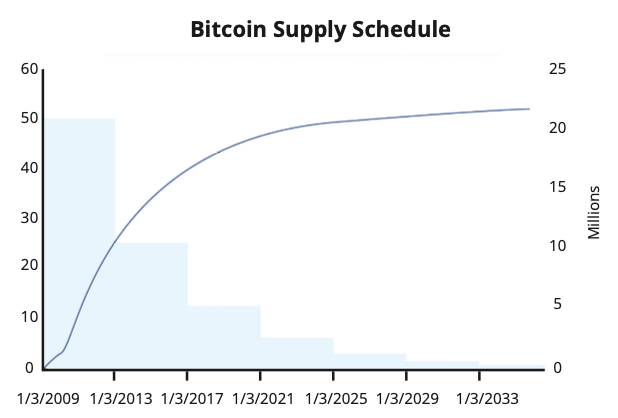
During each halving event, miners receive fewer bitcoin rewards, which lowers the issuance rate of new coins. As a result, Bitcoin’s mining difficulty increases to maintain a block time of approximately 10 minutes, ensuring new blocks are added to the blockchain at a steady pace. The reduction in mining rewards doesn’t necessarily mean miners make less profit, as they can also earn transaction fees for verifying transactions and adding them to the blockchain, which can offset the decrease in mining rewards.

Halving events are pre-programmed into the Bitcoin protocol, making the supply schedule of Bitcoin predictable and transparent.[Image from BD 2023 page 139-141]

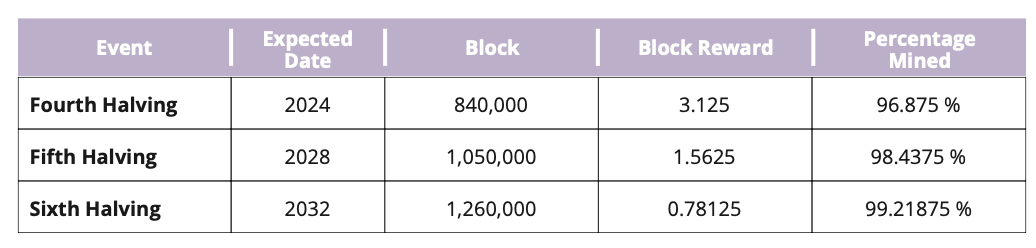
[TEXT BOX]

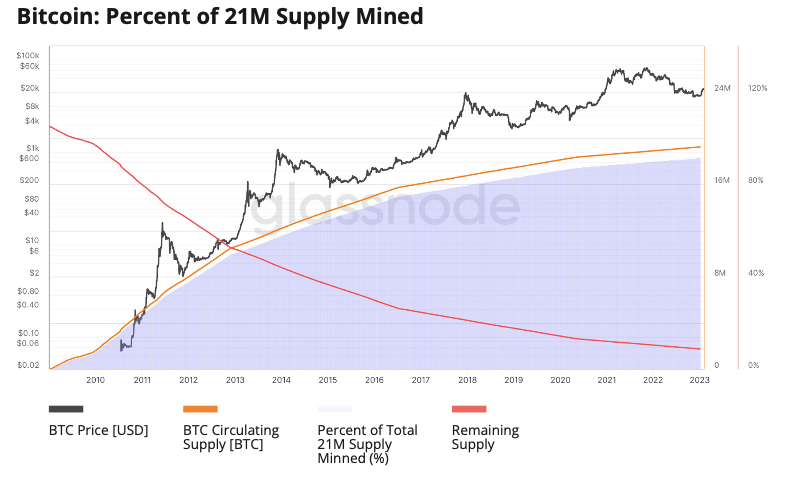
The **Bitcoin supply schedule** is the predetermined and public plan for the release of new bitcoin into circulation, designed to maintain Bitcoin’s scarcity over time.

[END TEXT BOX]



The following table outlines the details of upcoming halving events for Bitcoin, including the expected date of the next halving event, the block number at which the halving event will happen, the block rewards (per mined block) during that halving event, and the percentage of the total supply that will be mined.[Image from BD 2023 page 139-141]

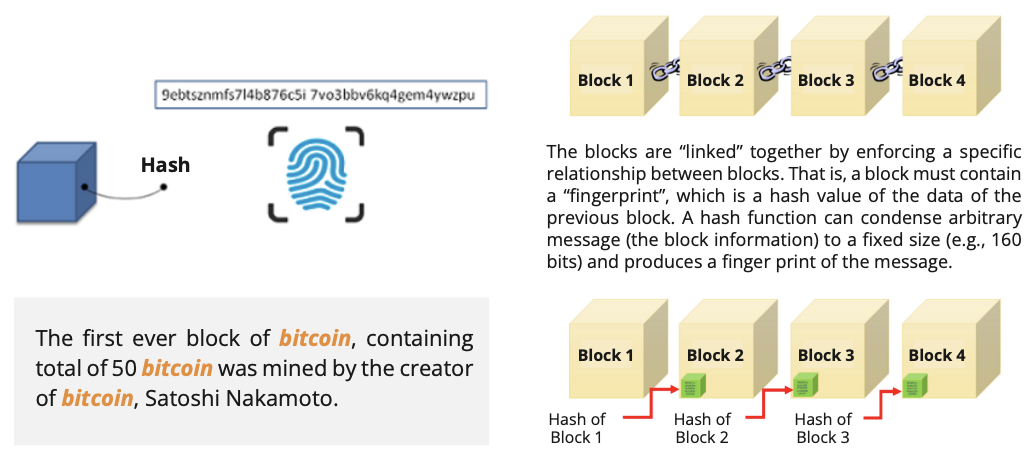


As more bitcoin is mined, the circulating supply and the percentage of the total supply that has been mined will keep increasing until the total supply of 21,000,000 is reached. The reduced supply, combined with rising demand, can boost Bitcoin’s price (measured in dollars). This benefits early adopters and also motivates miners to continue securing the network and contributing their computing power and resources.

What is a valid block hash in Bitcoin?

In Bitcoin, a valid block hash is like a special code that miners try to find. It's a unique number that helps keep track of each block in the blockchain, which stores information about transactions. The blocks connect in a chain from the first one (genesis block) to the latest, making a public record of all transactions. This block hash is crucial because it links each block to the one before it, making it easy for anyone to check the history of transactions. It's a bit like a fingerprint for each block, ensuring the information is correct and secure. The block hash acts as a way to confirm that the data in the block hasn't been changed.

[Image from BD 2023 page 139-141]



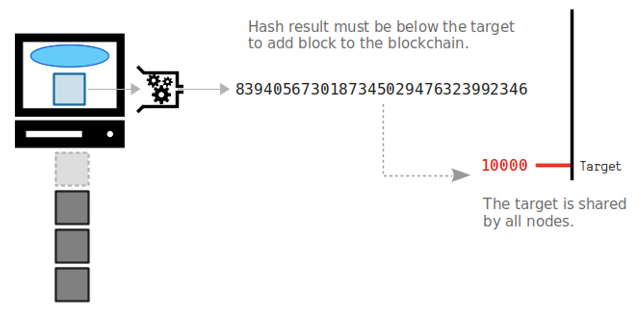
[TEXT BOX]

Satoshi Nakamoto, the creator of bitcoin, mined the initial block, which held a total of 50 bitcoins.

[END TEXT BOX]

The race to mine a block

Miners engage in a competition to uncover the block hash that aligns with the target (a special number) set by the network. The miner who’s the first to successfully discover the correct block hash is granted the opportunity to add that block to the blockchain and assign it with the corresponding hash ID. This solution serves as validation for the block’s authenticity.

[Image from BD 2023 page 142-144]

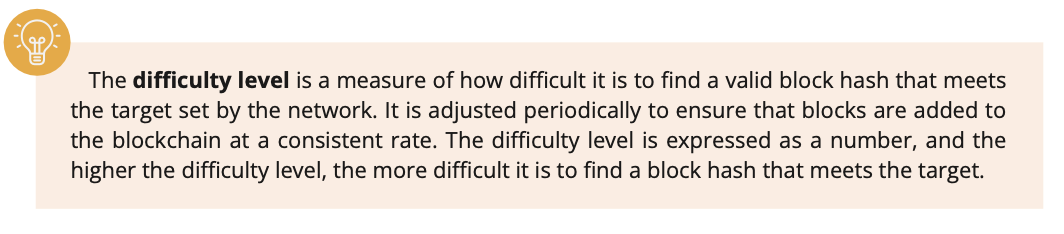
Mining can be compared to a race where the goal is to reach the finish line as quickly as possible. How difficult it is to find the block hash is adjusted periodically, ensuring that each block keeps being mined in approximately 10 minutes (as miners join and leave). This mechanism is called “the difficulty adjustment”.

Let’s say the target number set by the Bitcoin network is 1000. The miners would have to use their computational power and energy to search for a block hash (a specific number) that is lower than 1000. The first miner to find a block hash that is lower than 1000 gets to add the new block to the blockchain and is rewarded with bitcoin.

[TEXT BOX]

The difficulty level in Bitcoin mining is a measure of how difficult it is to find a valid block hash that meets the target set by the network. It is adjusted every 2016 blocks, or roughly every two weeks, to ensure that blocks are added to the blockchain at a consistent rate. The difficulty level is expressed as a number, and the higher the difficulty level, the more difficult it is to find a valid block hash.

[END TEXT BOX]



For example, consider two different hashes:

* Hash 1: 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK

Difficulty level: 1

* Hash 2: 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK

Difficulty level: 2

In this example, Hash 2 has a higher difficulty level than Hash 1, because it is a longer hash with more zeros at the beginning. It would be harder for miners to find Hash 2 because their computers would need to do more work.

[TEXT BOX]

By finding a valid block hash, a **miner demonstrates that they have done the work required** to add the new block to the blockchain and are paid a reward in bitcoin, plus transaction fees for their effort. **Proof of Work (PoW)** is the method the Bitcoin Network uses to validate transactions and add new blocks to the blockchain.

[END TEXT BOX]

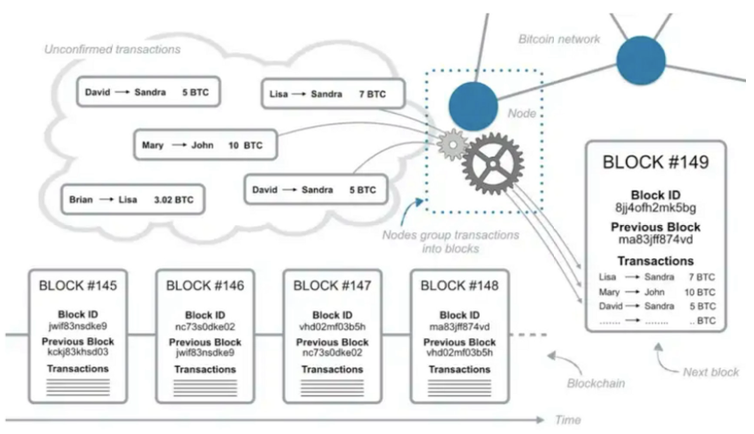


PoW keeps Bitcoin safe by making it difficult for anyone with malicious intentions to take control.

In summary, the tasks of miners consist of:

1. Bundling transactions into blocks: While nodes verify newly created transactions that are waiting in “the mempool”, miners select a subset of these to include in their candidate block.
2. Proof of Work: Miners race with each other to find the valid block hash.
3. Broadcast valid blocks: After finding the valid blockhash, they propagate the new block to the network.
4. Earn Rewards: Lastly, they receive newly created bitcoins and transaction fees for successfully adding the block to the blockchain.

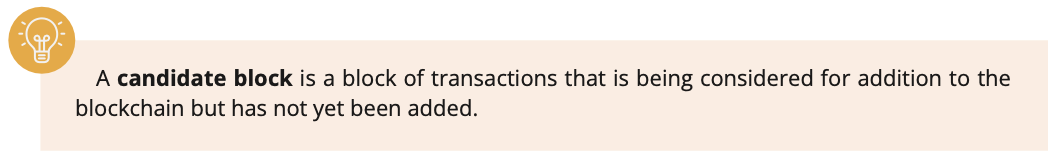
[Image from BD 2023 page 142-144]



Multiple miners can be working on creating new blocks simultaneously. The first miner to discover a block hash that meets the target set by the network announces it to the network, and the other miners then check the transactions in that miner’s candidate block to make sure they are valid. If the transactions are indeed valid, the block is added to the blockchain. The other blocks created by the other miners at the time are not added and are discarded. This process helps maintain consensus within the network and prevents double-spending.

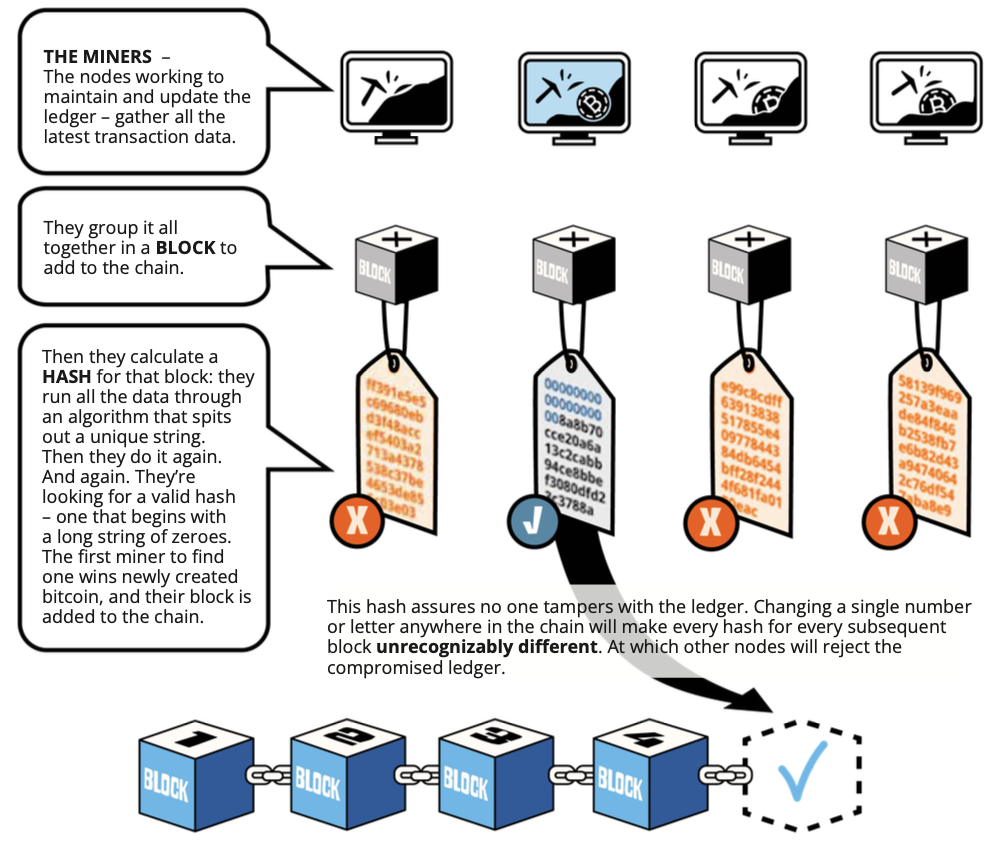
[TEXT BOX]

A **candidate block** is a set of transactions being considered for addition to the blockchain but has not been added yet.



[END TEXT BOX]

[Image from BD 2023 page 155]

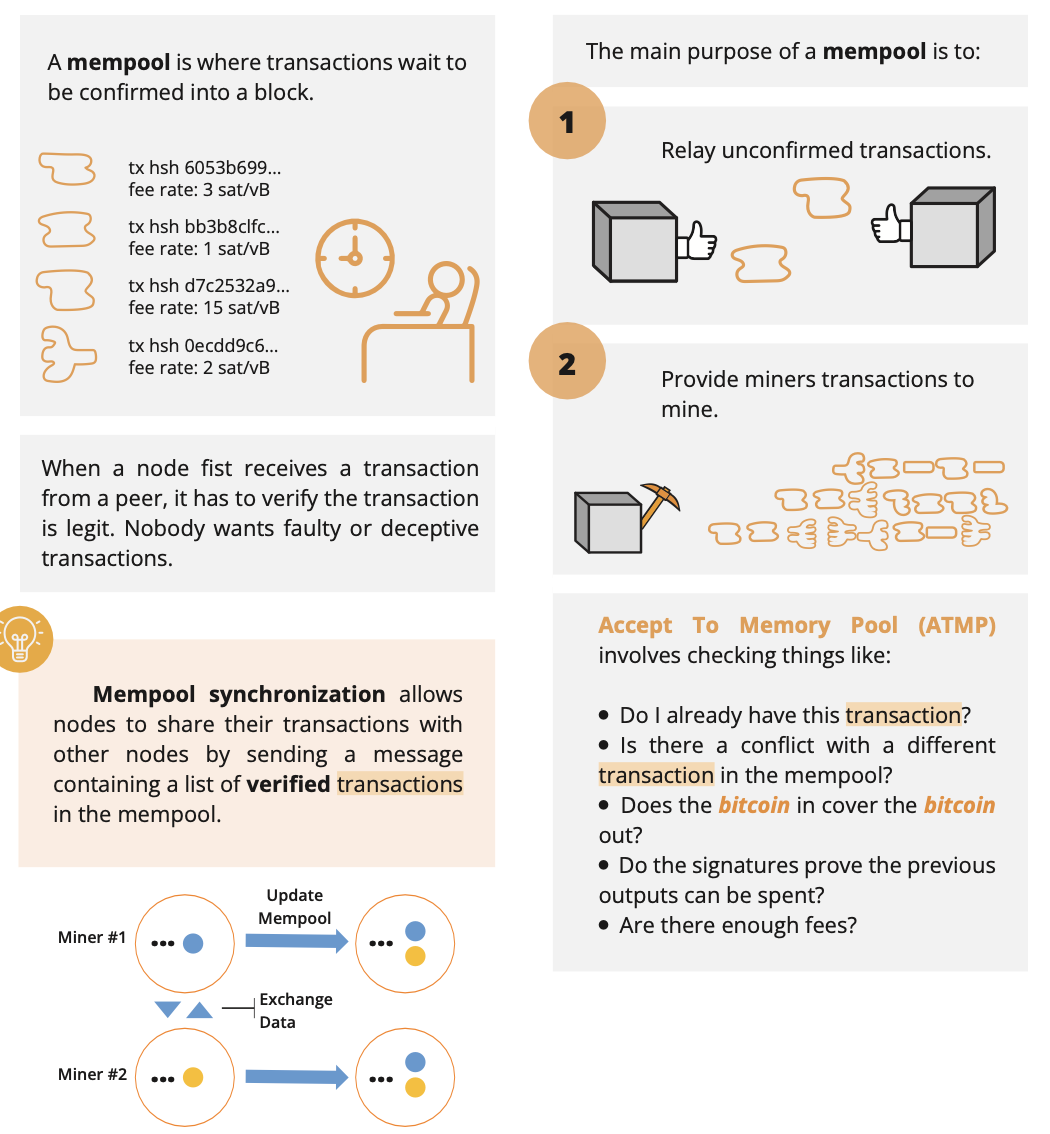


## 9.4 What is the Mempool?

The “Mempool” or Memory Pool is like a waiting room for transactions in the Bitcoin Network. When you make a transaction, it is first broadcasted to the Mempool before it is verified, selected, and added to the blockchain.

Imagine you are waiting in line at a restaurant. Your name is added to a list of people waiting for a table. When a table becomes available, the host calls your name and seats you. Similarly, a bitcoin transaction is added to the Mempool when it is made, and is confirmed and added to the blockchain when a miner includes it in a block.

[Image from BD 2023 page 128-130]

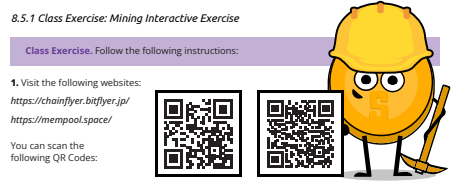


How are transactions verified and added to the Mempool?

When new transactions are broadcasted to the Bitcoin network, nodes verify these transactions to make sure they are valid and that the funds have not been spent before. Once these transactions are verified, the nodes will add them to their Mempool. Then the nodes will share the transactions with other nodes to double-check. Finally, if the majority of nodes agree, the transactions will be made available for miners to select and include them in a block. However, there are several reasons why a transaction might not be confirmed after 72 hours:

1. Low transaction fees: Transactions with a low fee may not be processed quickly enough, as miners are more likely to choose transactions with higher fees to include in their blocks.
2. Network congestion: If the network is congested, there may be a delay in confirming transactions, even if they have a high fee.
3. Double spend attempt: If a malicious actor attempts to double spend, their transaction may be rejected by the network.
4. Incorrect or incomplete data: If a transaction contains incorrect or incomplete data, it may be rejected by the network.
5. Malformed transaction: If a transaction is malformed, it may be rejected by the network.

To avoid having transactions rejected, it’s recommended to include a fee that is high enough to ensure the transaction is processed in a timely manner, and to double check that all the data in the transaction is correct before sending it.

[Image from BD 2023 page 152]

**Activity - Mempool**

1. Scan the following [QR code](https://mempool.space/):

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

*Note to designer: please keep the QR code that forwards to mempool.space and REMOVE the other one from the image → → →*

—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------

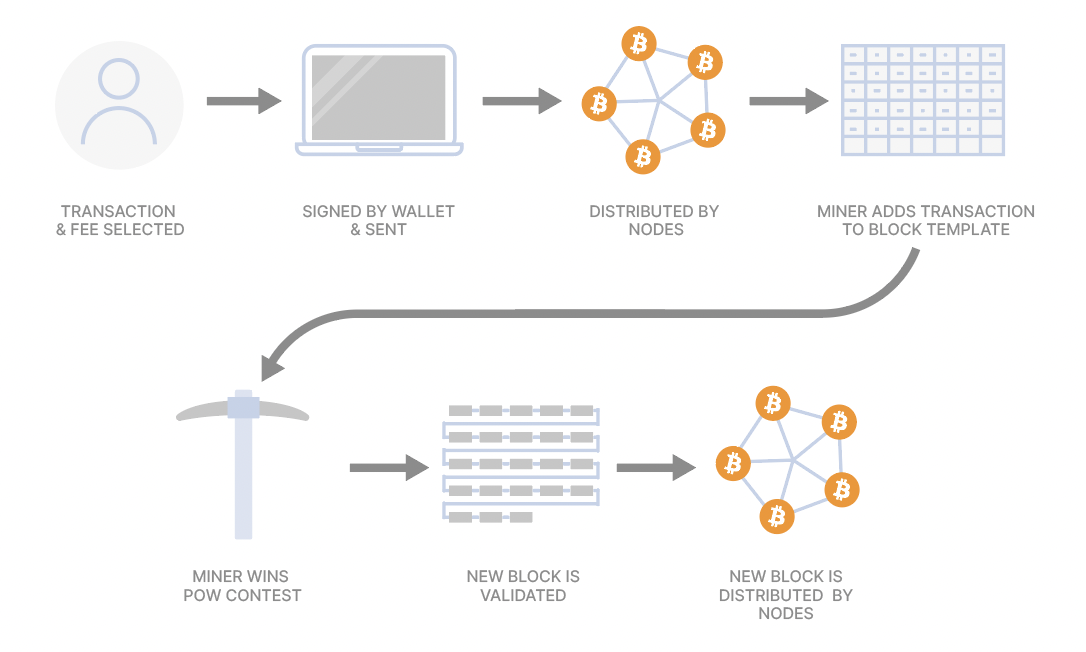
1. Review the various elements displayed on the page, including the latest blocks, confirmed transactions, the number of transactions, memory usage, and approximate value of the entire block. Answer the questions:

* What was the last mined block?
* How many transactions were included in that block?
* What is the total value traded in bitcoin?
* What was the size in megabytes of the block?
* How many zeros does the nonce of the block start with?
* How much bitcoin did the miner earn in total?
* What was the total value of fees received by the miner for adding the transactions to the network?
* Choose one of the highest-value transactions in the block. How many Bitcoin addresses did the amount get distributed to?

## 9.5 How Bitcoin transactions work from start to finish

1. Adam wants to send bitcoin to Gerardo. He picks one of his UTXOs, creates a transaction and adds all necessary details, including the amount of bitcoin he wants to send, Gerardo’s receiving address, and an above average amount of transaction fees.
2. After doing a final check if all details are correct, Adam uses his private key to sign the transaction.
3. Adam broadcasts the transaction to the Bitcoin network.

[Image from Chapter 9 Images Folder]



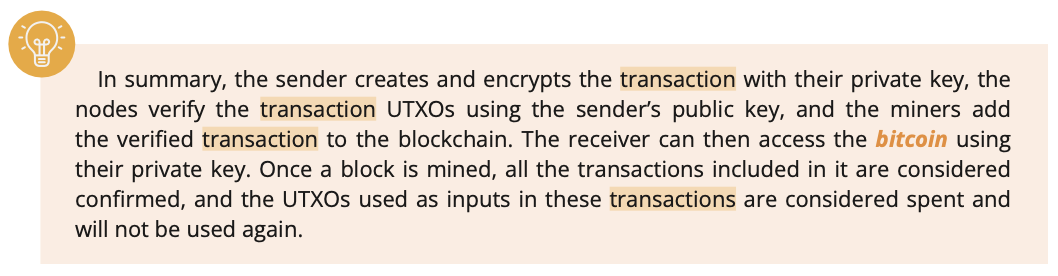
*From: Stevenot, Ted, “What is a bitcoin node and how does one work?”. Unchained Capital, 17, January, 2023, https://unchained.com/blog/what-is-a-bitcoin-node/*

1. The Nodes on the network receive the transaction and verify its validity according to the consensus rules (like checking if Adam’s signature is valid and if he has sufficient funds to make the transaction).
2. The transaction is marked valid, and the Nodes propagate it to other Nodes on the network, adding it to the Mempool.
3. Since Adam picked a high enough transaction fee, almost all Miners include his transaction in their blocks.
4. Proof of Work: Miners race and try to mine their block by finding the valid block hash. One of the Miners finds the hash and broadcasts their block to the network.
5. The Nodes receive the newly mined block and verify its validity. This includes validating all transactions within the block and ensuring that the Proof of Work requirement is met.
6. The majority of Nodes agree that the block is valid, and add it to the blockchain. Gerardo receives the confirmed bitcoin on his receiving address.
7. As additional blocks are added to the blockchain in the subsequent hour, the number of confirmations for the transaction grows. As the number of confirmations for the transaction increases, Gerardo gains greater confidence in its success and irreversible nature.

[TEXT BOX]

In summary, the sender signs the transaction with their private key, the nodes verify the transaction UTXOs, and the miners add the verified transaction to the blockchain. The receiver can then access the bitcoin using their private key. Once a block is mined, all the transactions included in it are considered confirmed, and the UTXOs used as inputs in these transactions are considered spent and will not be used again.

[END TEXT BOX]



As we wrap up this chapter, you've gained valuable insights into the fundamental concepts of how Bitcoin works. We've covered essential aspects, from the basics of money to the technical side of Bitcoin technology. Now, let's tie it all together in the next chapter. Chapter 10 awaits, where we'll delve into the significant question: "Why Bitcoin?"

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

* + ***Notes to designer:***
    - **Source images tagged “**[Image from Chapter 9 Images Folder]” from: <https://drive.google.com/drive/folders/1Dbg9PL0OpkJ78PDMFZ5HyKYu31sFDllU?usp=sharing>

—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------

#### 

#### 