Mi Primer Bitcoin
EL SALVADOR

Bitcoin Diploma

Bitcoin-Based Financial Education

Student Workbook

Third Edition | September 2022

Mi Primer Bitcoin has created this work and made it available free of charge under the **Creative Commons** license.

This work's license is:
Creative Commons
Attribution-Non Commercial-
No Derivatives
4.0 International (CC BY-NC-ND 4.0)

Bitcoin Diploma

Bitcoin-Based Financial Education

Student Workbook

Third Edition| September 2022

PARA DONAR:

Mi Primer Bitcoin
EL SALVADOR

bc1qc0h5ddd4ln4z05u55l87cp4umg8eg0jjkhcgvf

Acknowledgments

The Bitcoin Diploma has been a wild success and one that has grown faster than anyone expected. We'd like to give credit to all the wonderful people who got us here.

The core curriculum team, the driving force behind this content, is Dalia Platt, Gloriana Solano, Raul Guirola and Robert Malka. They have worked tirelessly behind the scenes for months, first to create this with a severe time crunch and then to continue to learn and improve. Without those four, none of this would have happened. Along the way that core group at various times has been aided by Giacomo Zucco, Pedro Solimano, María Andrée Maegli, Alejandro Machado, Gerson Martinez, and Vriti Saraf. Gerardo Apostolo and Enrique Jubis, designers with Activa, also did incredible work.

The Bitcoin Diploma story begins in February 2022 at a meeting at La Pacheco, a public school in San Marcos, El Salvador. We moved fast, raised funds from over 400 individual donors, started classes in April and graduated the first group in June.

The architects of that February meeting are also indispensable characters in this story. The director of La Pacheco, Asael Rodriguez, was dedicated to preparing his students for a changing world. The congressman Rodrigo Ayala, already a supporter of La Pacheco, also recognized the need for Bitcoin education. Carlos Toriello, community builder for Ibex Mercado, invited other Bitcoiners, myself included, to come and see the school and learn about the curriculum.

Carlos and IBEX deserve their own section here. They put up the funds for La Pacheco to build a new cafeteria, championed the cause, helped us crowd-fund the rest of expenses, and organized people from all over the world to participate and witness the first graduating class. The Bitcoin Diploma now exists in other places and with other sponsors, but that is built on the success of the pilot in La Pacheco and simply would not have happened without them.

Mi Primer Bitcoin is a non-profit with a singular mission—to provide quality, impartial Bitcoin education to everyone in El Salvador, then everyone in the world. As the first nation to adopt Bitcoin we believe El Salvador can be an example and that the foundation of success will be quality, impartial education. Our vison is to teach a nation and change the world. I know that sounds crazy, but I think we are on our way and the Bitcoin Diploma is a big part of that.

For a better world,

John Dennehy

Founder

Mi Primer Bitcoin

Table of Contents

Class #1 -

Introduction: The Monetary System ____ **9**

- 1.1 Activity: Introduction to Money ____ 10
- 2. What problems are there with today's money? ____ 10
  - • Consequences of Development ____ 10
    - - Needs vs. Resources ____ 11
  - • Modernization ____ 11
- 2. Definition of Money ____ 13
  - • Functions of Money ____ 13
  - • Characteristics of Money ____ 14
  - • Conventional Money and Monetary Assets ____ 15
    - - Types of Money ____ 15
    - –Activity: Are raisins good money? ____ 17

Class #2 -

The History, Evolution, and Devaluation of Money **19**

- 2.1 The History of Money ____ 20
- 2.2 Activity: Bartering Game ____ 20
- 2.3 The Evolution of Money Over Time ____ 22
  - • The International Monetary Standard in History ____ 22
- 2.4 The Sudden Change to Fiat ____ 23
- 2.5 Central Banks ____ 24
- 2.6 Class Activity: The Fractional Reserve ____ 25

Class #3 -

The Effects of Fiat Money and Centralization ____ **27**

- 3.1 Activity: Auction! ____ 28
- 3.2 Inflation ____ 29
  - • Why Does Inflation Matter to Us? ____ 29
  - • What Do Modern Economists Teach About Inflation? ____ 29
  - • The Causes of Inflation ____ 30
  - • Inflation Through Time ____ 32

3. Surveillance 33
4. Restrictions 33
5. Centralization vs. Decentralization 35
6. Conclusion 36

Class #4 -

Bitcoin 39

1. Why was Bitcoin created? 40
   - What problems need to be solved? 40
   - How were these problems solved? 40
   - Who solved these problems? 40
   - What difficulties did Satoshi face? 42
   - What is the Byzantine Generals' Problem? 43
   - What does this have to do with Bitcoin? 44
2. Introduction to Bitcoin 44
3. Differences between Bitcoin and Fiat 48
4. The Participants of Bitcoin 50

Class #5 -

The Purchase, Custody, and Movement of Bitcoin 53

1. On-Ramps and Off-Ramps 54
   - Do I have enough money to buy bitcoin? 54
2. Keeping Custody of Bitcoin 55
   - Wallet Types and the Lightning Network 55
   - How do I send or receive satoshis? 56
3. The Cycle of a Transaction (on-chain) 57
   - What is a Bitcoin transaction? 57
   - Bridges and stops to make transactions and save BTC 57
   - How does a transaction work, step-by-step? 58
   - UTXO - "Unspent Transactions" 60
   - Confirming a Transaction 61

Class #6-

Bitcoin as a Store of Value and Payments Network ____ **63**

1. The Double Spending Problem ____ 64
2. Memory Pool or the "Mempool" ____ 65

6.3 Transactions Verified, but Not Confirmed ____ 67

6.4 The Bitcoin Network (On-Chain) ____ 68

- Full Nodes ____ 68
- Activity: Seeing the Status of Transactions ____ 69

6.5 The "Lightning Network" (Off-Chain) ____ 70

- What is the difference between Layer 1 and Layer 2? ____ 70
- Activity: How Lightning Works ____ 73

Class #7 -

Miners and Bitcoin Mining ____ **77**

1. Mining Nodes ____ 78
   - How does the competition between miners work? ____ 78
2. A Little Detour – Understanding Hashes and Their Importance ____ 79
   - What is a function? ____ 79
   - What is a hash? ____ 80
   - What is SHA 256? ____ 80
     - Activity: Creating Hashes ____ 80
   - What is a "nonce"? ____ 81
   - What is a Merkle Tree? ____ 81

1. Mining ____ 82
   - Don't Trust, Verify ____ 84
   - The Block Hash ____ 85
   - The Nonce of a Block ____ 86
   - Activity: Analyze Blocks in Real Time ____ 86

Class #8 -

Scarcity, Cost, Price, and Volatility **89**

1. The Importance of the Block Reward 90

2. Halving 90

• Halving Reduction Events 90

8.3 The Value of Bitcoin Through Time 91

• Medium- and Long-term Factors 93

8.4 Miner Rewards 96

• The Difficulty 96

8.5 What or who do I have to take care of? 97

• Attacks on Bitcoin 97

• What is a 51% Attack? 98

Class #9 -

Bitcoin – Today and the Future **101**

1. Energy Consumption 102

2. Innovation 102

• Software - Bitcoin Core 102

• SegWit, Taproot, and Schnorr Signatures 103

• Taro 104

3. Bitcoin and the Future of El Salvador 104

9.4 Activity: Bitcoin Simulation 107

Class #10 -

Final Project **109**

• Why Bitcoin? 110

Clase Adicional -

La Magia de la Firma Digital **115**

• Claves Públicas y Privadas 116

• La Firma Digital 117

• Transacciones Válidas 117

Why Bitcoin?

Practical Exercise. Write below why you think it is important to learn about **Bitcoin**. There are no wrong answers.

Class #1

Introduction: The Monetary System

1. Activity: Introduction to Money
2. What are the problems with money today?
   - Consequences of the Development of Money
     - Needs vs. Resources
   - The Effects of Modernization
3. The Definition of Money
   - The Functions of Money
   - The Characteristics of Money
   - Conventional Money and Monetary Assets
     - The Types of Money
     - Activity: Are raisins a good money?

Introduction: The Monetary System

1.1 Activity: Introduction to Money

Class Activity. Wait for instructions from the teacher to perform this activity.

1.2 What are the problems with today's money?

It is a natural and healthy human impulse to overcome life's challenges - to better ourselves, to lead a productive, creative, and valuable life.

- We live in a world where there is a lot for a few, and very little for the many..
  - •Individuals with lower economic resources do not have the same opportunities. Why?
    - -They do not have access to the same levels of education.
    - -They are unable to access the credit necessary to start their businesses.

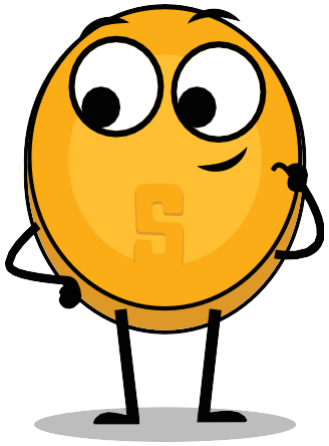
- To reduce poverty and stimulate social well-being, it is important to:
  - Improve access to financial education.
  - Develop the ability to manage money.
  - Learn how to use new technologies responsibly.
  - Know how to plan for the future.

We will see that **Bitcoin** is a tool and type of money that is:

- •Transparent, decentralized, borderless and global, digital, inexpensive, private, programmable, and easily and quickly accessible. Bitcoin's qualities can help remedy these circumstances.

SATOSHI

This is *SATOSHI*, an interactive assistant who will help you throughout the *Bitcoin Diploma*. *SATOSHI* will share data and recommendations as we go!



The Consequences of Development

- People have always needed to finance their future aspirations. They do this by exchanging wages, time, and energy for stores of value.

- If we had not invented money, we would have been stuck with a *barter economy*.
  - •Everything that someone would want to buy would have to be exchanged for something that that person could provide.

- Ongoing development of monetary systems has revolutionized societies and global interaction. In general, it has maintained a common interest in improving the quality of life of future civilizations.
  - As technology advances and productivity increases, we should see:
    - *Lower prices.*
    - *A strengthened currency.*
    - *The ability to buy more for less*
  - But the opposite is true:
    - *Prices go up, currencies are weakening, and we must spend more to buy less.*

- *How did we get here?*
- *How, why, and for what purpose is more money created and what are the consequences?*
- *What is hidden behind today's financial systems?*
- *What is the invisible danger of the loss of value of our money?*
- *How can we add value to our savings?*

● Today, only banks and governments have the power to issue money in an economy.

As a result, money simply does not run out. Governments print the necessary amount of money needed to finance their public expenditures, inject resources into the economy, and then withdraw them later in the form of taxes.

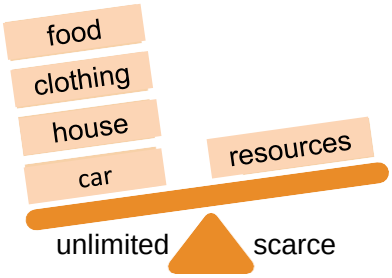
● The problem is that humanity spends more than it generates. As a consequence we have:

- A loss of confidence in the value of money and in the modern banking system.
- Global, economic, and political instability - even wars.

  - Why?

Needs vs. Resources

Our needs are infinite, but our resources are scarce.

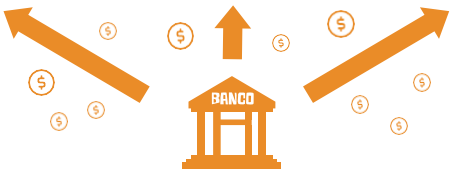


Modernization

"Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."

–Satoshi Nakamoto

Public administrations, companies, and many families need money and ask the bank for it. They pay interest on these debts to the bank.



The bank is an intermediary. That is, it buys money from savers and sells it to those who need it, at a higher interest rate.

Many families save. They deposit their money in the bank, and charge a small interest fee.

Introduction: The Monetary System

The banking business consists of:

- The purchase of money in the form of deposits from savers, and its subsequent sale through loans to those who need it.

- The banks profit, as in any other business comes from:
  - •A higher selling price than the purchase price – the interest rate of the money banks lend is higher than what banks pay to lenders.
  - •But the key to power in banking lies in the possibility of selling something which is owned not by the bank, but by the saver.

- Governments control the issuance of their currencies - they try to solve problematic economic cycles

- Governments print more money in times of recession to:
  - • Stimulate growth in the short term.
  - • Reduce short-term unemployment.

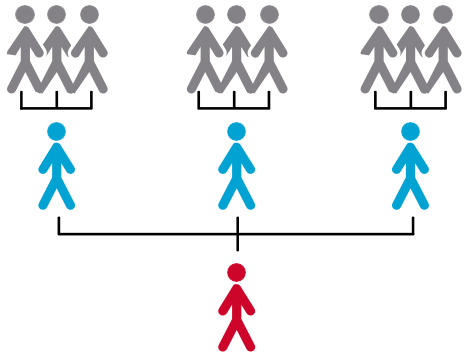
- The need for physical paper money has lost its importance.
  - •Internet banking has facilitated the use of credit.

The Benefits

— Banks facilitate immediate transactions and plan for the future.
— They record all movements of creditors and debtors in centralized databases.
— They constantly update the outputs and inputs of their users.
— They verify the legitimacy of the accounts.
— If the money disappears in an account for one of several reasons, it is replaceable.
— They have insurance policies in case they are victims of theft.

The Costs

— The banking system has a single source of failure, it is centralized and can be easily manipulated.



— Governments can:
  - Freely expand and contract the money supply.
  - Confiscate bank accounts.
  - Block withdrawals without prior notice.
  - Face serious technical problems or hacking.
  - Eliminate basic services.
  - Manage interest rates and taxes.

High inflation and negative interest rates cause the value of money to go down.

A bank is a place where they lend you an umbrela in fair weather and ask for it back again when it begins to rain."

- Robert Lee Frost

1.3 The Definition of Money

We pay in cash, check and/or credit card in exchange for goods and services.

•We rarely stop to think that all these means of exchange are only promises to pay.

Have you ever wondered what money is? In the following video, we will reflect on this.

— SATOSHI

Functions of Money

Money has **three functions**:

1.A store of value that can be invested, saved, borrowed, or lent
2.A medium of exchange to pay for goods and services.
3.A unit of measurement that allows us to compare prices between goods and services.

Store of Value. It tends to maintain its value over time.

Medium of Exchange. Eliminates the complex barter system by allowing the more efficient exchange of goods.

Unit of Measurement. It allows there to be a universal standard, a single price signal, to express the value of goods and services .

Practical Exercise. Write the name of the correct function of money in the spaces below.

_____ . The property of money that allows it to facilitate exchange because everyone accepts it as payment.

_____ . The property of money that helps us maintain our wealth, as it allows us to save and spend it in the future.

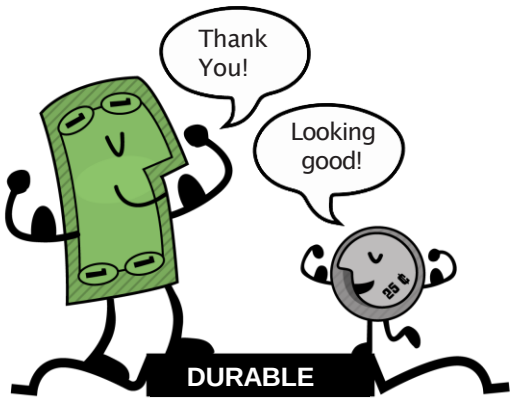
_____ . The property of money that allows us to measure the value of goods and services and to make comparisons between different goods. For example, an expensive price tag tells us something about the perceived value of the good.

Introduction: The Monetary System

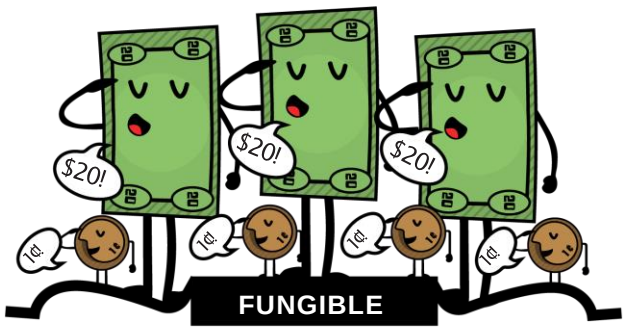
Characteristics of Money

Money can take many forms. The more of these characteristics a type of money demonstrates, the better money it is.

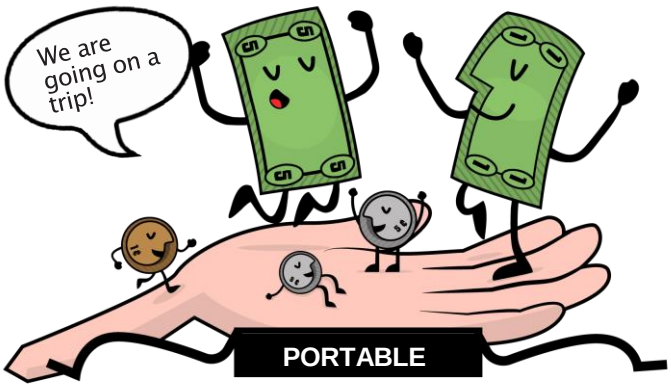
- **Durability**. Money must resist physical deterioration and last over time. It must be able to circulate in the economy in an acceptable and recognizable state.



- **Uniformity or Fungibility.** Each unit of money must be exactly the same as any other.

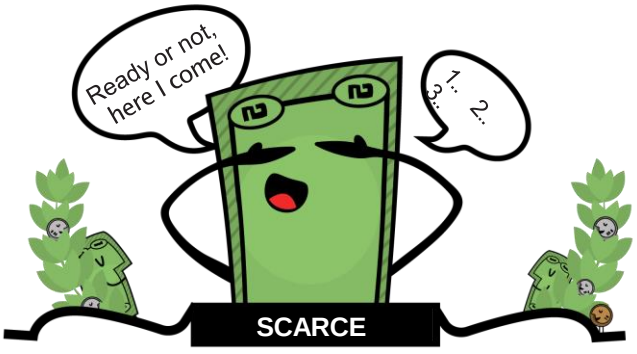


- **Portability**. It must be easy to move from one place to another. You must be able to accumulate a lot of value in a small weight.

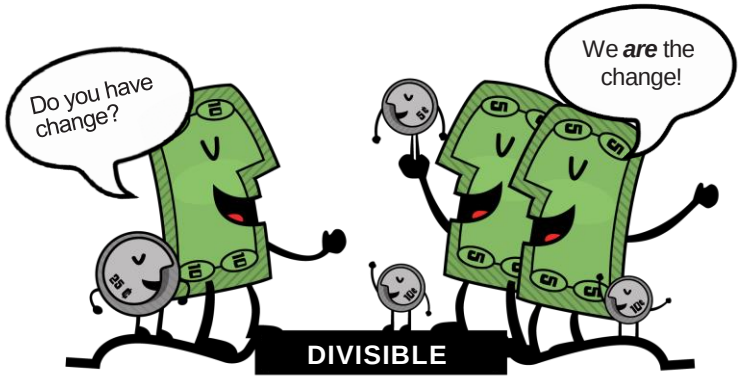


- **Recognizability or Acceptability.** The item used as money has to be recognized by everyone as money.

- **Scarcity.** The value of money depends on supply and demand. The more money is created, the more its value is decreased.



Divisibility. It must be tradeable for both expensive and inexpensive goods, and be easily divided without losing its value.



Conventional Money vs. Monetary Assets

● **Conventional money** is the money of general use in a particular society.

- •Includes cash in circulation, bank deposits, and central bank reserves.
- •Most money consists of credit or electronic entries.
- • *Conventional money does not necessarily save its value over time*.

● **Monetary Assets** generally *do keep their value over time*.

Types of Money

Commodity Money

- • Difficult to extract, therefore, scarce.
- • Attractive as a store of value.
- •Gold and silver endured as good money for thousands of years.

— [Monetary Assets]

Representative

- • Banknotes backed by gold or silver.
- •Each bill is exchangeable for its equivalent value in metal.
- •In modern history, the gold standard was adopted until 1971.

— [Monetary asset initially, but becomes conventional money over time if the money supply is increased].

Fiat / Trust Currency

- •Implemented as a monopoly and issued at will by a government.
- •It is not backed by a physical product.
- • It has no intrinsic value, its value relies on:
  - -The relationship between supply and demand.
  - -The stability of the issuing government.

[Conventional Money. Digital fiat has more counterparty risk than physical ~~risk~~].

Bitcoin

- • Scarce digital money.
- • Operates in a decentralized way.
- •It is based on software and "peer to peer" cryptography to perform movements.

— [Monetary Assets]

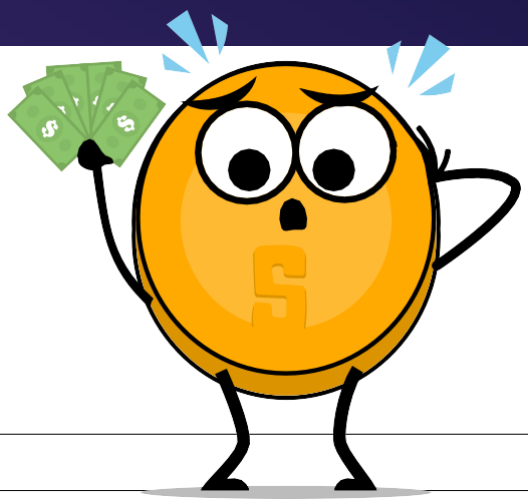
Introduction: The Monetary System

Practical Exercise. Mark with an **X** if the item has the indicated property.
Which item would you choose as money? ** Do not fill in the last column 'Bitcoin' until after completing Class #4.*

Characteristic	Apples	Shells	1oz. Gold	1 USD	Bitcoin
Uniform or Fungible					
Divisible					
Portable					
Scarce					
Durable					
Acceptable					

Which item would you choose as money and why?

Activity: Are raisins good money?



Class Activity. Wait for instructions from the teacher to perform this activity.

Class #2

The History, Evolution, and Devaluation of Money

1. The History of Money
2. Activity: Bartering Game
3. The Evolution of Money Over Time
    - The International Monetary Standard in History
4. The Sudden Change to Fiat
5. Central Banks
6. *Class Activity: The Fractional Reserve*

The History, Evolution and Devaluation of Money

2.1 The History of Money

Money is something we use every day, but rarely do we stop to ask: Where did it come from? How did our ancestors trade?

- What has constituted as money has varied over time and place

- Money is as old as language itself. It is simply a form of communication, a technology.

- There is no single universally agreed on definition of money.

- In principle, we would not need a special asset such as a bill to recognize who is owed goods and/or services.
  - •Anyone can have and maintain their own ledger.
  - •Our ancestors traded in this way and/or through barter without the need for banks or conventional money.

2.2 Activity: Bartering Game

Back to the Past: Bartering

In order to produce a barter, there must be a **double coincidence of needs**.

- A person who wants to exchange something needs to find a business partner who has what he wants and wants what he has.

- This means of exchange of goods and services requires a lot of time, restricts economic activity, and limits specialization.

- The use of money alleviates these problems.

Class Activity. Wait for instructions from the teacher to perform this activity.

1. What is bartering?

2. What are the main problems with bartering?

3. What is commodity money?

4. What problems arise when commodity money is used?

5. What is money?

6. Why are people willing to accept money?

The History, Evolution and Devaluation of Money

2.3 The Evolution of Money Over Time

The exchange of material goods or services for other goods or services. — is — BARTERING

Where money is not used

Evolution of Money Over Time — arose — As a need of the community and sociopolitical structures.

Money ≠ Monetary Units

COMMODITY

One asset represented money

which had

- **intrinsic value**
- **usage value**

met the characteristics of

- Being accepted as a means of payment
- A measure of value

examples

- salt
- cocoa
- livestock

CASH

Money was expressed

in

- **coins**
- **metal species**

they were characterized by being

- easy to transport
- divisible
- storable

the first coins were minted

- gold
- silver
- copper

PAPER MONEY

The issuance of supported documents

by

precious metals (which are accepted by everyone)

They were characterized by being

- easy to transport
- divisible
- full government backing

FIAT MONEY

It is backed by the trust of a society

not based on value

otherwise

in the general belief that such money has value

which led

creation of central banks

Authoritarian Monopoly

PLASTIC MONEY

Creation of the credit and debit card system.

as well as

- electronic wallets
- debit/credit cards

works like

banking transactions (lending a substitute value to cash)

CRYPTOCURRENCIES

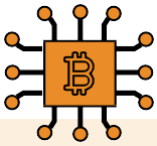
A digital medium of exchange that secured with strong cryptography

- transactions
- unit creation
- verify the asset transfer

they are independent from banks

its value depends on

- usability
- supply
- demand



The International Monetary Standard in History

Bimetallic Pattern (17th-19th centuries)
Banknotes could be converted into gold and silver.

Gold Standard (1870 - WWI)
Any citizen could convert their paper money into a preset amount of gold.

Interwar Period
The two wars and the Great Crash of 1929 put an end to convertibility into gold for individuals.

Bretton-Woods Pact
At the end of World War II, in 1945, the allies established that the currencies were convertible into US dollars.

Crisis of the 70's
In 1971, the US economic situation, coupled with the Vietnam War, caused the ECB's to try to convert their dollars into gold, which created a crisis in the US and had Nixon suspend the convertibility of the dollar into gold.

Current Stage
Since,1973, until today, money is fiduciary and digital money.

Let's watch the following video so that we can all understand money, its evolution and key concepts.

- Money has evolved throughout history, facing challenges and changing needs.
  - •Normally, the form of money that offered the superior characteristics was chosen.
  - •But since value of currencies, initially grounded in monetary assets, began to be diluted due to the transition from precious metals to paper-backed metals:
    - We moved from a natural selection of the best performing form of money, one of ease of use, greater portability, and divisibility.
  - • This led to a shift towards centralization.

2.4 Sudden Change to Fiat

The industrial era marked the beginning of the centralization of money in the modern world:

- The objective was to efficiently distribute produced goods.
  - • Central Banks were created.
  - •The credit and debit card system was born.

- When the control of money is centralized, profound problems can occur.
  - •Governments closely monitor the economic activity of their citizens.
  - • Abuse of power can lead to:
    - -Manipulating economic incentives through government interventions.
    - -The explosion of debt and irresponsible consumption.
    - -An increase in wealth inequality.

1971, representative money was used as a *medium of exchange* and *store of value.*

- Starting in 1971, we moved away from sound money to a debt-based economy.
  - •Richard Nixon, eliminated the free convertibility of gold for money.
  - •We moved on to the current experiment, which is ***fiat money***.
  - •Modern money is valid by decree rather than consensus.
  - •***Fiat*** comes from Latin and means by decree: it is chosen and established by law.

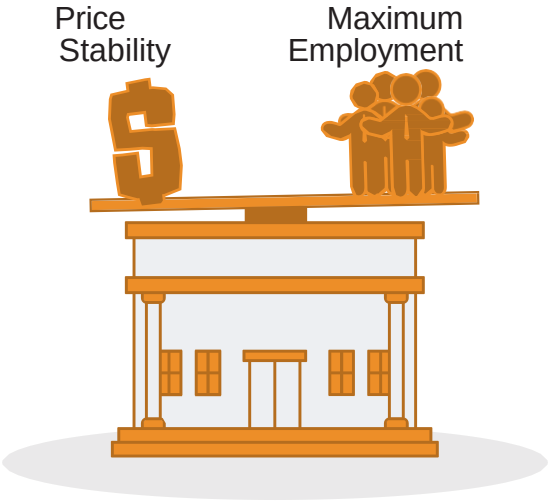
"That which worked yesterday, will not necessarily work today."

- Jordan Peterson

2.5 Central Banks

- The purpose and function of a ***Central Bank*** is:
  - To control a country's monetary policy in order to manage economic stability.
  - They function as the banker for the banks.
  - Their main job: to manipulate the supply of money in circulation.
    - Control inflation and maximize employment with economic and financial policies.
  - The U.S. Central Bank is called the *Federal Reserve*.

The Federal Reserve has been given a dual mandate:



- Who defines and who benefits from these objectives?
  - Large banks can influence federal and even global policies.

- How does the Federal Reserve alter the money supply?
  - Through the **fractional reserve** banking system.
  - Banks in the U.S. only hold 10% of their deposits in reserve..
  - Fractional reserve banking results in a **bank multiplier**.
    - *More than two people use the same money at the same time in a country's economy.*

Banks are required to keep a certain percentage of all deposits in the bank. Reducing that percentage means that more money can circulate, and increasing it means that less money circulates.

- What problems can be caused by **fractional reserve banking**?
  - Banks "borrow and lend on a long-term basis."
    - -Deposit withdrawals can exceed cash reserves.
    - -Banks incur large losses.
    - -In the worst-case scenario, a bank run may occur.
  - Changes in interest rates or the cost of capital affects risks.
    - -More money in circulation means cheaper and less demanding loans.

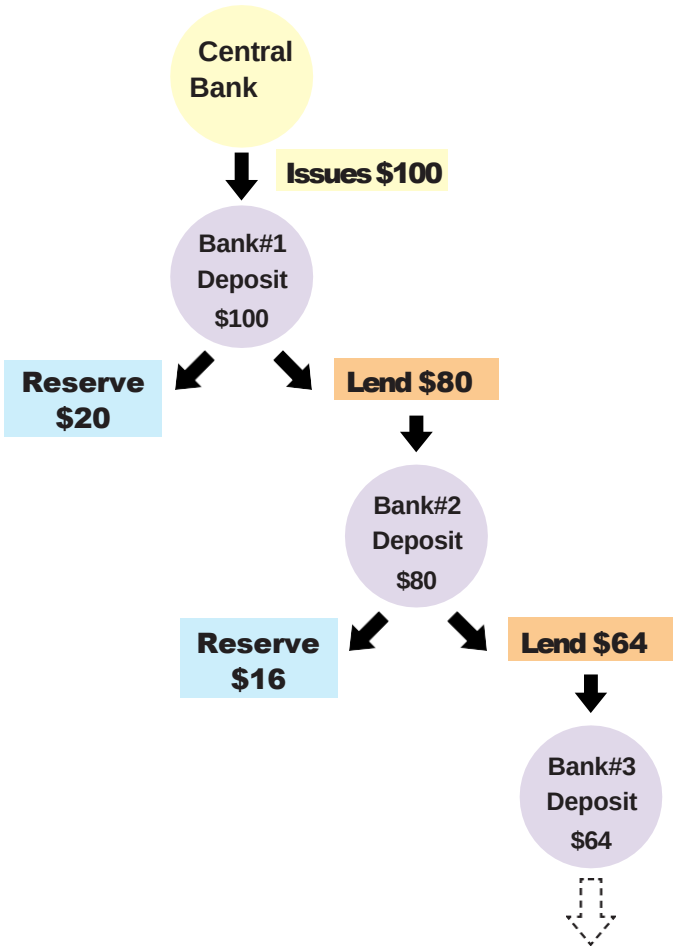
- Open market operations (*to increase or decrease the money in circulation*).
  - The government buys or sells monetary securities (high liquid debt).
    - -If you want to increase it: buy treasury bonds.
    - -If you want to reduce it: sell treasury bonds.

2.6 Activity: Fractional Reserve

Class Activity. Wait for instructions from the teacher to perform this activity.

BANK REGISTER

	Loans	Dollar Deposits	10% Reserve Requirement
Depositor A			
Borrower A			
Depositor B			
Total Dollars			



Class #3

The Effects of Fiat Money and Centralization

1. Activity: Auction!
2. Inflation
   - Why Does Inflation Matter to Us?
   - What do Modern Economists Teach About Inflation?
   - The Causes of Inflation
   - Inflation Through Time
3. Surveillance
4. Restrictions
5. Centralization vs. Decentralization
6. Conclusion

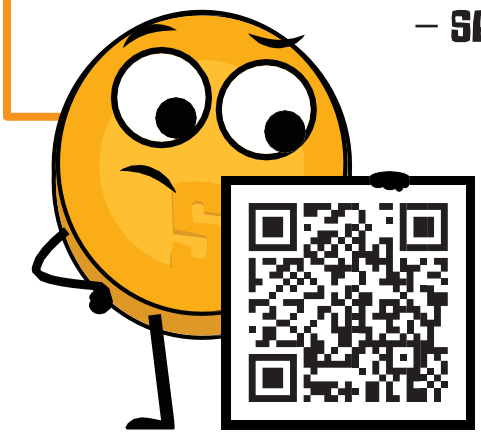
3.1 Activity: Auction!

Class Activity. Wait for instructions from the teacher to perform this activity.

3.2 Inflation

Let's analyze the following video about inflation!

— SATOSHI



- The term ***inflation*** was originally used to indicate:
  - The loss of value of a currency.
  - The devaluation of its purchasing power caused by the increase in its supply.

- This loss of value normally produces, in terms of that currency:
  - A general and sustained increase in the price of all goods and services.

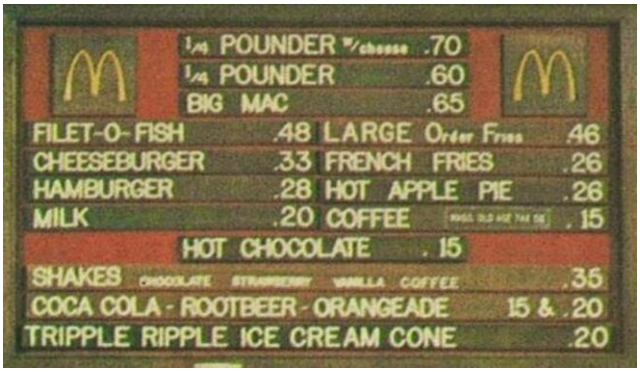
- The term "inflation" has come to be used to indicate price increase.
  - Regardless of the cause

Why do we care?

- When more money chases the same number of assets:
  - Prices go up.

- If product prices increase faster than wages and salaries:
  - People become poorer.

McDonald's in 1970



McDonald's in 2020

What do modern economists teach us?

- We need to stimulate inflation in order to effectively manage an economy.

- If we do not incentivize spending and investment (through currency devaluation):
  - We risk a lower demand
  - Leading to decreased production
  - Worst case, this can result in a stagnant economy.
  - All this implies that it is difficult, impossible, or even unwise to save.

The Effects of Fiat Money and Centralization

- The current situation encourages us to spend. It is a counterproductive theory.
  - •We don't think about a future beyond a couple of days, weeks, or months.
  - •We should be able to prepare for the future of our grandchildren.
  - •Inflation prevents us from having financial discipline.

- All decisions have consequences.
  - •This is known as "***opportunity cost***".

Study

- **Best career option.**
- **More prepared.**
- **Academic prestige.**

Work

- **Salary received.**
- **Work experience.**
- **Social prestige.**

➡ One has *a high time preference* when one prefers things one can get now to things one might get in the future.

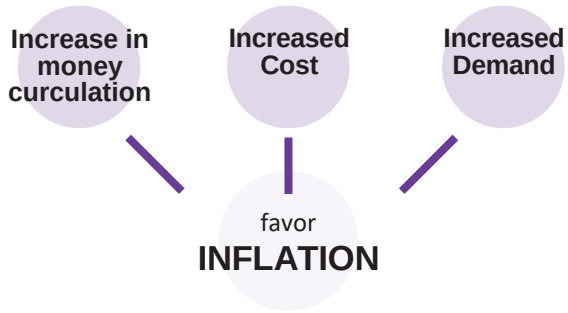
➡ One has *a low time preference* when one prefers to do things in the present in order to obtain better things in the future.

- Inflation encourages a *High Time Preference*, which means that we prefer $100 today instead of $200 in two years.

- Our goal should be to create a *Low Time Preference*

High Time Preference	Low Time Preference
Spend Money	Saving Money
Fast Food	Cooking at Home
Browsing Socials	Reading a Book
Watching TV	Exercising
Consuming Content	Creating Content

Causes of Inflation



In the following video, you will learn the three reasons why inflation occurs.

1. Cost or Supply Inflation

- Increases the price of inputs, and is caused by:

•Government regulations, wars, droughts, supply chain difficulties, and other situations.

•Rising tax rates increase the cost of raw materials.

•Specialized jobs become more expensive.

-Lack of skills or resources in a society.

- New technologies are usually very expensive.

-Over time, they lower the costs of products.

2. Demand Inflation

- The supply of goods is not enough to meet the demand.
- Due to a reduction in taxes (or a reduction in interest rates on loans), an increase in disposable income is created:

•Excess money begins to circulate in the market.

•There is competition for the same goods with more money.

- This drives up prices.

- Eventually the supply increases, and then prices go down again.

3. Inflation by government policies

- The government finances the deficit by printing more money.

•Are the jobs/projects created through inflation authentic?

•Why is it important to governments that people buy things with their money?

•What types of goods do we buy as a society when there is more money in the economy? Are they essential goods for living?

•What happens when tax rates rise faster than the increase in wages in an economy?

- Inflation means that the work you did a while ago has less value than today.

•Last year you were paid $10; you could buy 10 lunches for $1 each. You decided to save your money.

- Today:

-There is more money circulating in the economy.

-There are more people wanting to buy lunches.

-The same number of lunches are for sale.

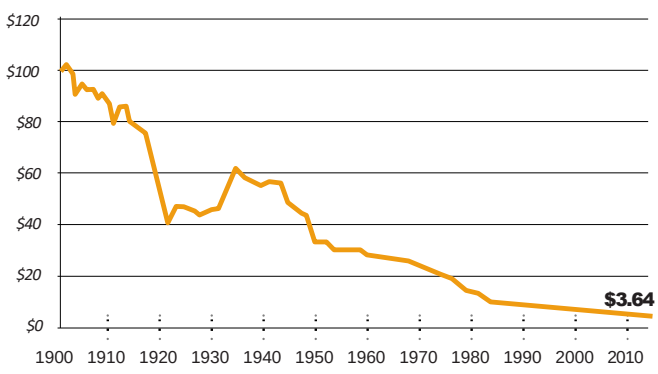
- The price rises to $2 per lunch.

•Today you can only buy 5 lunches with the $10 you saved from a year ago.

•In theory, this doesn't make sense. If you put in 8 hours of work, that reality does not change even if 10 years have passed. That energy should be able to stay with you.

- We could say that inflation is a type of theft of value.

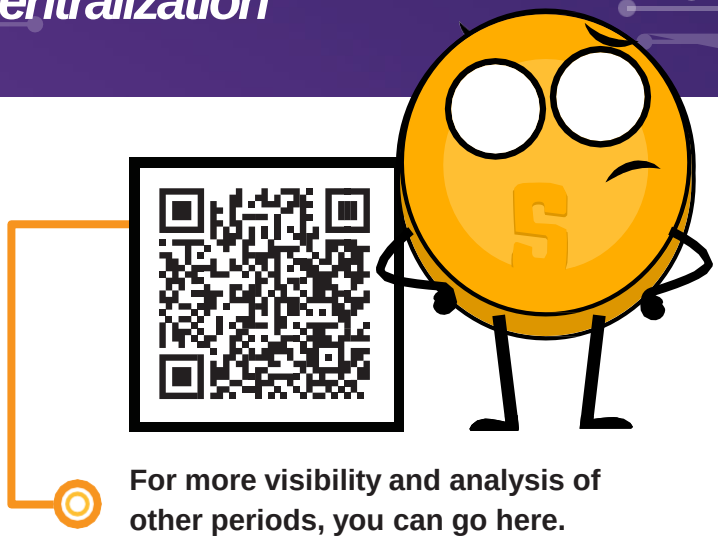
- The following graph shows the loss in value of the dollar (USD).



The Effects of Fiat Money and Centralization

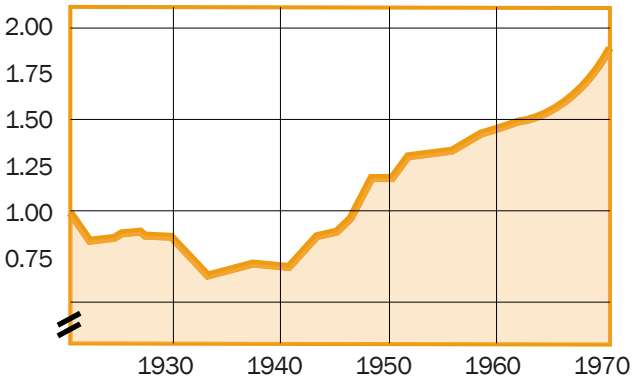
Inflation Through Time

- Inflation between 1970 and 2020 was much higher than that of the previous 50-year period, 1920 to 1970.
  - •What will happen if we continue in the same trajectory?
  - •Who had greater economic hardship, your grandparents' generation or your parents' generation?



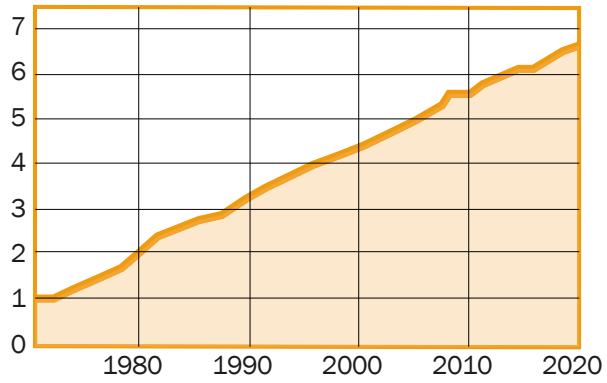
For more visibility and analysis of other periods, you can go here.

$1 from 1920 to 1970



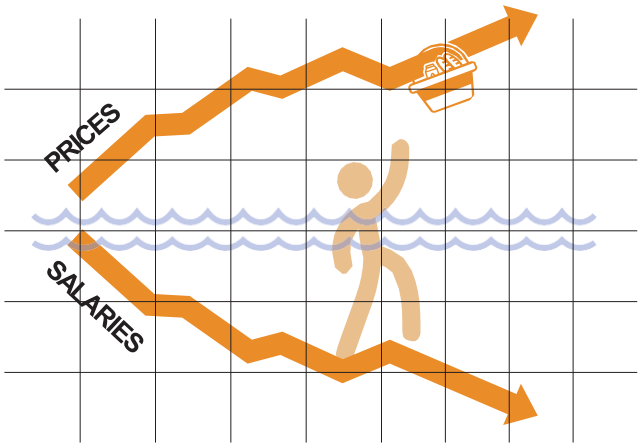
Result: **$1.94**
Average Inflation Rate: **1.33% per year**
Total Inflation Factory: **93.72%**

$1 from 1970 to 2020



Result: **$6.67**
Average Inflation Rate: **3.87% per year**
Total Inflation Factor: **566.60%**

- Do you think wages and salaries went up at the same rate as prices?



- In other words, what we can buy today (2022) with $100 would have cost us approximately $7 in 1920.

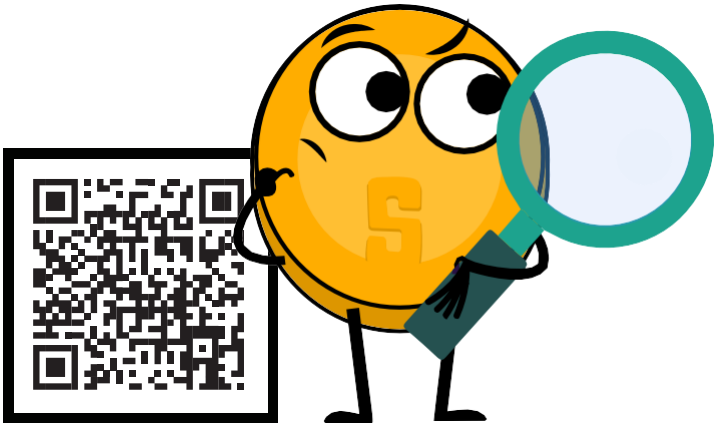
- Inflation causes a loss in ***purchasing power***:
  - -Increases in wages are lower than increases in food prices.
  - -Individuals are forced to reduce their consumption.
  - - ***Overall purchasing capacity is reduced.***

INFLATION WINNERS	INFLATION LOSERS
THE STATE Because with higher prices and wages, their tax revenues increase while their expenses increase at a much lower rate.	**SAVERS** Who see how their savings are worth less and less.
THOSE WHO CAN BORROW Since inflation will make it easier for them to recover money while the debt remains fixed.	**LENDERS** Since when they get their money back, they will be able to buy less with it.
	PENSIONERS AND WORKERS Since pensions and wages tend to rise less than prices.

3.3 Surveillance

- Governments impose regulations in order to find and catch people who launder money or make other illegal transactions.
  - Surveillance is a double-edged sword.
  - The more fraud occurs, the more vigilance on the part of the State and private companies:
    - -Invade our privacy thanks to technological progress.
    - -Control our movements on social and economic networks.
    - -Sell personal data of users in exchange for the enjoyment of certain services.

- Some of the consequences are:
  - Digital scams, online harassment, extortion, identity theft, and other problems that jeopardize the privacy and security of users.
  - Our card purchases are tracked, analyzed, and monitored.
    - Unless we use cash to purchase goods and services.
  - If someone gets your password for your internet banking, or hacks the centralized servers, they would have access to all of your information.



We need money that protects our privacy and does not share all our personal information with governments and private companies.

3.4 Restrictions

- It is difficult and costly to move money between nations.

- Governments control foreign currency exchanges, even if it is between two known persons.

Here is a list of policies and ways in which this can happen:

The Effects of Fiat Money and Centralization

Government Policies

- *Capital Control*: The amount of money that its citizens can transfer, exchange, or take abroad is restricted.
  - Examples:

- Ar*gentina, Russia, Indonesia, Cuba and China.*
-The average Chinese citizen can only convert up to $50,000 of renminbi (~$8,000 USD) a year.

"The only solution we have found in Cuba is Bitcoin. We are now on equal footing, with equal ability to compete with any other country because we have full, free access, without sanctions or prohibitions to a technology that allows us to create, grow, and connect."

-Eric García Cruz, Cuban entrepreneur and Bitcoin enthusiast.

Banking Policies

- Banks have limits on the amount of cash that can be withdrawn from an account, or they have a maximum amount than can be transferred.

- Most of these transactions have commissions.
  - Examples:

-After its 2015 crisis, *citizens of Greece* could only withdraw *$60 euros a day.*
  - This is a clear reminder of who really controls your money.

-In El Salvador, remittances represent 23% of their gross domestic product (GDP).
  - In 2020, it was almost $6 billion. About 60% of that money comes from remittance companies and 38% from banking institutions.
  - Companies like Western Union have very high rates,
  - Especially for amounts less than $1,000 USD.

Commissions or Charges

- These charges only enrich the banking institutions.

- They only increase the gap between rich and poor.
  - For small amounts, say $10, commissions can be up to more than $3, or 33%.
  - For $ 100, the rates range from 12% to 15%.

Schedule

- To send/receive a remittance:
  - Both the sender and the recipient must go to the nearest branch office.
  - This must be during business hours, of course.

Security

- Visiting a Western Union office poses additional risks:
  - People must bring their cash in person, increasing the chances of being robbed.
  - If centralized servers fail (which happens frequently), access to any client's funds may be denied.

3.5 Centralization vs. Decentralization

- The centralization of modern economies leads to:

• Censorship, abuse of power, corruption, inequality of opportunity, inequality of wealth, and single points of failure.

- Banks operate through centralized servers.

• This means that banks have access to all the financial activities of its users.

What do banks know about their customers?

- How much you get paid.
- What you spend your money on.
- Who you send your money to.
- Everything else related to your account.

Characteristics of a Centralized System

- You have to trust that the centralized organization will keep your data safe and secure.
- They have complete control of the system and your data.
- If the main servers are compromised, your data is at risk.

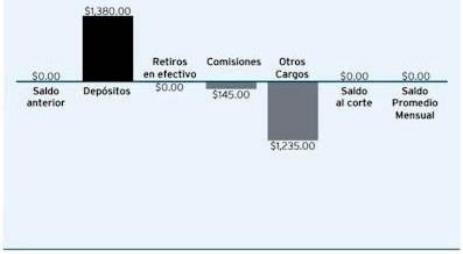
Central bank digital currencies (CBDC's) are the continuation of the current system, but in digital form. That is to say: mutable, censorable, closed, centralized, exclusive, and surveilled.

Carlos Pérez Pérez.
Av. Independencia # 543 interior 2.
Col central C.P 34004

BANCO

Contrato: 25687451
Sucursal 1
Cuenta: 123321
Clave Interbancaria: 00000123321
Cliente: 963258
RFC: PEPC920212R47

Comportamiento

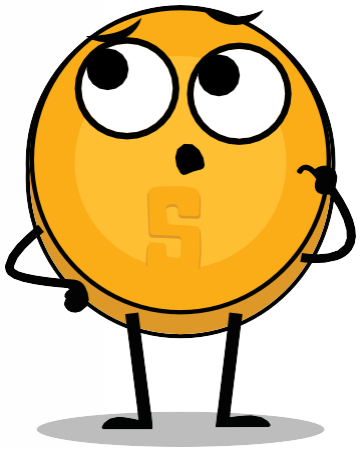


Resumen En Pesos Moneda Nacional

Saldo anterior	0.00
Depósitos	1,380.00
Retiros en efectivo	0.00
Otros cargos	1,235.00
Saldo al corte	0.00
Saldo promedio mensual	0.00

Detalle de Operaciones En pesos Moneda Nacional

FECHA	CONCEPTO	RETIROS	DEPÓSITOS	SALDO
25 DIC	SALDO ANTERIOR			0.00
11 ENE	PAGO RECIBIDO DE BBVA BANCOMER			
	POR ORDEN DE MAURICIO DEL			
	MORAL DURAN REF.0000001			
	ARTICULOS RASTREO:			
	BNET01001601110002067854		1,380.00	1,380.00
11 ENE	IVA POR COMISION MANEJO DE			
	CUENTA	23.20		1,356.80
11 ENE	COMISION PENDIENTE MANEJO DE			
	CUENTA 8110401166	145.00		1,211.80
11 ENE	COBRO DE 600501077330			
	MAS9106148R6 Domi Asistencia			
	Familiar 10	89.00		1,122.80
11 ENE	RETIRO POR TRASPASO	1,122.80		0.00
22 ENE	COMISION MANEJO DE CUENTA			
	PENDIENTE POR: 145.00 MAS			
	I.V.A.			0.00



How do we counteract these phenomena, which are caused by bad government policies?

Characteristics of a Decentralized System

It is described as a peer-to-peer, or P2P system because:

- People do not have to identify themselves to interact and be interconnected with each other through the internet.
- Everyone is responsible for their own device but incentivized to lend and share their resources.
- If there is an attack on the network, hackers would have to control a majority of the computers – this is almost impossible.
- In the event of an error or failure by one server, the rest will not be affected.
- It achieves a more fair and just society – takes control away from powerful corporations.

3.6 Conclusion

Let us ask again, will there be a solution to today's money problems?

THIS **WAS MONEY**

=

Backed by gold and silver

THIS **IS PAPER**

=

Backed by "good faith and government credit"

THIS IS THE FUTURE

Backed by the citizens of the world with the use of technology.

=

Class #4

Bitcoin

1. Why was Bitcoin created?
   - What problems need to be solved?
   - How were these problems solved?
   - Who solved these problems?
   - What difficulties did Satoshi face?
   - What is the Byzantine Generals' Problem?
   - What does this have to do with Bitcoin?
2. Introduction to Bitcoin
3. Differences between Bitcoin and Fiat
4. The Participants of Bitcoin

4.1 Why was Bitcoin created?

The 2001 attack on the Twin Towers in New York was a major blow to the world economy. As a result, with the support of the private sector and the objective of facilitating mortgage financing for people with lower-incomes, the US began to rapidly lower interest rates to levels never seen before.

Thus, loans and credits were given to people without income, assets, or employment. These types of mortgages were baptized "subprime mortgages," and of course, they had a high probability of default. The effects of this crisis are still being felt today. The peak occurred on September 15, 2008, when the investment bank, Lehman Brothers, declared bankruptcy. From that moment on, the United States has suffered an economic collapse, followed by the rest of the developed world. Consequently, day-by-day mistrust in banks grew due to their excessive risk taking and lack of regulation in the industry.

What problems need to be solved?

- ***The lack of individual sovereignty.***
- ***The Centralization of banks.***
- ***Inflation.***
- ***Surveillance.***
- ***The need for intermediaries.***
- ***Poor accessibility to banking services.***
- ***The high cost of international remittances.***
- ***And more...***

How were these problems solved?

- With the use of technology developed in 1991, called the *blockchain*.

The *Blockchain* is a core part of the technology behind **Bitcoin**, the most famous digital currency. The Blockchain is a decentralized online database that functions as a transaction ledger. It is a decentralized *peer-to-peer* payment network. It uses cryptographic keys and is distributed and shared across many computers, thus reducing the risk of fraud and counterfeiting.

Who solved these problems?

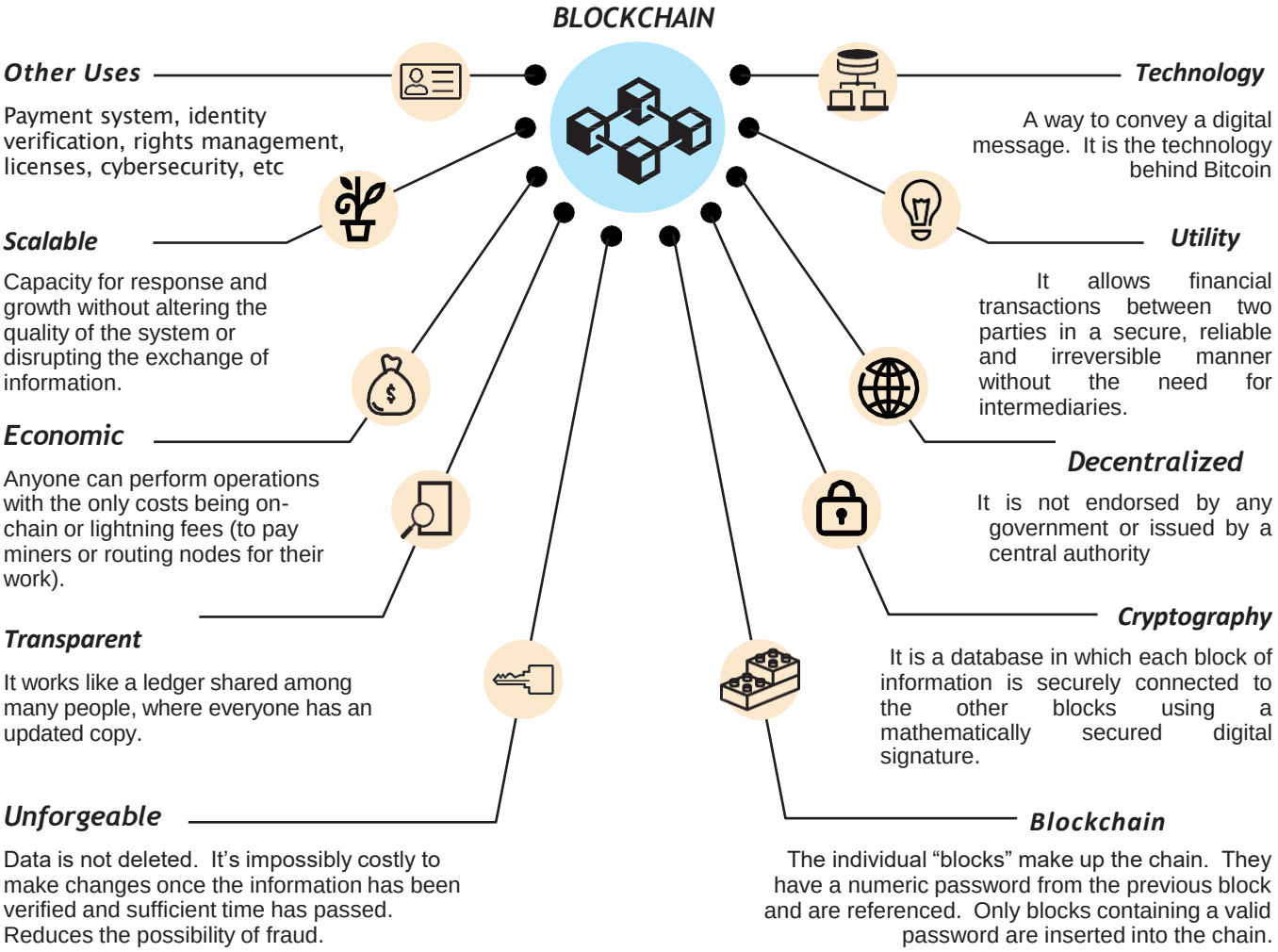
- *Satoshi Nakamoto* appeared in October 2008. His identity is still a mystery.

- He proposed his idea of a new electronic cash system. This money would be called ***bitcoin***.

- He devoted his time to creating a guide to explain a new means of payment that:
  - •Enables the execution of fast, low-cost value transfers.
  - •Cannot be controlled or manipulated by governments or financial institutions.

- Thanks to this person, or group of people (it is not known), there is a solution to the problem of *"double spending"*.
  - •With Bitcoin it is impossible for anyone to spend the same virtual money if it has already been spent.

- The nine page document that explains how Bitcoin works is known as the *Whitepaper*.



•Satoshi shared his idea to an e-mail list called *Cypherpunks*:

-A small, but active group with technical discussions.

-The discussed mathematics, cryptography, computer science, politics, philosophy, and even personal arguments.

● Satoshi had cynicism towards the traditional monetary and banking system.

• This can be seen in the *genesis block*, where he posted a message that read:

Here you can download the Whitepaper by Satoshi Nakamoto.

Bitcoin

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

- Satoshi Nakamoto, Genesis Block.

- It is in reference to an article in the *Times newspaper titled* "*Chancellor on brink of second bank bailout*".
  - •The British Chancellor was deciding whether to inject (print) billions of British Pounds into the economy to rescue the banks..

- Here are some other basic facts we know about Satoshi, his *Whitepaper* and the creation of **Bitcoin**:

1. The whitepaper is 9 pages.
2. It describes an "electronic money" system without intermediaries.
3. The word blockchain does not appear in the paper.
4. It defines a digital currency as a chain of digital signatures.
5. The term 'mining' came from an analogy that helps us teach 'proof of work.'
6. Bitcoin's base layer focuses on more secure transactions rather than tx speed.
7. The increase in the size of the chain was initially estimated to be at 4.2 MB/year.

- The first ***bitcoins*** transaction was from Nakamoto to a cypherpunk named Hal Finney.
- Satoshi's last known "sign of life" was with Gavin Andersen, a software developer:
  - *"...I've moved on to other things,...It's in good hands with Gavin and everyone."*

- In public messages, and even in private messages that were later published, Nakamoto never spoke about anything personal. It was all about bitcoin and its code.

- Many people have claimed to be Satoshi, but we still do not know who he is.

- It is estimated that Satoshi has approximately 980,000 bitcoins.

What challenges did Satoshi face?

- Could someone send the same money to two people at the same time?

- On the internet, who can trust whomever is on the other side?

- How do we know if someone has enough money in their account (or wallet) to buy one product from another?

- How do you ensure that a decentralized network can make correct decisions, even if some of the nodes (connected participants) are dishonest?

- Can we created a distributed and reliable system that does not automatically assume that the participants will act ethically and work in the interest of the group?

- How do we know that the person who wants to receive money through this system is who they claim to be?

"Double Spend Problem" = "Byzantine Generals Problem"

What was the Generals' dilemma

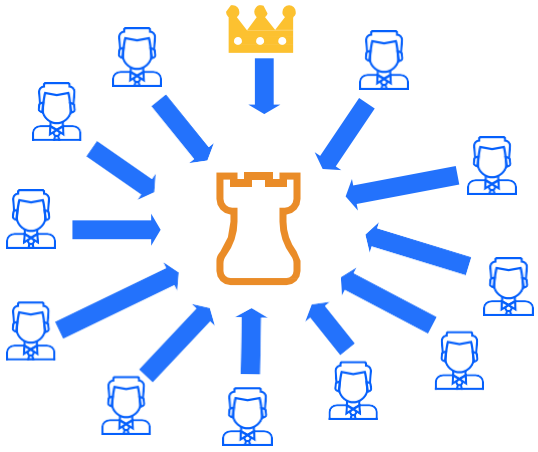
- The problem of the Byzantine Generals is a metaphor for the difficulty of transmitting reliable information without the intervention of a trusted central coordinator.

What is the story?

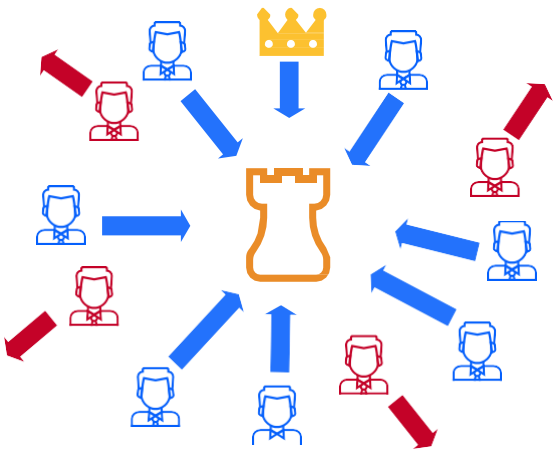
- There was a castle in Persia, which is very well supplied and fortified.
- The Byzantine generals have surrounded the castle and plan to launch an attack.
- Since the army is so dispersed, there is no centralized control (Hence multiple generals!).
- The generals communicate with each other through messengers.
- The two possible commands are "attack" and "retreat".
- They all must agree to attack the Persian army, and they must do so simultaneously.
- If any of the generals attempt to attack separately, they will lose the battle.
- If there is a traitor in the ranks, he could persuade the loyalists to disagree.
  - For example, a traitor could tell one general to attack and another to retreat.
- One morning, a general receives the following message: "*The attack will take place on Tuesday*." It does not bear the signature of any central authority.

How can the general be sure that it is a true order and not a deception of the enemy transmitting information contrary to the strategy of the army?

What happens if the one who sent the message is a traitor and plans to betray the army? What happens if the general himself is corrupt and seeks to sow discord among the other generals?



Coordinated attacks lead to victory.



Uncoordinated attacks lead to defeat.

The solution to this problem was originally used as a method to avoid email spam.

What does this have to do with Bitcoin?

The problem of the Byzantine generals describes:

- The difficulty that decentralized systems have in agreeing on a single truth.

- It is the same as when you make a money transfer without a reliable intermediary.
  - A way is then required to verify that the message has not been modified, which had not been achieved until the appearance of Bitcoin with its *consensus* mechanism.

- The use of cryptography is essential in this process, but what is *cryptography*?
  - Cryptography in Bitcoin is used to digitally sign and verify transactions on the Bitcoin network.

- **Bitcoin** also uses a *proof-of-work* mechanism and a *blockchain* to solve the "*double spend*" problem.

- **Bitcoin** achieves:
  - 1) The ability to transfer a digital asset (or money) to another user over the Internet.
  - 2) So that only the owner can initiate the operation.
  - 3) Only the addressee can receive it.
  - 4) Everyone can validate the transfer.
  - 5) And it is recognized by all participants.
  - 6) It is immutable, or impossible to reverse or delete.
  - 7) All of the above is done in a totally *distributed* and *decentralized* way.

- Within the blockchain framework, each 'General' represents a *node in the network*.

- The nodes must reach an agreement to determine the current status of the shared accounting record.
  - -If the majority of the network on the blockchain agrees, the transaction history is updated in each wallet where bitcoin was sent and received.
  - -If a large majority of the network is malicious, the system is vulnerable to failure.

4.2 Introduction to Bitcoin

What is Bitcoin? *What is* ***bitcoin****?*

- It is many things

- **Money**. A virtual and intangible currency that fulfills the three functions of traditional money: a unit of account, a store of value, and a medium of exchange.

- **Software**. Software that you can download and run on any computer.
  - A *payment system* without a central bank or single authority.

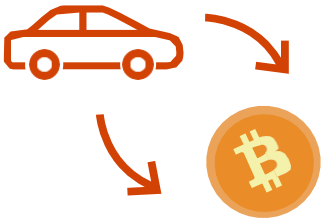
- **Network**. Set of people and computers working through consensus to function seamlessly.

It is a currency, like others.

But it is digital.

Not controlled by a central authority.

It is exchangeable for goods or services.



It is portable and secure.

It can be used in thousands of stores and has the same value throughout the world.

What is the difference between ***Bitcoin*** ***and*** ***bitcoin****?*

Bitcoin with 'B' refers to the network of computers that works with the same program, while ***bitcoin*** with '**b**' refers to the digital asset ($) that is managed within the network. In other words, ***bitcoin*** is a unit of virtual currency encrypted by cryptography, which serves us to exchange value within the **Bitcoin** network.

What is its main function?

- It allows for the transfer of peer-to-peer (P2P) payments, without intermediaries, economically, and without international barriers. It is a store of value.

What technological breakthrough has it achieved? Why will it revolutionize banking?

- It prevents people from spending the same money twice.
- It eliminates the need for a central authority to monitor transactions.

What makes it valuable?

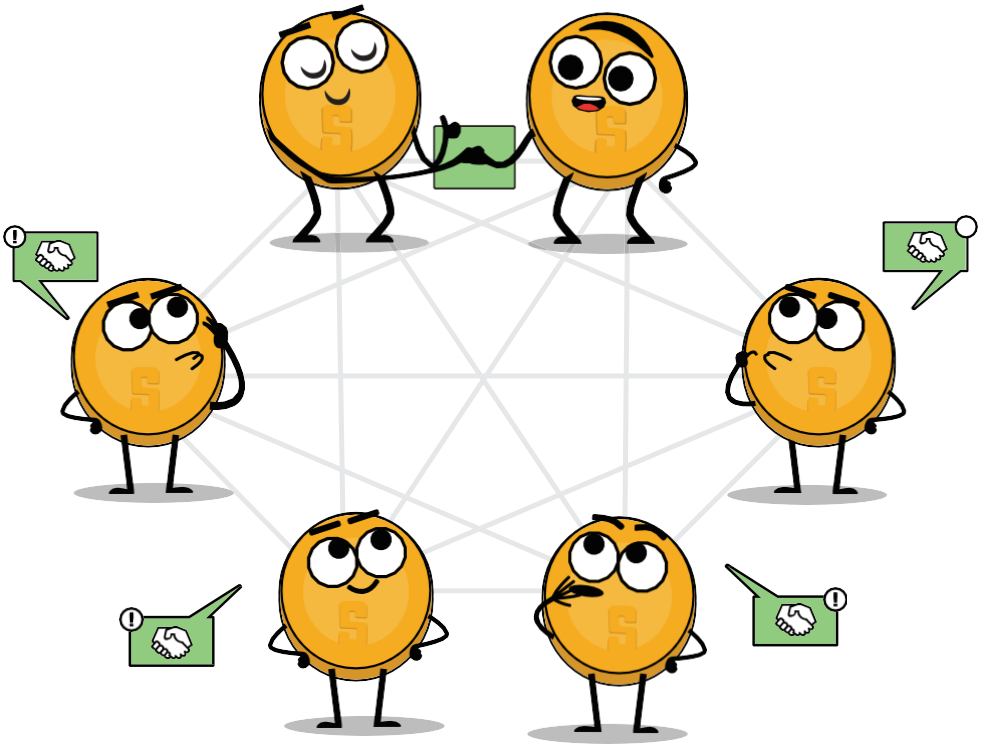
Bitcoin

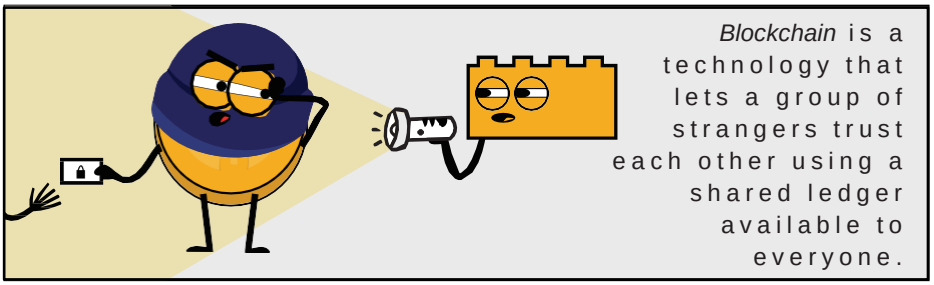
*What is the relationship between blockchain and **Bitcoin**?*

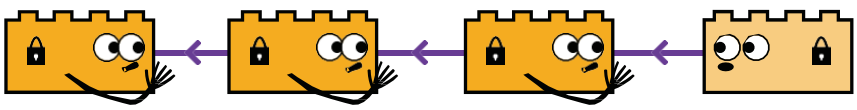
- The blockchain is the public ledger where the most important **Bitcoin** transactions are permanently recorded.
- **Bitcoin** is the only blockchain that records transactions made with the ***bitcoin*** currency.

*What are **bitcoins** made of?*

- Nothing that can be physically touched, such as a banknote or dollar bill.
- They are just strings of numbers and digital letters.
- A unique identity (just as your fingerprint gives you a unique identity).







The Blockchain is a secure transaction record because it is distributed among the members of a network.

Each transaction is permanently recorded for everyone and thus no movements can be hidden.

Data is stored in encrypted blocks that are connected sequentially or "chained" together, making it difficult to modify the information without the consent of the entire network.

Its features make it a technology that could make processes such as government spending and even elections more transparent.

*Is **Bitcoin** anonymous?*

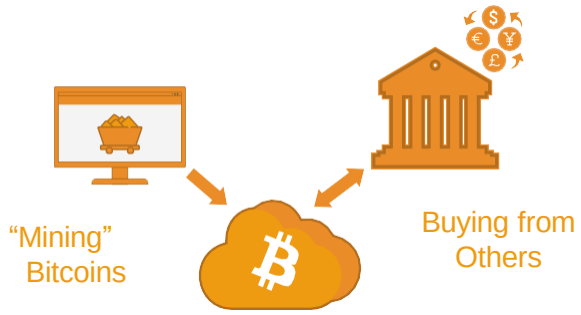
- No, it is pseudonymous. Transactions are visible, accessible, and transparent to everyone.
- People are identified not by first and last name, but by strings of letters and numbers.

*Who can use **Bitcoin**?*

- Unlike the traditional banking system, anyone with access to the internet can use Bitcoin.

*How can I get **bitcoin**?*

- It is purchased online through platforms called *exchanges*.
- New bitcoins are created through a process called mining (also known as proof-of-work).



*What are the barriers to **Bitcoin**?*

- Internet access is required for bitcoin transactions.
- Some countries prohibit entries, but it is impossible to prohibit exchange.

*Where are **bitcoins** stored?*

- In a wallet which we can access with our private keys, or in an exchange.

How can a currency that does not exist in the physical world and that is not supported by anything, or by anyone, have value?

- Value grows with user confidence, scarcity, utility, level of demand, and other factors.

*Is **Bitcoin** safe?*

- The goal of mining is to discourage bad actors and hinder unwanted behaviors such as double spending and spam.
- Cryptography protects information in a very secure way. It uses:
  - **Public keys** (similar to a bank account number, but unique in each transaction).
  - **Private keys** (similar to a secret PIN belonging to that bank account).

Who and what ensures that transactions are executed without failure?

- Miners and mining.
- The objective is to discourage bad actors and hinder unwanted behavior.

*What are some of the advantages of **bitcoin** over fiat?*

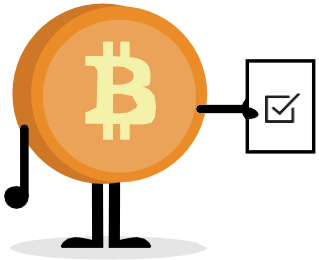
- The price of bitcoin is the same in all countries of the world.
- There are no borders.
- Its inflation is controlled and its emission is predefined.
- Governments have no decision-making power over its governance.

4.3 Differences between Bitcoin and Fiat

	Bitcoin	Fiat
Tangibility	It is a virtual currency and can only be used digitally.	It can be used both physically (coins and bills) and digitally (i.e. checks, apps).
Regulation	It is created through mining and is controlled by a distributed and decentralized system of computers.	It is created and controlled by a central government and/or central bank. It is the legal tender in the country whose government authorizes its creation.
Governance	A voluntary consensus mechanism and requires high levels of agreement.	Governed by the central government.
Value	Backed by user trust. The more users, the more stable it will become.	Determined by supply and demand and vulnerable to inflation.
Offer	Limited to 21 million.	There is no upper limit.
Transaction Validation	Through cryptography and the use of blockchain technology.	Through a bank or a broker.
Transactio n Costs	Minimal.	Significant, since there are intermediaries.
Time and Speed of Transactions	Ten minutes, on average (in Bitcoin), and instant (on the Lightning Network).	Instant (in cash), days or even months (bank transactions).
Security	Cryptography (branch of mathematics). Prevents a 51% attack.	Internal security of banks, and can be negatively affected by fluctuations in government policies.
Changes	Bitcoin transactions cannot be reversed, changed or cancelled.	It is common for there to be disputes in transactions, and changes or reversals.

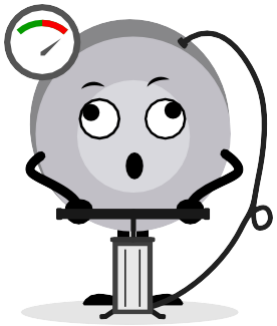
Bitcoin vs. Fiat

Controlled inflation, predictable and predefined amount in circulation.

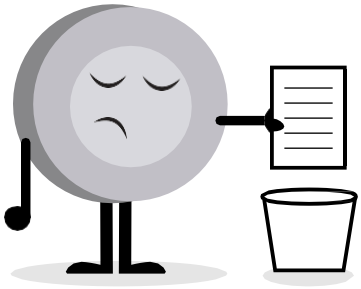


Changes can only be applied if users accept them.

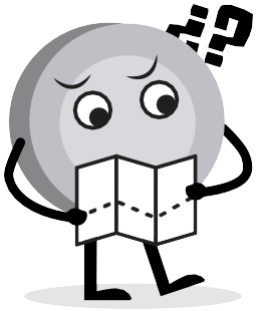
There are no borders, it can be accepted by anyone, in any place, in the world.



Inflation at record levels and can be devalued by printing as many bills as an issuer chooses.



It changes at the discretion of leaders, without consulting the citizens.



It is only accepted within the issuing country and cannot be used outside the country.

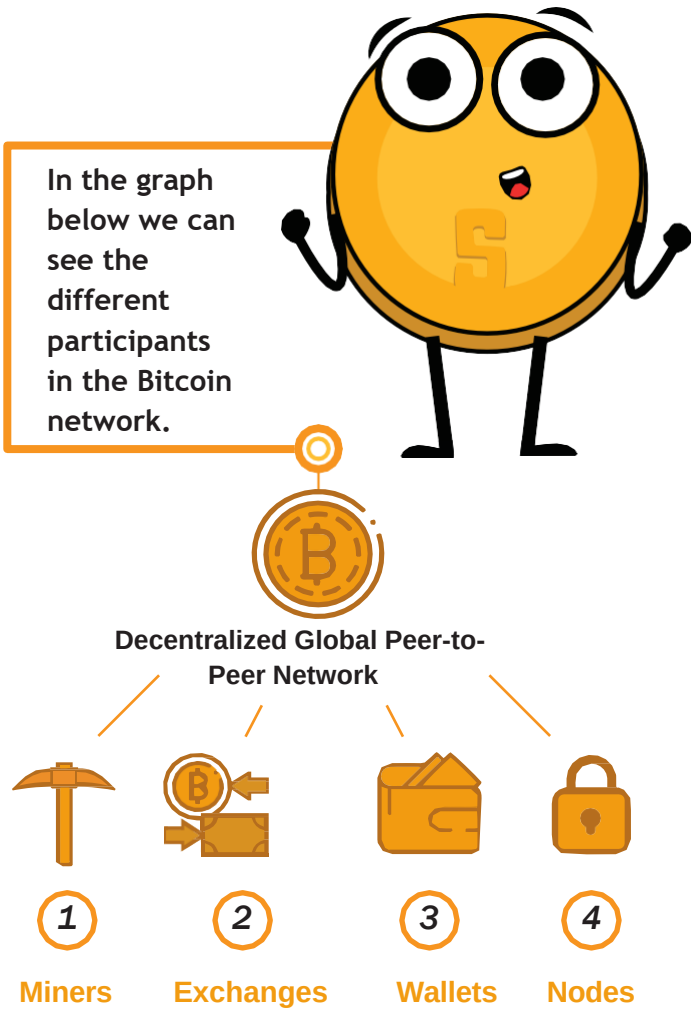
Practical Exercise. Finish completing the exercise for Class #1, on page 16. In the 'Bitcoin' column, mark a box with an X if Bitcoin meets the indicated characteristic. *Which item would you choose as money?*

4.4 Bitcoin Participants

To understand how someone or a system participates in the **Bitcoin** network, we must ask ourselves:

- *Can this person or computer only see the transactions in which it participates?*
- *Do they have access to more information?*
- *What are the transactions they can make?*
- *What permissions do they have over the network?*
- *How do they interact with the network?*
- *Do they have Access to a copy of the entire chain?*

In the graph below we can see the different participants in the Bitcoin network.



- **1. Miners**. Specialized computer equipment:
  - They compete in solving mathematical puzzles with each other to create new ***bitcoins***.
  - They confirm transactions and maintain the security of the network.
    - Similar to employees in a bank, they are paid for the work they perform.

- **2.Exchanges.** They exchange fiat coins for ***bitcoin*** and other cryptocurrencies.
  - They offer a way to get in and out of the market for those who are not miners.
  - Similar to banks, they offer services to users.

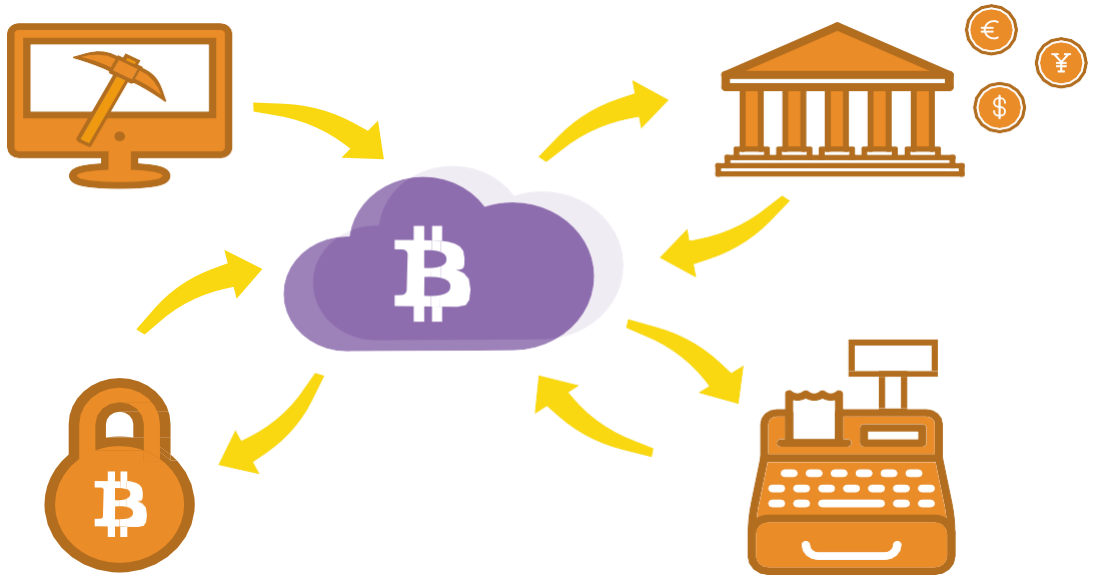
- **3.Wallets**. Applications used to store, send, and receive ***bitcoin***.
  - This is similar to bank accounts or apps used to transfer money online.

- **4.Nodes.** Devices connected to a digital network that validate, transmit, process, and store BTC transactions (in addition to being wallets, they have many other functions).
  - They consist of two things: hardware and software.
    - Similar to a mobile phone and an app.
    - Hardware is the physical material necessary to run the software.

- **5. Developers.** They maintain and propose improvements to the code.

Miners create ***bitcoins*** using specialized computers to solve mathematical functions. The same process also verifies previous transactions.

Exchanges do the conversions between conventional currencies and ***bitcoin***, offering a way for non-miners to enter the market, as well as a way to withdraw money.



Users download a **wallet** that functions like an email address, providing a way to store and receive currency. ***Bitcoins*** can be transferred from one wallet to another using a web browser or smartphone app.

Businesses create a **wallet** in the same way as an individual user, typically by using a website button to enable a ***bitcoin*** payment. For companies with a physical establishment, QR codes can be used to allow customers to pay quickly and easily.

Class #5

Buying, Taking Custody, and Transacting in Bitcoin

1. On-Ramps and Off-Ramps
   - Do I have enough money to buy bitcoin?
2. Taking Custody of Bitcoin
   - Types of Wallets and the Lightning Network
   - How do I send or receive satoshis?
3. The Transaction Cycle (on-chain)
   - What is a Bitcoin transaction?
   - Bridges and Stops for Transactions
   - How does a transaction work, step-by-step?
   - UTXO - “Unspent Transactions”
   - Confirming a Transaction

Buying, Taking Custody, and Transacting in Bitcoin

5.1 On-Ramps and Off-Ramps

- The first step in obtaining ***bitcoin*** is to buy it. There are several options:
  - *Exchanges, brokers, ATM's, fintech companies, gift cards, P2P, etc.*

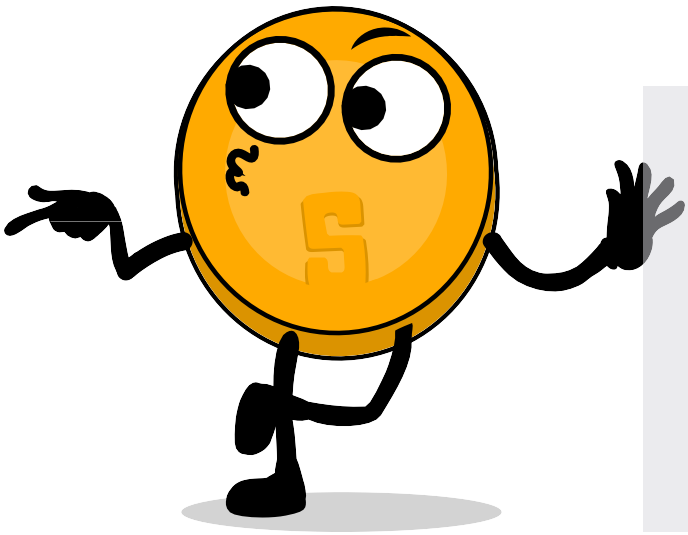
- Conventional money (euros, dollars, etc.) is exchanged for its equivalent in ***bitcoin***.

- The services that provide these functions are called "***access ramps***".

- Governments can regulate on- and off-ramps.
  - They can prohibit banks from sending money to/from a ***bitcoins*** exchange.
    - Which would affect our ability to buy and sell ***bitcoins***, *but, it would be impossible to prevent sending/receiving* ***bitcoin***.

Do I have enough money to buy bitcoin?

- **BTC** is the common unit of the ***bitcoin*** currency.



- The symbol ₿ can be used to refer to ***bitcoin***, the same as (**USD**) or **$** is used for the US dollar.

- ***Bitcoin*** maintains an equivalent value against all the currencies in the world at any given time.
  - For example, at of this writing:

  1 ₿ = US$21,464 or 1 ₿= $95,288,229 COP (Columbian Pesos)

- ***Bitcoin*** is much more divisible than $1, as $1=100 cents. There is no such thing as a ½ cent or 1/10 of a cent.

- A ***Satoshi*** (or ***Sat*** for short), is the lowest denomination of the ***bitcoin*** currency.
  - 1 BTC = 100,000,000 sats ≈ 0.0003 USD
  - This means that one ***bitcoin*** can be divided into one hundred million units.

- ***Unity Bias:*** False belief...
  - You don't have to buy 1 whole ***bitcoin***. Instead, you can buy as many *Sats* as you want.

'If you add a little to a little, and then do it again, soon that little shall be much."

- Hesíod

Satoshi	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

5.2 Taking Custody of Bitcoin

*How do you custody **bitcoin**?*

- When Sats are purchased on a website, they will most likely be credited to a virtual wallet.
  - •It's similar to receiving a credit on a bank account when money is transferred to it.

- It may seem the case that the person owns his bitcoin, but in reality the money is in the possession of a third party.

- Therefore, it is important to understand the risks of investing in bitcoin and start by:
  - •Knowing the best ways to keep custody of your bitcoin.
  - • Discover what a wallet is.
    - *- Which one offers the best security.*
    - *-How to choose the one the best suits your needs.*
  - •Analyzing the trade-offs of the wallets you can select..
    - *-Understand that there is no ideal wallet that satisfies all needs*

Types of Wallets and the Lightning Network

*Who controls my **bitcoin**?*

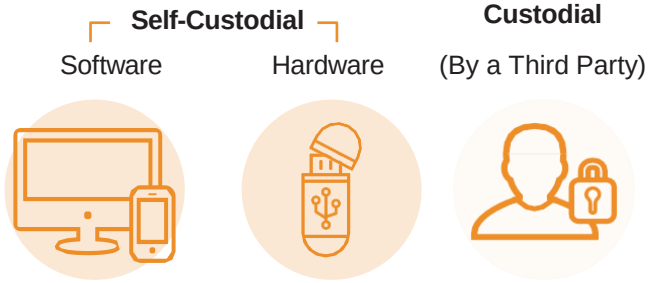
Self-Custodial Wallets

- *Benefits:*
  - -It is the only way to have full control over the bitcoin you have purchased.
  - -No outside permission required to send/receive.
  - -There is no approval process for an account.
  - -Anyone in the world can download a wallet and use it immediately.
  - - It's like having the money locked up in home instead of entrusting it to a bank.
  - -Self-custody of your bitcoin is highly recommended to avoid hacks/theft.
  - -No company/government has control/authority over transactions.
  - –No third party may arbitrarily confiscate bitcoin in self–custody.
  - -In times of stress, we are assured that our bitcoin is safe.
- *Risks:*
  - -There is no way to recover the funds in a loss of private keys.
  - - There is less access (no) customer service.
  - - Responsibility is on the individual and not distributed.

Custodial Wallets

- A third party stores your bitcoin.
- •The funds (private keys) are under the control of the provider.

- *Benefits:*
  - - If you lose or forget access to your account, the money may be recovered.
  - - Services/providers usually have some customer service.
- *Risks:*
  - - They are always connected to the internet, which makes them more vulnerable.
  - - Not your keys, not your coins.



Buying, Taking Custody, and Transacting in Bitcoin

What is the most convenient wallet?

- **Hardware Wallets [Cold]**
  - •Could be understood as "non-connected" wallets, since they do not require the internet to operate.
  - •They are the most secure wallets in existence.
  - •Ideal for storing large amounts of ***bitcoin***.
  - • Your keys are stored on a disk and can be used directly from the hardware. [ex: Coldcard MK3.]
  - •Losing the wallet without backing it up results in unrecoverable funds.

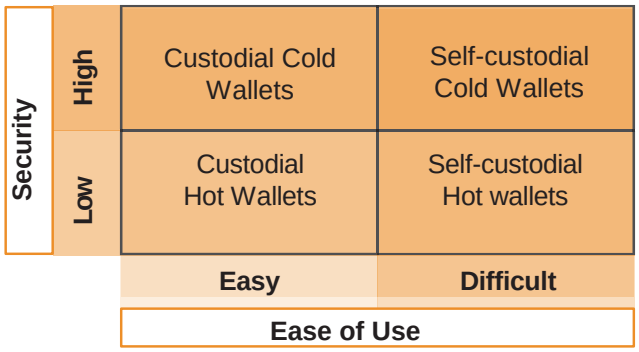
- **Paper Wallets [Cold]**
  - •Private keys are copied onto paper to protect them (keep them offline).
  - •One of the most secure, but extremely inefficient ways to store ***bitcoin***.
  - •A new private key must be copied each time a transaction is performed.

- **Software Wallets [Hot]**
  - • Connected to the internet.
  - •Can be installed and/or accessed through a mobile application or via the web.

  - **Mobile Wallets**
    - •Portable and convenient; ideal when doing face-to-face transactions.
    - •The app stores may remove them without notice.
    - •If your mobile device is damaged or lost, it may be difficult to recover funds.
    - - Ideal for use with QR codes.

  - **Desktop Wallets**
    - •Users can have complete control over the funds.
    - •Some offer support for cold wallets.
    - •It's difficult to use QR codes when making transactions.
    - •Susceptible to viruses that steal ***bitcoins***.

Bitcoin Wallet Architecture



How do I send or receive satoshis?

- **On-chain**:
  - •Through wallets connected to the "main" network.
  - •This is a very secure, but slow way – it takes 10 minutes, on average, to confirm the transaction.
  - •The commissions for each transaction are proportional to its digital size, not to the amount being sent.
    - -If you send a value of $1 USD on-chain, and $1 is paid in fees, this represents 100% of your transaction cost.
    - -If you send $10,000 USD on-chain, and $1 is paid in fees, this represents 0.01% of your total transaction cost.

- **Lightning Network** (***off-chain***):
  - •A "layer 2" solution – built on top of the "base layer" of ***bitcoin***.
    - *- It allows for nearly instant transactions with very low fees.*
  - • It is used in countries where there are:
    - *-Policies and regulations that encourage mass adoption of the Bitcoin network.*
    - *-Needs for fast, private, economic and efficient payment solutions.*

5.3 The Transaction Cycle (on-chain)

What is a Bitcoin transaction?

What is sent and stored through the **Bitcoin** protocol is ***bitcoin***, not pesos or dollars.

- This transfer of money is called a transaction.

- A transfer of value between two wallets, which is recorded on the blockchain (**Bitcoin**).

When a new transaction enters the network:

- It must pass a verification process to be accepted by the nodes.
  - • Valid transactions*:*
    - -Are transmitted from one computer to another until they all have a copy of the updated ledger.
    - -Approximately every ten minutes, thousands of transactions are bundled to be processed all at once.
    - -A new block is created through a process called mining.
    - -New transactions are recorded on the blockchain forever, within a single block.
    - –Once recorded, it is impossible to modify them, delete them, or add information to them.
  - • Invalid transactions*:*
    - - They are simply rejected and do not propagate through the network.

Bridges and stops to perform transactions and saving BTC

A transaction through a wallet is similar to the following process:

- Let's imagine that all the bitcoin in existence were stored in safety deposit boxes.
  - •Each one had a different amount of BTC, but it was completely transparent which box had how much.
  - •Anyone could see how much bitcoin is in each box and the history of how it got there.
- Each box has an address belonging to only one owner.

- This address is protected with a security lock, which then requires two different keys:
  - • One of the keys, the private key, unlocks the lock and gives access to the BTC inside.
  - •The other key, the public key, closes the lock and protects the BTC.

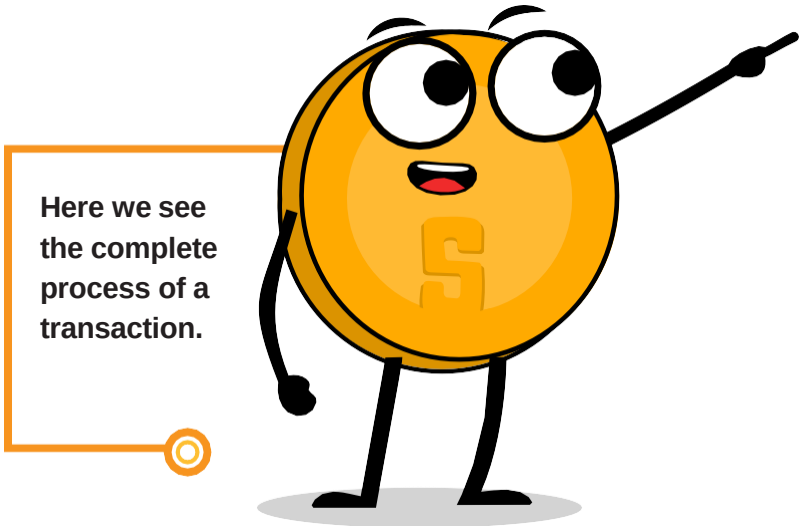
- Each participant in the network keeps his or her private keys in very secure locations.

Buying, Taking Custody, and Transacting in Bitcoin

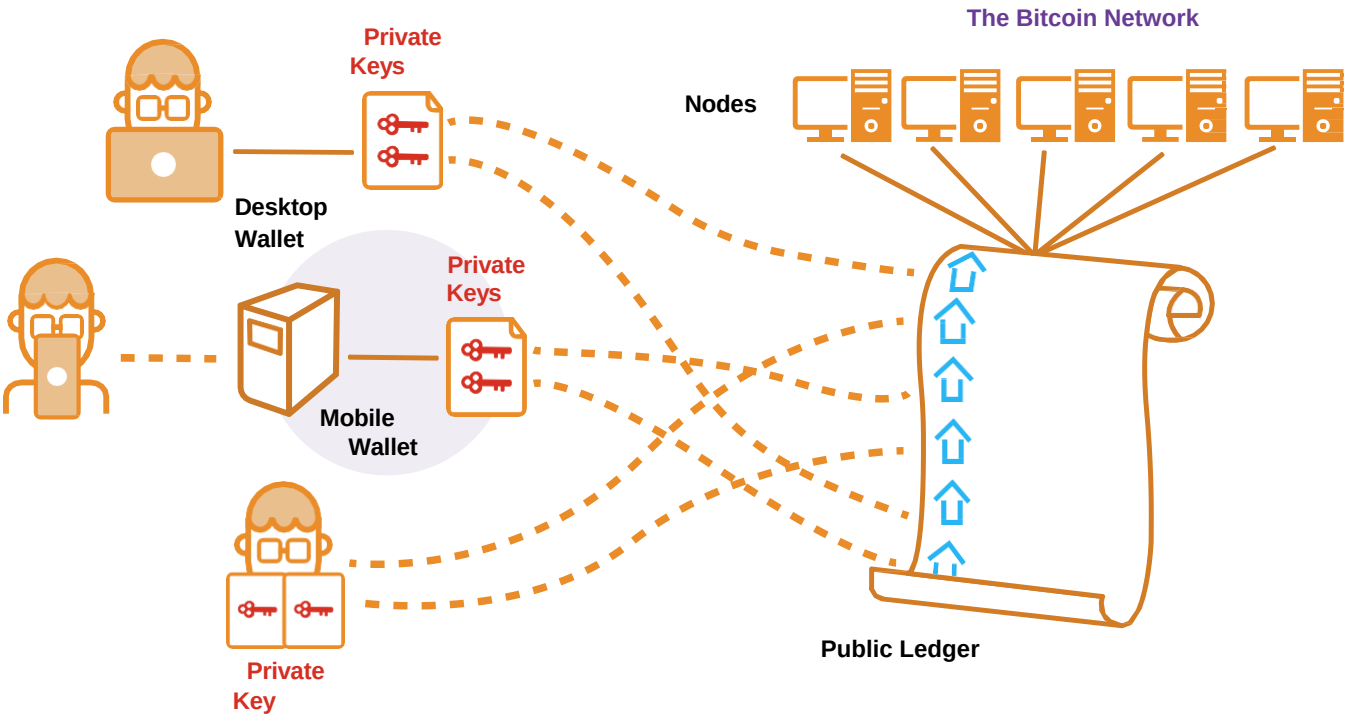
- If you are the owner of a box in which bitcoin is held, you can at any time:
  - •Transfer any desired amount of funds to a different box.
  - • First taking into account there are thousands and thousands of boxes:
    - -You need an exact address, to ensure that the BTC will be deposited in the correct box.
  - •Finally, the safe lock must be closed with the public key of the box.
    - - So that no one, outside of the addressee, has access to the bitcoin.
- In the future, the box can only be opened with the private key of the person who received the BTC.

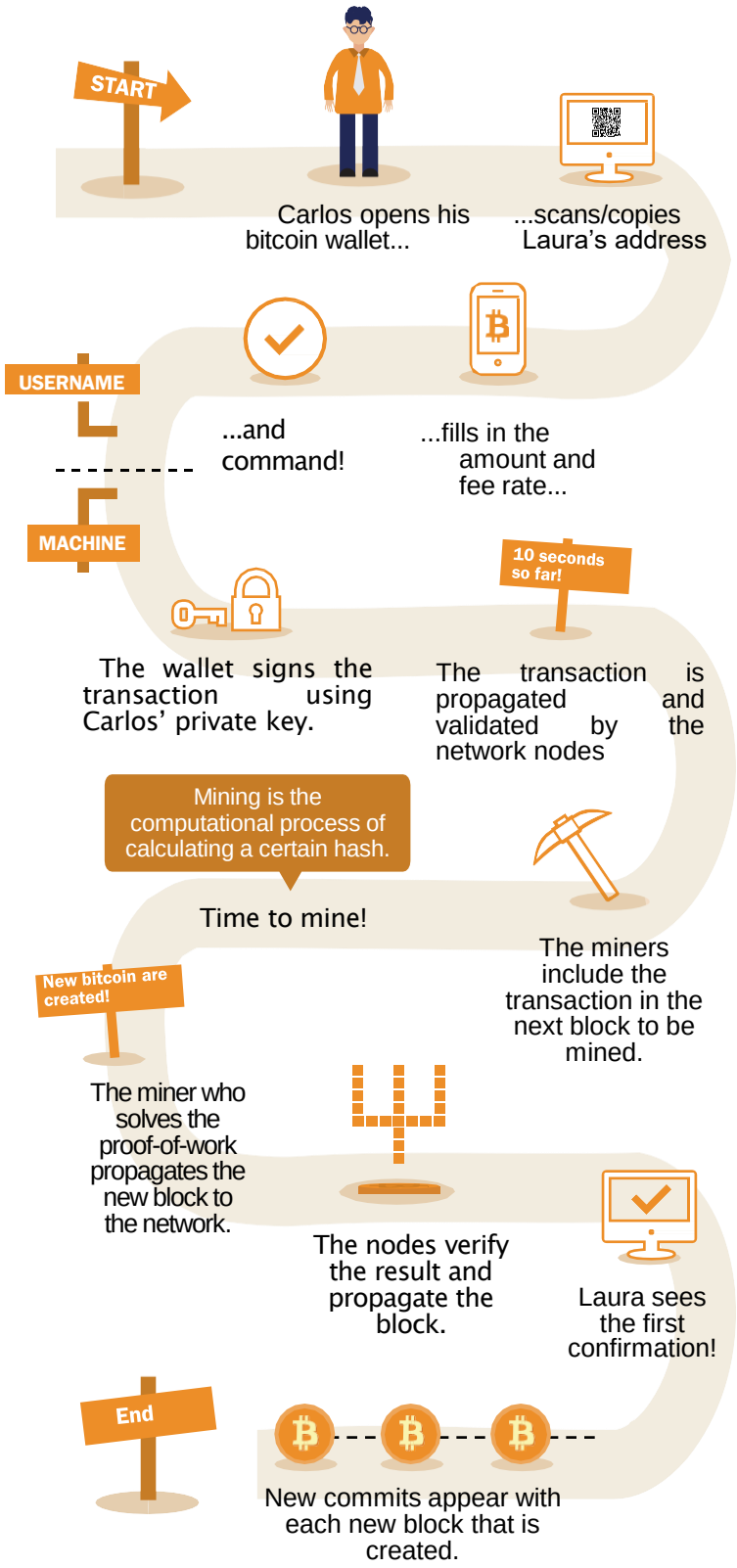
How does a transaction work, step-by-step?

The success of transferring money in a decentralized network was only achieved under the premise that each transaction is unique and recognizable.



Here we see the complete process of a transaction.





- Suppose Carlos is going to send 0.5 bitcoin to his sister Laura. They both have wallets.

•It is necessary to create a transaction that carries a ***unique and unrepeatable identifier***.

- The identifier is the fingerprint of each transaction.

-This is to prevent two transactions from appearing to be identical.

- This also makes the process of verification simple.

- For this to happen securely but efficiently, each transaction needs to be encrypted, decrypted, signed, and verified.

- **Encryption:** Carlos has to send the ***bitcoin*** through a secure channel without being intercepted by anyone.

- **Decipher**: Laura has to receive the money, making sure no one else can access and use it.

- **Signing**: Carlos has to prove to Laura that the money he sent did belong to him originally and that he is sending the correct amount.

- **Verify**: Users in the network have to verify that Carlos did have that money in his account to spend, they have to deduct it from Carlos' total account, and they have to add it to Laura's account. .

Let's see how it happens:

1. Carlos opens his wallet on his cell phone and asks Laura for the public key.
2. Laura shares it (*in the form of a QR code, email, or some other method).*

- 3. In this transaction, Carlos scans the QR code and links it to the amount he will send.
  - •He adds a small fee as an incentive for miners to select his transaction for the next block.
- 4. One click verifies whether Carlos has sufficient funds in his wallet.
- 5. Carlos' wallet signs the transaction with his private key.
  - •His *bitcoin* becomes available to Laura.
- 6. The transaction is transmitted through the network to the nodes to be approved.
  - • After being verified, it remains in a waiting area.
- 7. Mining nodes select thousands of transactions and reject invalid ones.
  - •Valid transactions are added to "candidate blocks," which have not yet been accepted.
  - • They consolidate all the information and each one creates a block identifier.
- 8. A competition between mining nodes (similar to a raffle between block identifiers) begins:
  - •To see who is next to add their block to the blockchain.
- 9. The winning block contains the Carlos-Laura transaction and propagates it to other nodes.
- 10. The nodes verify the identifier of the winning block and add it to the blockchain.
  - •All transactions on the blockchain are confirmed on the blockchain.
  - • There will be no way to modify or delete it; it will be permanently recorded.
- 11. Laura becomes the accredited owner of that *bitcoin*.
  - •She will have received her 0.5 BTC in about 10 minutes of less.
  - •Carlos will see it subtracted from his wallet balance.
- 12. The transaction will be successfully completed.

UTXO - "Unspent Transaction Outputs"

Transactions are simply inputs and outputs of *bitcoin* from one wallet to another.

- Any bitcoin that has not yet been spent is considered a UTXO, or an unspent transaction output. So, a UTXO is simply unspent bitcoin.
- This can also be understood as: the current state of the blockchain is the UTXO database.
- The inputs refer to the money that is used to generate a transaction.
- Outputs generally indicate two points to which the transaction is directed:
  - •An output goes to the person to whom the payment is made.
- When a user unlocks his UTXO with his private key to send to another user,
  - •Their balance may be at risk because their safe deposit box is open.
  - •For this reason, it is always advisable to send any balance to a new wallet.

- If the original wallet has a balance:
  - •The other output goes to a new address created to receive the change.
    - Converting this amount into a new ***UTXO***.

- For the nodes in the network, it is easy to arrive at a consensus since:
  - •Everyone keeps a copy of the same database.
  - •You can check the balances of each of the addresses.

Confirmation of a Transaction

- To authorize and send any output from a bitcoin wallet,
  - • The transaction must be signed with the private key.
  - •This step is necessary to prove that you own your own funds.

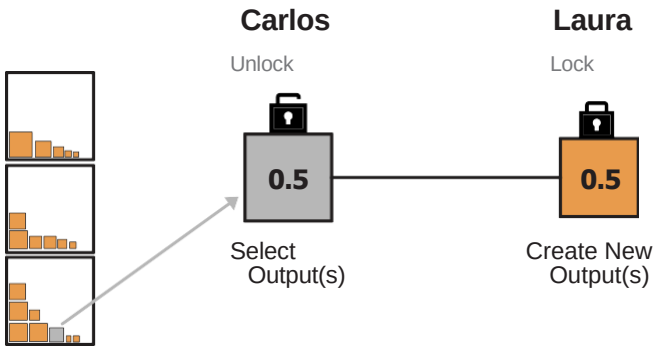
- To receive an input sent to a wallet:
  - • A user must have shared their address with the sender.

- The transfer is CONFIRMED when:
  - •**Bitcoin** ***has noted the amount of*** ***bitcoin*** deposited to the new address.
  - • And it has been subtracted from the wallet of the one who sent it.

Let's see how a transaction is confirmed:

- The yellow boxes represent UTXO

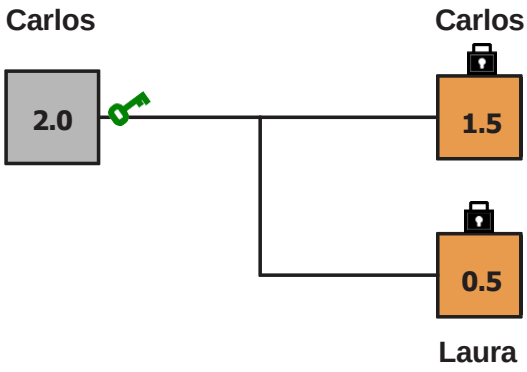
- The gray boxes represent wallets in which there is no more bitcoin (completely empty)



•The node confirms that there was enough bitcoin pointing to the original address (0.5 BTC in Carlos' wallet) to execute the transaction.

•When the transaction is confirmed, a certain amount of bitcoin has been distributed to two different addresses.

•Some boxes now have more bitcoin (Laura's), and the original box (Carlos') has less.



•After having confirmed the transfer, the blockchain will only monitor the wallets that received money, the 1.5 BTC wallet and the 0.5 BTC wallet.

- This is now the new state of unspent bitcoin, or UTXO – which is also the state of the blockchain!

Class #6

Bitcoin as a Store of Value and Payments Network

1. The Double Spend Problem
2. Memory Pool or the "Mempool"
3. Transactions Verified, but Not Confirmed
4. The Bitcoin Network (On-Chain)
   - Full Nodes
   - Activity: Seeing the Status of Transactions
5. "Lightning Network" (Off-Chain Transactions)
   - What is the difference between Layer 1 and Layer 2?
   - Activity: How Lightning Works

6.1 The Double Spend Problem

Before going into detail, let's consider the following:

- **Bitcoin is digital money.** This means that unlike conventional money it:
  - Cannot be duplicated as other types of digital files can (photos, videos, etc).
  - Cannot be replicated, forged and/or sent to multiple persons simultaneously.
  - It cannot be billed as a 'double charge' as with a credit card.

What are the benefits of this feature of Bitcoin? Let's explain with an example.

- It is common for people to store their receipts and/or keep a record of their expenses.
  - Periodically, people compare their accounts with their bank balances to verify that there are no discrepancies.

- For example, someone may realize that a restaurant charged their credit card twice:
  - There are two $5.08 withdrawals on Wednesday, January 26, 2022.
  - You realize you have been double billed for the same lunch.
  - You probably call the bank to reverse one of the payments.
  - In the best case, if the bank accepts your dispute, you will get your money back in a few months.
  - In the worst case, the restaurant refuses to refund the money on the grounds that there were two purchases.

- Let's continue exploring day-to-day examples to illustrate the idea of the "double spend":

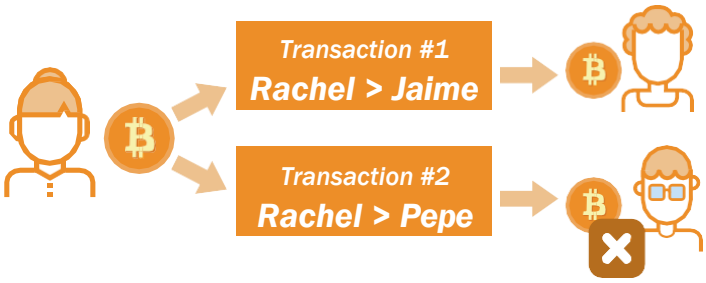
  - **Day #1: Let's say Rachel orders a lunch at McDonalds for $10 USD.**
    - *She pays in cash with two $5 bills.*
    - *Payment is confirmed instantly.*
    - *Both parties have witnessed the procedure physically.*
    - *It was a simple exchange – a hamburger was given in exchange for money..*

  - **Day #2: Rachel orders the same lunch and has two $5 bills again..**
    - *But one is original and one is fake (an exact copy). She uses both as payment.*
    - *Since the serial numbers are identical, the cashier can easily see that one is a fake.*
    - *Or simply accept payment as they did the day before.*
    - *Having a busy day, the cashier accepts the payment without taking time to study the bills.*

  - **Day #3: Rachel had a good experience, but is afraid to go back to McDonalds.**
    - *Now, she will try to duplicate her bitcoin, as she replicated her cash at McDonalds.*
    - *She owes 0.2 BTC to both Jaime and Pepe, but only has 0.2 BTC in her wallet.*
    - *Rachel opens her wallet on her phone and on her moms phone with her seed phrase.*
    - *From her personal phone, she sends 0.2 BTC to Jaime.*
    - *From her mom's phone, she sends 0.2 BTC to Pepe.*
    - *She makes sure to send the two transactions at exactly the same time.*

○*Two different nodes receive the transactions.*

○*Let's remember that Rachel only had 0.2 BTC in her wallet to spend.*



- The network nodes take notice, and one of the two transactions is rejected!

- But how? If we have a system in which no computer is in charge, how do we decide which transaction is rejected and which is left unchanged on the blockchain?

- To achieve this, Satoshi Nakamoto managed to find a successful mechanism that:
  - •Checks if a transaction is valid or not, in a consensual way among all the participants in the network, before adding it to the blockchain.
  - •An ingenious solution to problems like those mentioned above.

How does it work?

6.2 Memory Group or "Mempool"

- Before any transaction can be executed and fixed in a block,
- It will enter a waiting area called a "***mempool***", or memory group.

What is it and what happens to the transactions in the mempool?

- The mempool is an organized que where transactions are stored and sorted before being added to a newly created block.
- There is no global mempool; each node must:
  - Verify the validity of the transactions before including them in their ***mempool***.
  - Propagate verified transactions to neighboring nodes.
  - Reject invalid transactions.

Here you can see how quickly the valid transactions are dispersed from node to node.

- Nodes must decide whether transactions are valid or not.
  - If accepted:
    - -They wait for a miner to select it and add it to the next block.
    - -Eventually they are permanently saved in the shared database.
  - Otherwise, they can be rejected if: :
    - – There is a conflict with another transaction.
    - – If there are insufficient funds to transfer..
    - –If the signature is not valid and you cannot verify that said BTC can be spent.

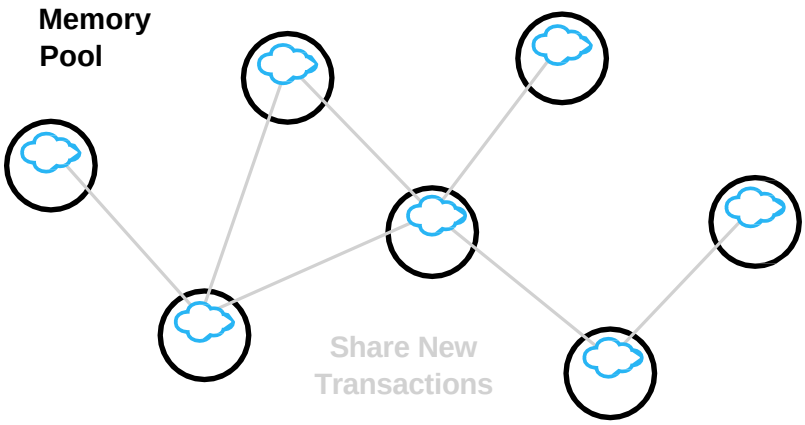
•Some transactions sit in the waiting area if they do not add a sufficiently attractive monetary incentive for miners.

- If a transaction remains unconfirmed for over 72 hours, they are rejected.

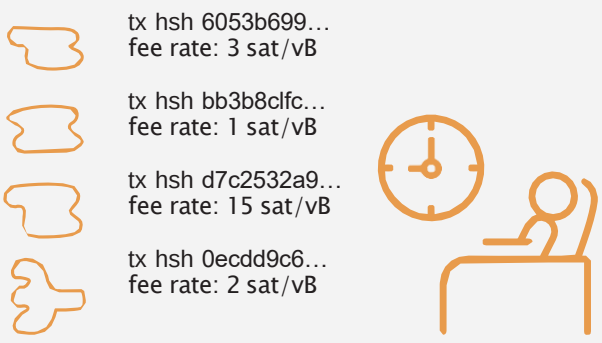
● The mempool provides an additional layer of security and resistance against DDoS attacks..

•DDoS attacks happen when a network is flooded with tiny transactions.

- Causing unmanageable congestion.



A *mempool* is where transactions wait to be confirmed in a block.



When a node first receives a transaction from a peer, it must verify that the transaction is legitimate. No one wants flawed or misleading transactions.

The main purpose of the *mempool is*:

1 Transmitting unconfirmed transactions.

2 Provide miners with transactions so they can mine.

6.3 Activity: Transactions Verified, but Not Confirmed

Class Activity. Follow the teacher's instructions for this activity. Follow the link of the QR code to start.

- Below we can see a real unconfirmed transaction:
  - A unique identifier (*the fingerprint of the transaction*).
  - The memory space it occupies.
  - The commission that is paid.
  - The amount of the transfer.

TxID: **a434948b2de9de18398294f84e42436ec59fb86faf34a21052bd640a97cd94b7d**

_____ input ➡ _____ outputs

Size: _____ vbytes *(Memory space it occupies)*

Fee Rate: 27.01 sats/vbyte *(Commission rate/ current vbyte)*

Fee:_____ sats *(Transaction fee)*

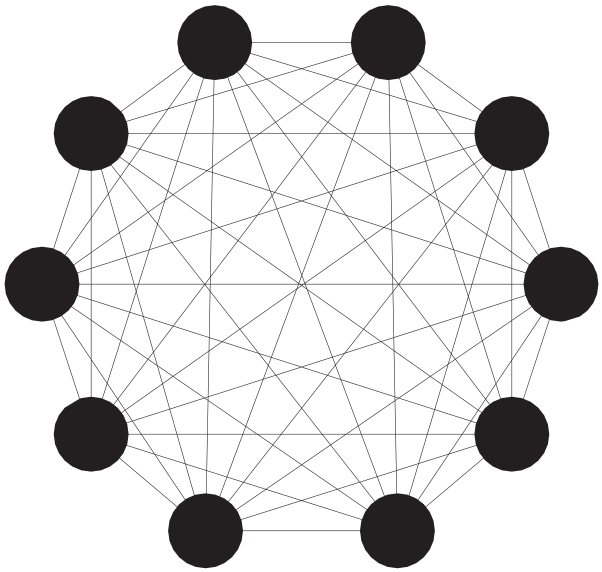
Total Value₿ _____ BTC ≈ $ _____ USD *(Total transaction value)*

- *Could we analyze one or more other transactoins?*
  - Is it more or less?
  - Did participants pay a higher or lower commission?
  - Which transaction will be most likely to be found in the next block? Why?
  - What will it mean when a block falls into the abyss?
  - What does it mean when a transaction is confirmed?

6.4 The Bitcoin Network (On-Chain)

- It is composed of **Bitcoin** nodes.
  - •It's made up of computers that adhere to a system of rules (software known as *Bitcoin Core*).
    - -Nodes communicate with each other through cyberspace as a network.
    - -Each one runs its own version of the **Bitcoin** software.

The Bitcoin Network
Nodes connected following a common set of rules.

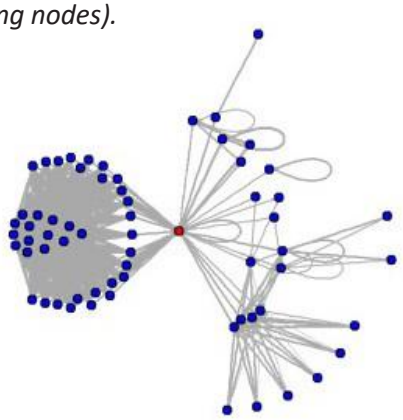


- Information (i.e. transactions) can be created, sent, and received from these connection points.
  - •There are different types of nodes, with each having a different role in the network.

Full Nodes

- They run the **Bitcoin** software.
  - •They have autonomy to make their own decisions, however, through consensus:
    - -They make the same decisions,, making them a reliable and secure decentralized network.
    - - The full nodes have three different functions:

1. Information sharing *(to its neighboring nodes).*



This diagram represents the propagation of a transaction.

- There are two types of transactions that nodes share:

— A. New Transactions

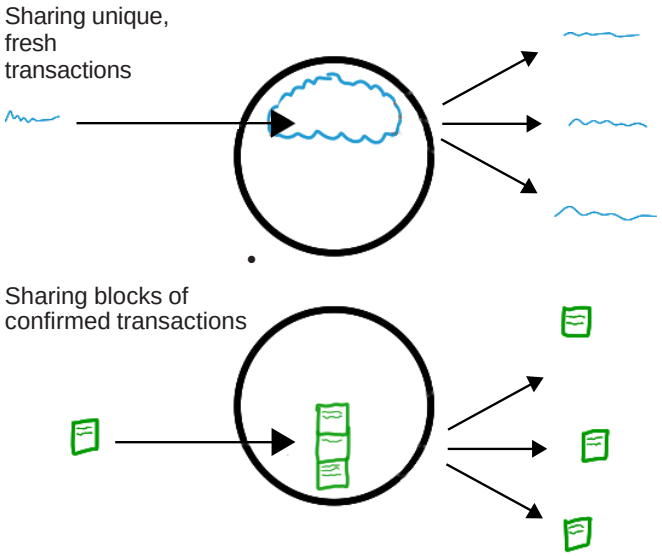
- These go directly to the *mempool*.
- –The nodes are in charge of verifying or rejecting these transactions.
  - -They are based on the history of the blockchain and the rule set of the software.

-They relay valid transactions to their neighboring nodes.

- -No one wants to receive faulty or malicious transactions.

— **B. Confirmed Transactions**

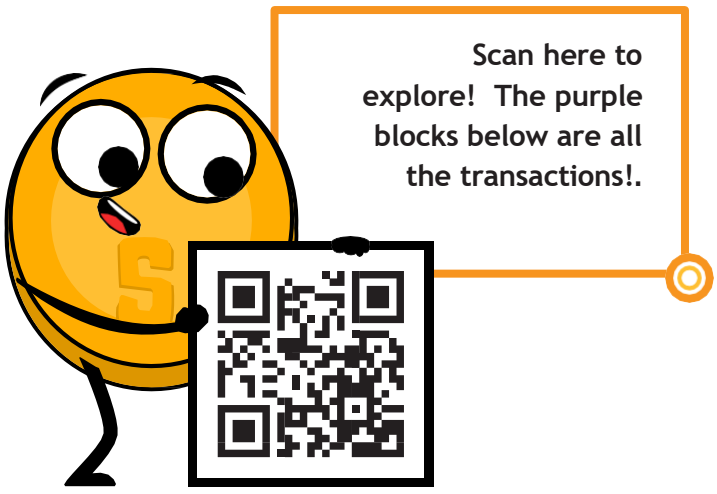
- Transactions that have been "confirmed" and written in a block.
-These are grouped together and form blocks; they are not shared individually.



2. Saving a copy of confirmed transactions.

•They keep a complete copy of all the blocks in the block chain,

•Each confirmation exponentially reduces the risk of the transaction being reversed.



3.Validate the blocks and reach a consensus with the other nodes.

•All participating nodes must unanimously agree to the information contained in an entire block before including it in the blockchain.

• A copy of the blockchain for safekeeping and sharing with other nodes.

- The status of your new and confirmed transactions signed can be located on the internet. How?

•Block explorers are a window into all blockchain transactions.

•They allow you to check the balance of each address, view the details of each transaction, and more.

Activity: Transaction Status

Class Activity. We go to the following link where we can observe different properties of the transactions.

https://www.blockchain.com/explorer?view=btc

Finish answering the questions on the next page.

On blockchain.com, we can locate and identify all of the following:

- The total amount that is transmitted.
- How many inputs and outputs are there?
-The size (or the memory it occupies in the block*).*
- The ID of a random transaction.
- The status of the transaction.
–If the transaction has already been confirmed, it shows the total number of confirmations so far.

What information do you recognize? Which one surprises you? What is the value of the last transaction? Can we see if it is already confirmed*?*

- Not all users have enough space on their hard drive to run a full node.
•If that is the case, you can simply download a wallet and make transfers or save BTC for the long term.

6.5 "Lightning Network" (Off-Chain)

What is the difference between Layer 1 (base layer) and Layer 2?

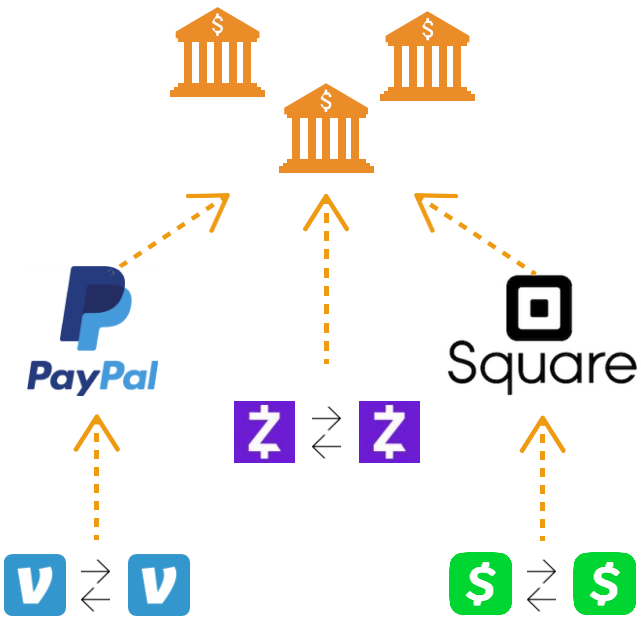
What do you do with a safe but congested road? Simple, you connect a new road to offload traffic. This is exactly the difference between Layer 1 and Layer 2 blockchain networks.

- Many important aspects of **Bitcoin** and even many transactions do not occur on the "blockchain".

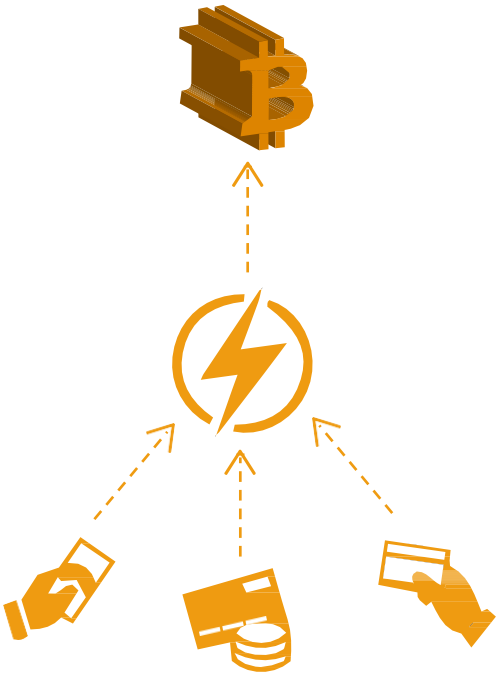
- **Bitcoin** is revolutionary as it is the base layer of the decentralized internet.
-But it has a fundamental scalability problem.
-Bitcoin transactions can be slow and expensive.
-It is argued that ***bitcoin*** Cannot be used as a means of payment because it is slow and expensive for micropayments.
-There are $1-$2 transactions that end up costing more than $5 to transact when using the main network.
-Visa processes up to 65,000 transactions per second (tps), while **Bitcoin** can only handle 7/tps.

- That's where the magic of layer 2 technologies, like lightning, come to the rescue.
-With the Lightning Network, bitcoin has the potential to be the currency of the digital age. Lightning makes bitcoin:
- Fast
- Immutable
- Decentralized

Modern Monetary System = Closed Networks
Banks maintain the finality.



Bitcoin Monetary System = Open Network
Bitcoin maintains finality.



All applications created in Lightning Network are interoperable.

- ***Lightning***, is a set of rules (*smart contracts*), built on top of **Bitcoin**:
  - That allows instant transactions
  - Can maintain high volumes of transactions.
  - That is disconnected from the main network.
  - It is not necessary to record all transactions on the network.
    - It is a more efficient alternate network.
    - Provides all of the security of **Bitcoin** without some of its drawbacks.
      - But with different types of compensation.
  - Offers more privacy than the base layer.
- ***Lightning*** addresses Bitcoin's scalability issues.
- Let's analyze the following analogy:

○A guest checks in to a hotel where they ask for your credit card in advance of the stay.
- -To cover room charges and incidental fees for the stay.

○It's more efficient and less expensive than charging the card every time you incur an expense.

○The hotel keeps a record of all customer expenses.

○There is an independent pharmacy and hairdresser within the hotel.
- -The guest buys products, uses services and signs the debt to his room.
- -The hotel charges a commission for intermediating the payment between the guest and the business.

○If the guest has a problem or a complaint, the necessary amount is deducted from his account.

○The card is only charged after the stay, when the guest and hotel have verified that the charges and balance are correct..

Bitcoin as a Store of Value and Payments Network

Lightning Network works similarly to the analogy, but differently. How so?

- The analogy is precise with the exclusion of the need for trust.
  - •This is a very common misunderstanding of ***Lightning***: *it is not a credit system.*
  - • Lightning transactions are not promissory notes:
    - They are valid **Bitcoin** transactions that move real UTXOs.
- Instead of giving someone a credit card and leaving an account open:

• Two nodes can open a payment channel, or a transfer route.

• The parties can carry out transactions as many times as they wish.

-Always keeping the balance updated.

• The larger a channel,

-The greater the amount of ***bitcoin*** that can be transferred along the channel.

•You can build routes with everyone you transact with.

• The more channels,

-The more connections and shorter paths to reach certain destinations.

• If there is a direct route,

-Everything is simple and a transaction is made according to the size of the channel.

•If the connection is through a third party (routing node),

- you pay a toll (fee) to pass.

•To open a new channel, both nodes pay a small fee to the miners.

• It is not necessary to update and verify every transaction on the network.

-This would be expensive and time consuming.

-On the contrary, each movement is approved with both digital signatures.

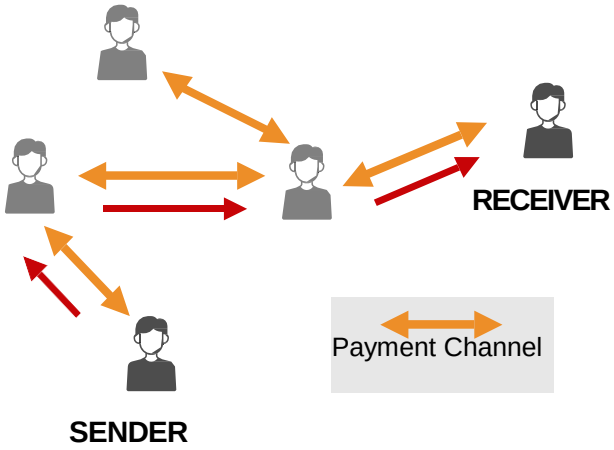
•When either party decides to close the channel,

-You unilaterally transmit the latest transaction to the **Bitcoin network.**

See a visualization at the following link:

https://lnrouter.app/graph/zero-base-fee

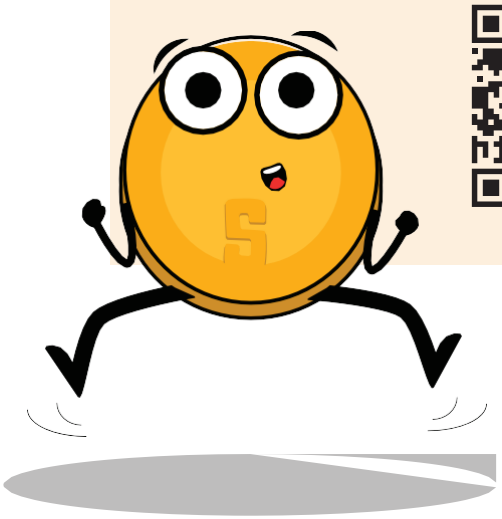
- If Alice has an open channel with Bob, and Bob has an open channel with Carl, Alice can send BTC to Carl via Bob, without needing to trust or know Bob.



Activity: How Lightning Works

Class Activity. Let's see a simulator. Wait for instructions from the teacher to complete this activity.

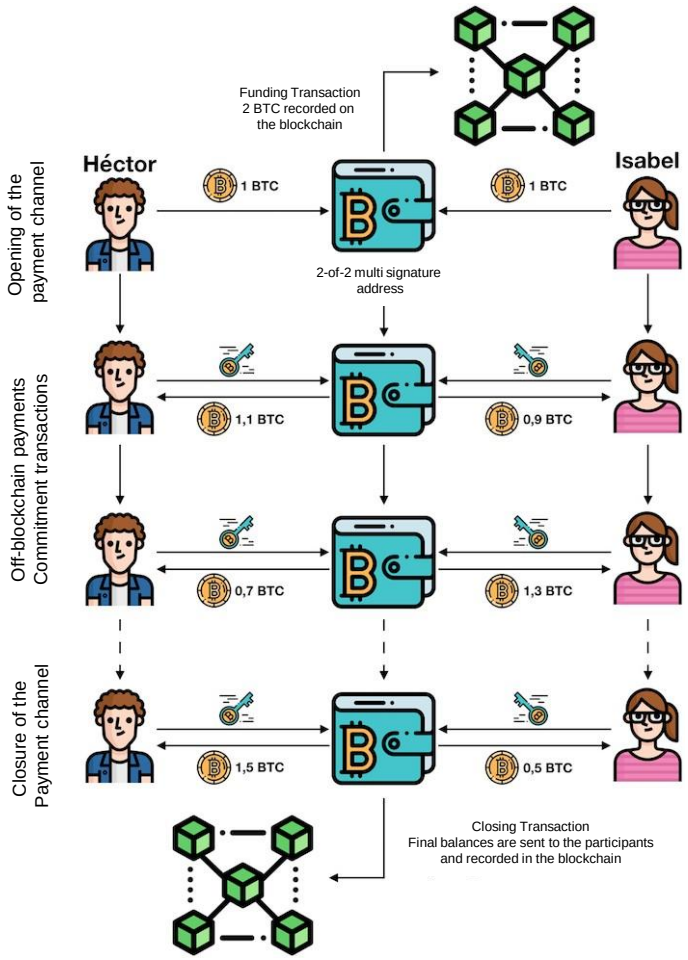
https://www.robtex.com/lnemulator.html?conf=A5-5B,B5-5C&send=A2C



- Using ***Lightning*** is as cheap and fast as sending an email.

  –With the added benefit of the secure and trustless nature of **Bitcoin**.

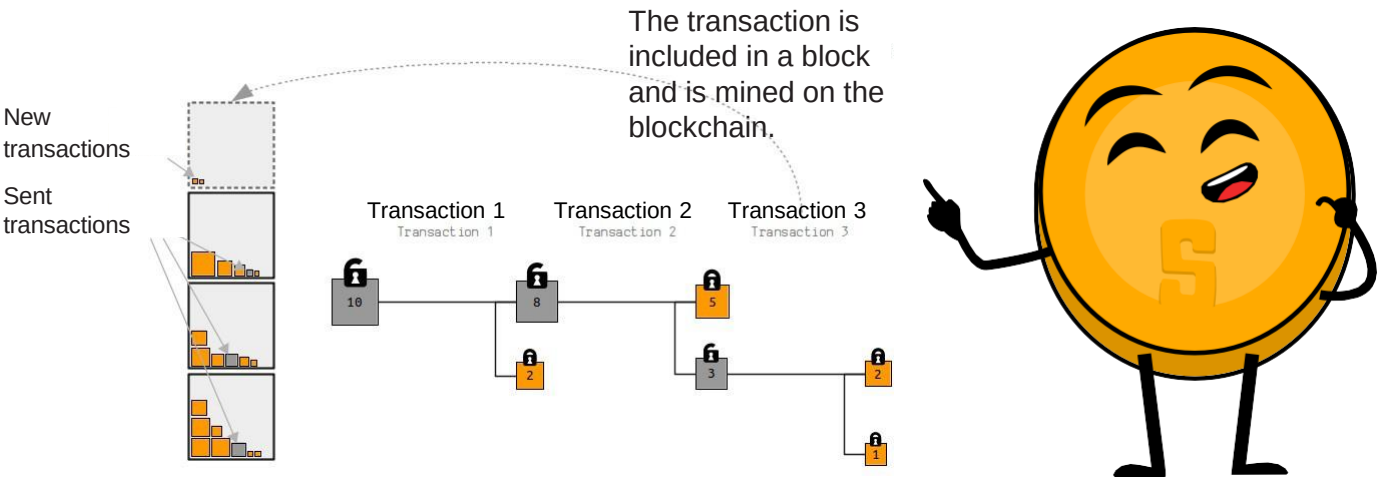
  -Only the two people holding money in an open channel know how much, how often, and when that money moves.



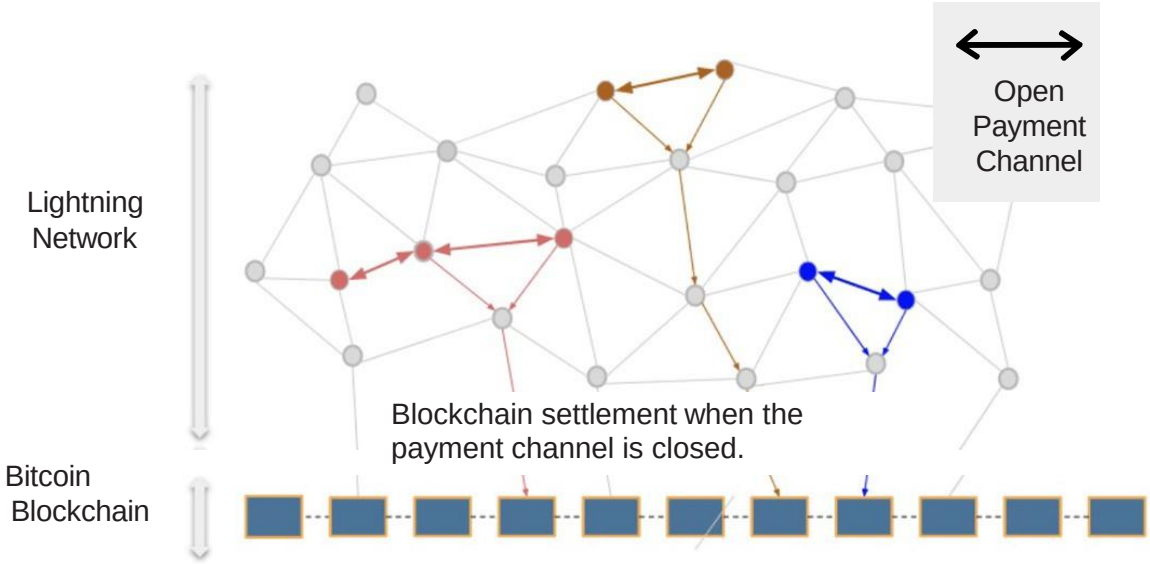
- In comparison, if three transactions are made "on-chain," that is, if they remain in the base layer:

  •Transactions would have been much slower and more expensive.

•Each of these transactions would have to involve all participants in the network.
• It could be displayed as follows:



How the Lightning Network works:



Class #7

Miners and Bitcoin Mining

1. Mining Nodes
   - How does the competition between miners work?
2. A Little Detour – Understanding Hashes
   - What is a function?
   - What is a hash?
   - What is SHA 256?
     - Activity: Creating Hashes
   - What is a “nonce”?
   - What is a Merkle Tree?

1. Mining
   - Don’t Trust, Verify
   - The Block Hash
   - The Nonce of a Block
   - Activity: Analyze Blocks in Real Time

7.1 Mining Nodes

- They strive to be the first to solve computational math problems and create new blocks.
  - •The aim is earning monetary rewards.
  - •And the condition of showing work was expended on it.
  - •Thus, they help to keep the network secure.

- Miners always run a full node, but they also:
  - •Package valid transactions into groups, creating and proposing blocks.
    - -Through a mechanism that gives security to the network called PoW (*proof-of-work)*.
    - -It is necessary for security, which prevents and disincentivizes fraud and enables trust within the network..

- The reward for mining each block consists of:
  - •New ***bitcoin*** made by the **Bitcoin** software.
  - •And the transaction fees for all transactions included in the block.
- A key difference between full nodes and mining nodes:
  - •Mining nodes can propose new blocks to the **Bitcoin** network.
    - -They try to solve cryptographic puzzles in a process called “mining.”
    - -They must prove that they are the ones who have performed the work required to mine the block.
    - - Therefore, they can receive rewards for the blocks.
  - •Full nodes cannot propose new blocks
    - - Therefore, they cannot receive rewards.

How does the competition between miners work?

- Again, let’s go back to an analogy:

○Each miner has a special die that is marked with the numbers 1 to 1000, that is, it has 1000 faces.

○The miners get ready to enter a competition, with the incentive to win a little over 6.25 ***bitcoin*** in the next 10 minutes.

○**Bitcoin** picks a target number from 1-1000 and publishes it for everyone to see on the network. Let’s say you pick #8.

○ The goal is to land on a smaller number than 8.
  - -Some miners have advantages and have a higher chance of winning. Why?
  - -They have more purchasing power and have bought more than one die.
  - -Some throw at a higher speed than others.

○ Competition Begins:

- Miners start rolling their dice hundreds of times, but this requires a lot of work. Their hands get tired.
  - • A lucky miner raises his hand and says “I won!”
  - •All the other miners stop rolling their dice and look at the table where they are playing.
  - • In this way, everyone can verify the miner is telling the truth.

•If the majority, by consensus, agress that the miner is the winner, he is given his reward.

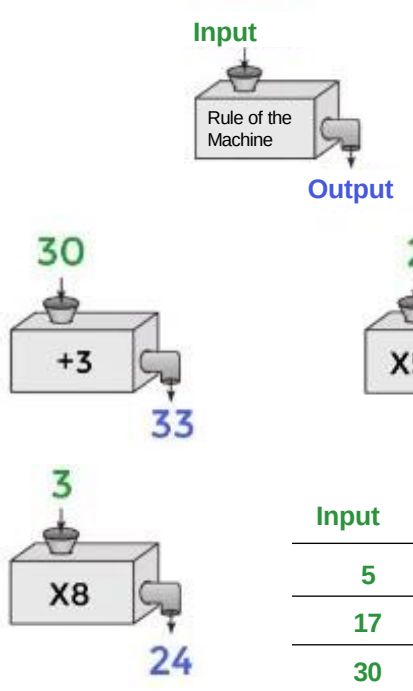
• The game starts again.

○If more miners enter the next competition, Bitcoin lowers the target number so that it always takes about 10 minutes for someone to win.

7.2 A Little Detour to Understand the Importance of Hashes

What is a function?

- As a transforming machine:
  - ·Something is introduced, modified by strict rules, and something completely different emerges.
  - •That is, the input data, x, or the data that one enters is supplied.
  - •Predefined mathematical operations (addition, subtraction, multiplication, etc.) are applied to it.
  - The result is an output, ***f(x),y***.



Input	Output
5	8
17	20
30	33

- Example: f(x)=3x+4, tells me:
  - •Multiply the input data (x) by 3, add 4 to it, and get the output of f(x), or y.
  - •What would be the answer of f(2)? That is, what is the result of y when x=2?
  - •Now what is the question here? F(x)=15. Are we looking to find the input or the output? Is it possible to find the value? Let's see...

f(x)=3x+4=15 3x+4=15…. x= ?

- Some functions are unidirectional.
  - •They have the property of being easy to calculate but difficult to invest.
  - •Even if we know the result, we will not be able to decipher the input data.

- If you hate math, let's formulate an analogy that will help you better understand this concept.

We are going to make a red fruit juice.

- These are the input data: (c=cup)
- •1 c water, 3 ice cubes, 19 raspberries, 8 strawberries, 15 c blackberries, and 1/5 c sugar.
- The operation of the function:
  - -Mix it all together in the blender.
- Output data result:
  - - It turns out a delicious juice

- •It is almost impossible for another person to figure out what its exact ingredients and portions are.
- ·This is what is meant by a unidirectional function.
- •The juice cannot be converted back into its input data.

Miners and Bitcoin Mining

What is a hash?

- **Bitcoin** uses cryptography, a branch of mathematics, to secure the network.
  - •Its input and output process is very similar.
  - • A cryptographic *hash* function:
    - –It is a cryptographic operation that takes any amount of data,
    - -It returns a hash value of unique and unrepeatable, deterministic and chaotic identifiers.

My First Bitcoin → **Function Hash** → 41798cc97f-682c23159597a-1b039b5abb-9700ff9160b-850dee4d88ad-86bf1594

- There are no restrictions on the input data:
  - •The hash always results in the same length of characters.
  - • The hash is also considered a fingerprint of input data.

GLOSSARY

***Deterministic**: The same inputs, or letters, will invariably produce the same outputs, or results.*

***Chaotic**: A slightly different input (or even the same repeated input) will produce a completely different and unrelated output.*

What is SHA 256?

- The particular hash function that Bitcoin uses is called *SHA256*.
  - •Its result or hash is always hexadecimal (numbers between 0 and 9 and letters between A and F)..
    - ***SHA256(input)=hash***

- Let's create *hashes*. Let's see the following examples:

SHA256(Dalia) =
bbadb37bc80b041a1cafdfadf1efd93d
6386117b33046d650e75ec2cb101758c

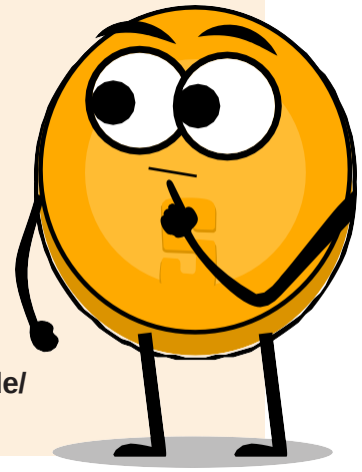
SHA256(DaliaP) =
25cad1ff3deb7bc5ba54ccf1f0fe8e8ff
4a17f58826847b8cae2ddbd6cd6ab77

SHA256(Hola, me llamo Dalia. Soy de Medellín, Colombia.) =
619010e5ab4877ef398e82a277e7134
529a5ff1875f7671ff0177c7ab0302423

Activity: Creating Hashes

Class Activity. How do you create a hash? On the following websites we will be able to practice it:

https://hashgenerator.de/



First, what happens when you enter Dalia's 256 hash, or My First Bitcoin? Compare it with the hashes written here.

Do you realize that although the result is random:

- The result of a particular input will always be the same.

- If instead of name, surname, and date of birth, we identified ourselves with a number like this, there would not be the problem of having two "Maria" or two "Jose" in class.

What is the hash of your name? Your full name?

What happens if you change a letter in your name? Could you have predicted this hash?

What is a nonce?

- The term "nonce" comes from "number used once."
  - •It is simply a number used once.
  - •Nonces are very useful for mining since one of the main goals is to find SHA256 (Input) results that satisfy certain predetermined ocnditions.

- Suppose the goal is to find a hash that starts with the number "zero."
  - •Changing only the last digit to SHA(DaliaP). The nonce would change the "P" :

SHA(Dalia**1**) = c2cb88c9aec429a7fe9194351e-748247f668241ff75c708b43ea83ecd730268f

SHA(Dalia**2**) = 17df2ae3b1dec56c7bde0cf8b-161f24329d351e08cb797adbd76af46401da-df3

... We were lucky and just needed to try eight times to achieve our goal:

SHA(Dalia**8**)=**0**93d4ddb-855114f49f3b775803529ed1cbd5598b5995c-327091552bab5672658

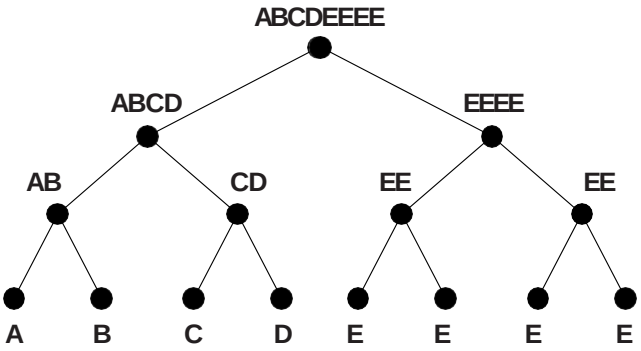
What is a Merkle Tree?

- A data structure divided into several layers of hashes that allows the information of all transactions to be verified quickly and efficiently.

- It is like an inverted tree, starting from the leaves and progressively climbing through the branches until reaching the root node.

- The root node is the main identifier that allows verifying the data set as a whole.

- Its final unique root, which contains all the information of all the transactions is called -
  - The Merkle Root.



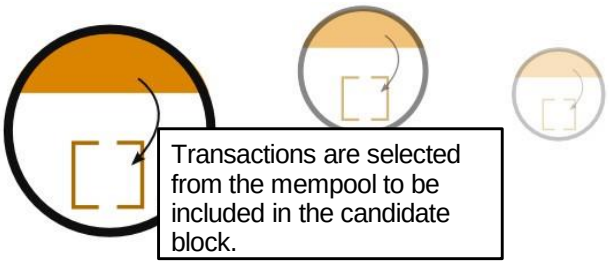
7.3 Mining

Now back to the **Bitcoin** process.

- Miners are free to choose transactions to include in their next block.
  - They select and group new verified transactions to a new "candidate block".

Which transactions should they choose for their "candidate block"?

- They choose those with greater monetary incentives and that occupy the least memory.
  - Depositors add commissions (or fees) to incentivize miners.
  - Additionally, the miners are motivated to work honestly.



- The more transactions there are in the mempool, the more congested the network.
  - The monetary incentives (fees) are generally greater when there is a lot of traffic.
  - During heavy traffic, miners choose transactions that have higher fees.
  - Once traffic has decreased, those with lower incentives are added.

What does each candidate block consist of?

- The size of a block is approximately 2.5 MB.

- Each block holds a few thousand transactions at most, so it is important to choose efficiently.
  - Includes a block header.
    - This block header is hashed.

SHA256(*header*) = RESULT

What is this RESULT used for?

- The goal is to produce a valid identifier for a new block, which fits perfectly behind the last block in the existing chain.
  - For this, a miner must produce the "winning hash".

- Which must be below a specific "target value".

•As long as the RESULT is greater than the desired hash,

-The miner sets a nonce and tries again.

-The miners repeat this several thousand times per second,

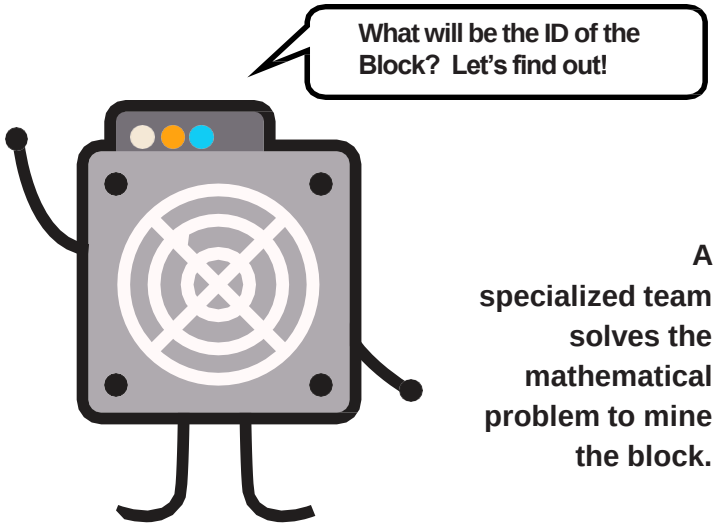
-In order to win the block offset.

-And create a "fingerprint" or a unique hash of said block

•The process requires changing the nonce thousands and thousands of times, generating many possible RESULTS, until achieving the "winning hash" before any other miner.

•Very similar to our initial example of rolling the dice many times, until a miner manages to win with a RESULT below the target.

- This means that any mining node in the network can mine a new block.
  - •But you need to expend energy to be able to do it.

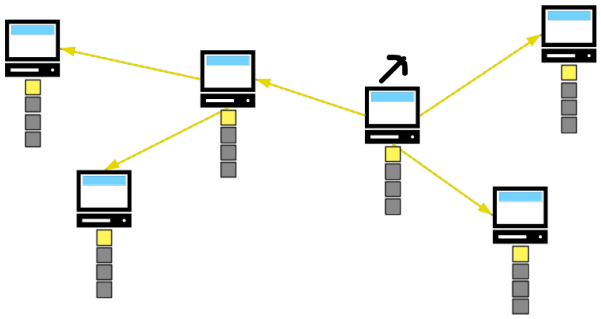


A specialized team solves the mathematical problem to mine the block.

What happens when the "winning hash" is found?

- A lucky miner finally produces the winning hash,
  - Broadcast the success to the entire network.
    - That hash becomes the "block hash" or its unique identifier.

- For the rest of the miners, the confirmation of the block validity is a simple process.
  - •You just have to ensure that all transactions remain valid.
  - •And that the hash of the block is less than the "target value".



- When the block is confirmed, the other nodes will add it to the existing chain.
  - •All the transactions contained in said block will be permanently recorded in the block chain.

- The process will repeat approximately every 10 minutes.
  - •Miners will start trying to mine a new block on top of the last one.

And how does the miner who has found the target value earn the reward?

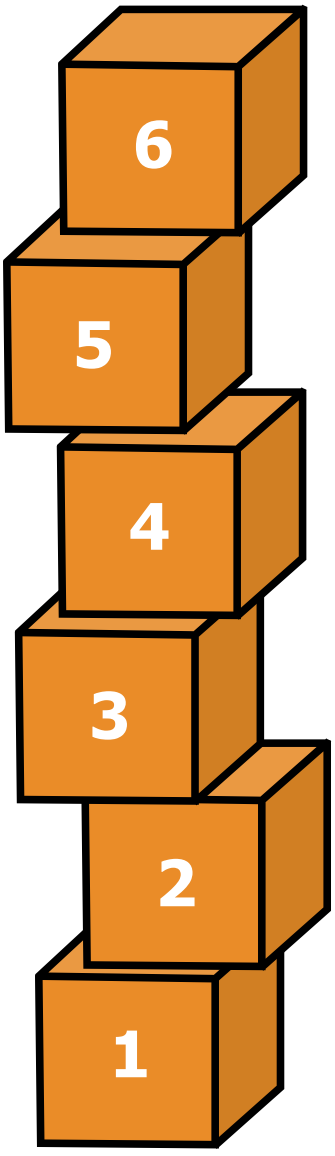
- All candidate blocks create a first transaction that includes a reward:
  - •It contains an amount of new bitcoin that will be released when the block is created.
    - And all the commissions generated by the selected transactions.

- Only the winning miner can collect said reward.
  - For his great computational effort, PoW or Proof of Work:
    - *PoW has been a successful method*:
    - Because finding the hash is extremely difficult, but verifying it is very easy.
- This transaction is called coinbase, or base currency. (Not to be confused with the crypto exchange "Coinbase").
  - •It is the first in each block of the blockchain.

Don't Trust, Verify

What does this mean?

- Transactions get a confirmation when they are included in a block and then after the confirmation of each subsequent block.
- For such a block to be included in the blockchain, it must be properly linked under the last block created on the network.
- A confirmation on the blockchain indicates that "the transaction has been processed and validated by the network and is very unlikely to be reversed."
- It is recommended to wait a minimum of six confirmations to ensure that the funds have been transferred.
- Bitcoin is known as the most secure and truthful blockchain in existence.



Block #6:
6 confirmations - your transaction is secure.
60 minutes

Block #5:
5 confirmations
50 minutes

Block #4:
4 confirmations
40 minutes

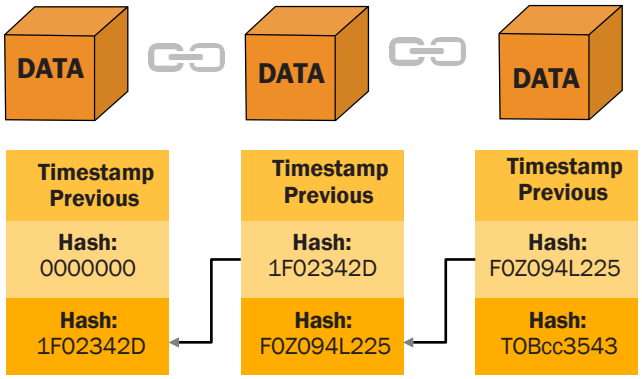
Block #3:
3 confirmations
30 minutes

Block #2:
2 confirmations
20 minutes

Your transaction is confirmed!
10 minutes

The Block Hash

- Each block refers to a previous block,
  - •Through the 'previous block' field (previous hash) in the block header.



- The sequence of hashes that link each block to the previous one creates a chain that goes back to the first block ever created.
  - •The first block is known as the genesis block.

- Any minor modification to any transaction will change the hash of the block, detaching it from the previous block.

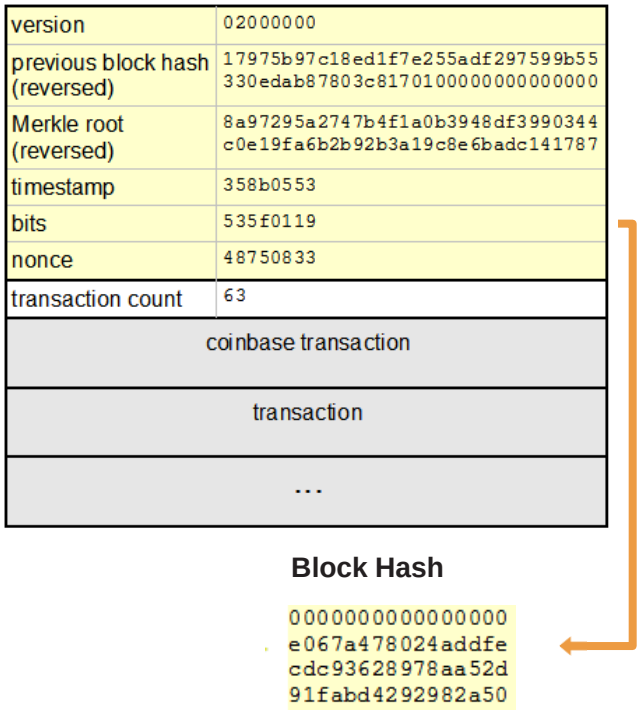
- If a hacker tries to tamper with even a comma of a transaction, it will create a cascade of failures to verify subsequent blocks.

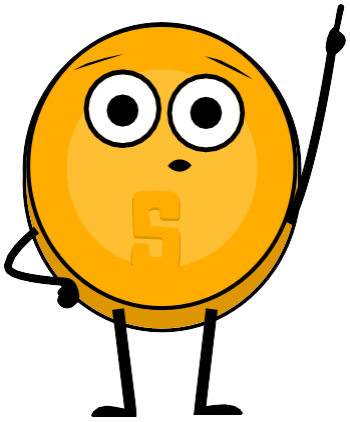
- This is because each block has information about the previous one.

- Blocks are made up of a block header and its transactions.

  - • The header contains:
  - ~~1.~~ The summary of the data within the block, that is, all the transactions compressed into a Merkle Root.
  - ~~2.~~ The hash of the previous block in the blockchian.
  - ~~3.~~ A nonce, which can change as many times as necessary in search of a "target value."

- Using the SHA256 function, all the information contained in the block is compressed.
  - •This result is the "hash of the block" or representative of its "fingerprint".





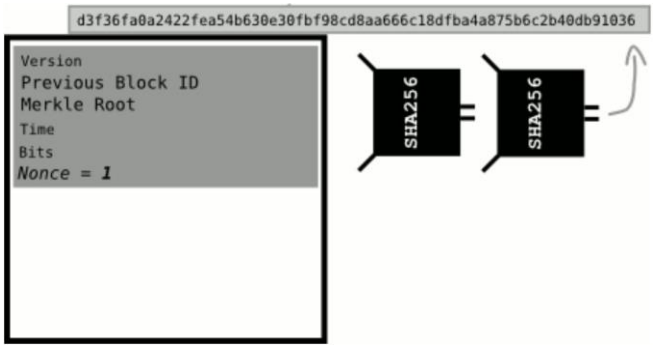
Miners and Bitcoin Mining

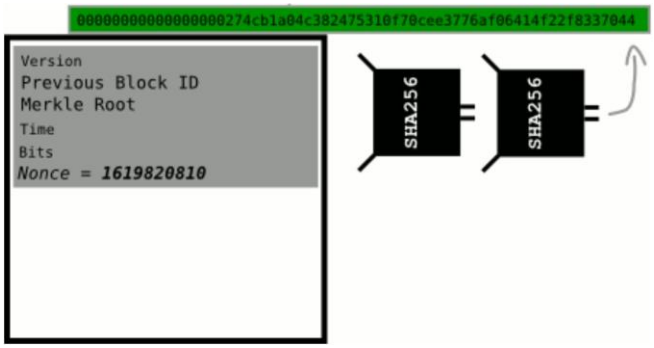
The Nonce of a Block

- The nonce of a field is a number within its header:
  - Miners modify it until the header hash results in the target difficulty or target value.

- The difficulty target always starts with a number of zeros.
  - The number of zeros is variable.
  - It depends how many miners are trying to mine the block.

- When a miner finds a nonce that, added to the header hash, meets the difficulty objective, it adds it to the header of the new block and sends it to the network so that the rest of the miners can verify that the solution is valid.





Activity: Analyze Blocks in real Time

Class Activity. In the following link you can analyze the chain of blocks in real time. Answer the questions based on the information on the website.

1. What was the last block mined?

2. How many transactions were included in that block?

3. What is the total value traded in bitcoin?

4. What was the size in MB of the block?

5. How many zeros does the nonce of the block start with?

6. How much did the miner earn in total?

7. What was the total value of the commissions (fees) that the miner received for adding the transactions to the network?

8. Choose one of the highest value transactions in the block. The amount of BTC was distributed to how many wallets?

Class #8

Scarcity, Cost, Price and Volatility

1. The Importance of the Block Reward
2. Halving
   - Halving Events
3. The Value of Bitcoin over Time
   - Medium and Long Term Factors
   - The Lindy Effect
4. The Rewards to the Miners
   - The Difficulty
5. What or who do I have to take care of?
   - Attacks on Bitcoin
   - What is a 51% Attack?

Scarcity, Cost, Price, and Volatility

8.1 The Importance of the Block Reward

In order to create a successful decentralized economic system:

- Miners invest money and computational work to mine ***bitcoins***.

- They secure the network to prevent attacks, and at the same time:
  - •They generate new coins that can circulate freely in the network.

- The block reward acts as a subsidy and incentive for the miners.
  - •Transaction fees or commissions ensure that there are no network failures.

8.2 Halving

- Satoshi Nakamoto designed a very strategic way of distributing new bitcoins without one person or group of people being in charge of distributing them.

- In order to pursue a deflationary model, it was established that:
  - •Every 210,000 blocks the number of bitcoins released is halved.
    - -This happens about every four years.
  - •Unlike the problems we face with fiate currencies, where no one really knows how much credit or dollars are in the system,
    - **Bitcoin has a full supply fixed at 21,000.000.**
    - –This fixed supply cap is automated control.
    - It is enforced through consensus.
  - At the start, the bounty was set at 50 bitcoins per block.
  - •Approximately every four years, the reward is halved, which is why it is called a halving event.

Halving Events

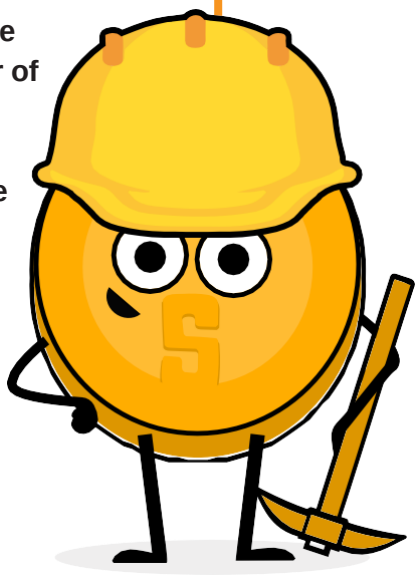
- The first halving occurred at the end of 2012.
  - Block 210,001 only awarded 25 BTC.

- The second halving occurred in 2016.
  - The reward reduced to 12.5 BTC.

- And so it will continue until the year 2140.
  - •When the 21 million bitcoins will have been mined ***bitcoins***.

- This halving of rewards was implemented with the intention of:
  - Preventing Inflation
  - Adding Natural Scarcity

Here you can see the total number of mined bitcoins currently circulating in the net.



So why the change? Why not keep the reward same? Isn't that unfair to the miners?

The answer to that question lies in the law of supply and demand.

- If coins are created too fast and there is no limit to the amount of bitcoin that can be created:
  - •Soon there will be too much bitcoin in circulation and its value will decrease.

- If all 21 million had been released at once:
  - •A few people may have hoarded it.
  - •No one else would have had the opportunity to accumulate it.

- The following graph exemplifies how the halving affects the price over time:

8.3 The Value of Bitcoin Over Time

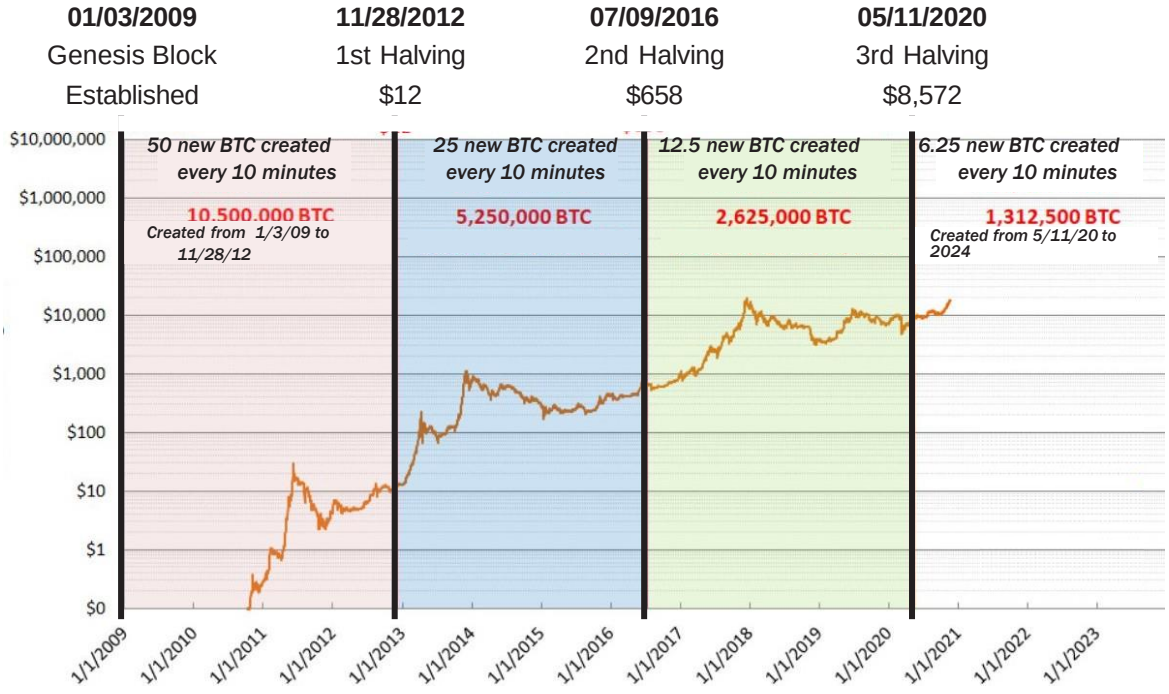
The value of bitcoin has increased:

- Less than $0.01 in 2009 (on first transaction).

- Up to a maximum of around $67,000 USD, in November 2021.

- In the last decade, although it has had falls of up to 80%, not only has it recovered, but in the long term, its trend is upward.

- Factors affecting supply and demand have diversified
  - *Why is bitcoin valuable?*
  - *Why has the price gone up so much?*
  - *Why is it so volatile?*



Scarcity, Cost, Price, and Volatility

To better understand this, there are some terms important to us that we must define:

1. Circulating Supply:

- •The amount of bitcoin created so far..
- •As of July 2022, approximately 19,101,000 bitcoins have been created.

2. Total Supply:

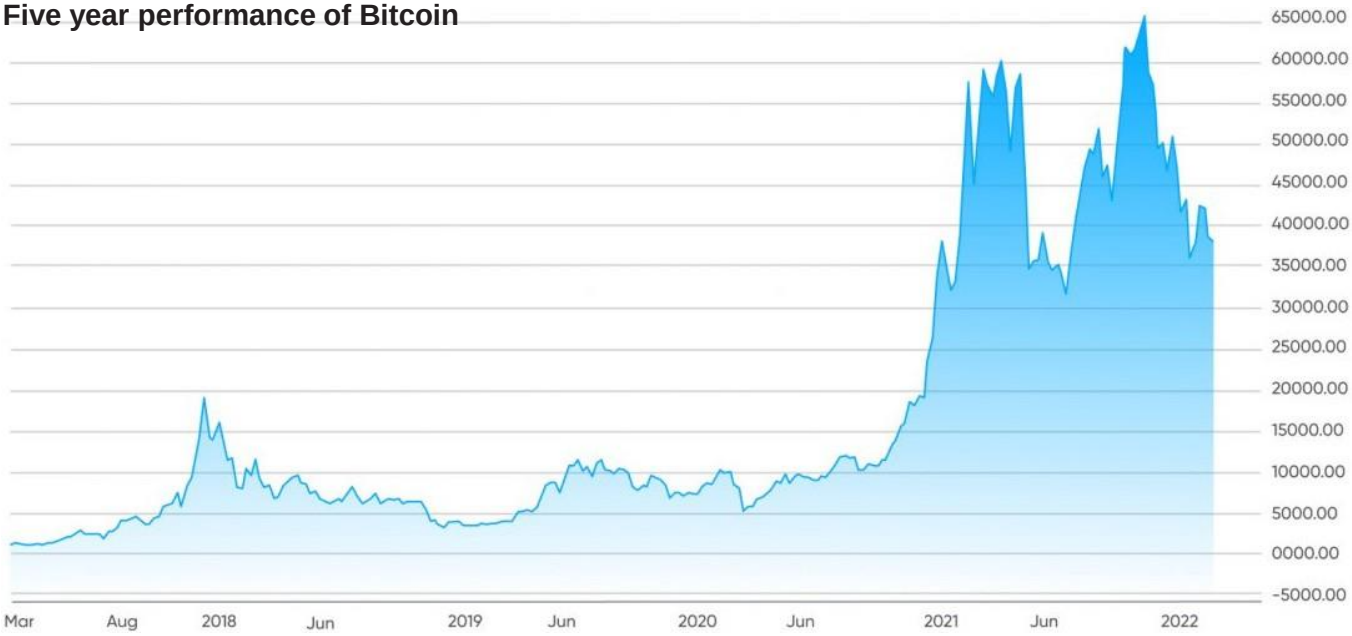
- •Number of coins already in circulation, plus coins that have not been mined.
- • In total, the total supply of bitcoin will be 21 million.
  - -It is estimated that around 4 million bitcoins are missing or considered “lost."
  - -Believed to be unspendable due to lost passwords, incorrect output addresses, or program errors.

3. Market Capitalization:

- •The total market value of the circulating supply of bitcoin reflected in fiat currencies.
- •Multiply the current price of a bitcoin (in USD) by the current supply.

Market Capitalization =
Current Price x Circulating Supply

Five year performance of Bitcoin



- In the graph on the previous page, we see the price of bitcoin over the last 5 years.
  - •This is an easy way to visualize how sensitive or volatile the price is.
    - X axis is for time and Y axis is for price in USD.

What world events might be related to price changes?

So what factors determine its price? How is mining involved? When does the halving affect the price?

- The demand continues to grow permanently.

- Your supply system has a fixed supply.

- It is a nascent asset that is only 14 years old and just beginning to be regulated.
  - -Of course volatility in its price is expected.
  - -However, its price has been on the rise since its creation.

Analyze the historical chart of bitcoin prices.

ColinTalksCrypto.com

Medium and Long Term Factors

- The factors that determine the price of bitcoin can be analyzed in the medium and long term. Next we will see each of them.

Medium Term Factors:

• *Daily Commerce*

- –Unlike other financial markets, it operates 24 hours a day, 7 days a week.
- -Transactions can be made through mobile devices.
  - Allows you to easily exchange any amount of ***bitcoin***.
- -For HODLers this is a nightmare as the price can change up to 20% in a single day.
- -For traders, it is an opportunity to take advantage of these price changes and make profit.

• *World News and Events*

- Sensitive to world events, news and speculation.

• *Mining Costs*

- -The miners are responsible for adding more and more bitcoin to the total supply.
- -If electricity costs go up, miners are forced to sell 40-60% of their bitcoin as they have to cover bills and hardware expenses.

• *Market Bubbles*

- -In recent years, bitcoin buyers have become more diverse and their buying and saving habits vary.
- -The size of your holding in Bitcoin and your behavior towards it can change the overall price of bitcoin.

• *Government Regulations*

- The regulation of cryptocurrencies

increases daily, this can affect the value of ***bitcoin***.

- Joe Biden introduced a law in which, from now on, digital asset transactions worth more than $10,000 must be reported to the Internal Revenue Service.

Long Term Factors:

• *Halving*

-The bitcoin reward happens to be halving around every 4 years.

-The miners' reward decreases drastically at these times.

• *Mass Adoption*

- If everyone starts using it, a process called hyperbitcoinization, and by extension invests more of their money in bitcoin, the price will rise exponentially.

1998 2005 2014 2021

2012 2013 2014 2021

• *The Lindy Effect*

-It is a theory about the aging of non-perishable things.

- The older an idea or technology, the longer its life expectancy.

-Non-perishable things like technology age, linearly, in reverse.

• *Limited Offer*

- The fact that there is only a finite amount of bitcoin means that it is not possible to dilute the system after 2140.

- The "rainbow chart" uses a logarithmic scale to visualize the price of ***bitcoin***.

○ The color division:

-Shows when the currency is oversold (blue and green zones).

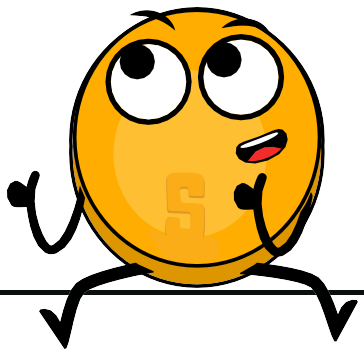
-Or when it is overbought (orange, red, and purple zones).

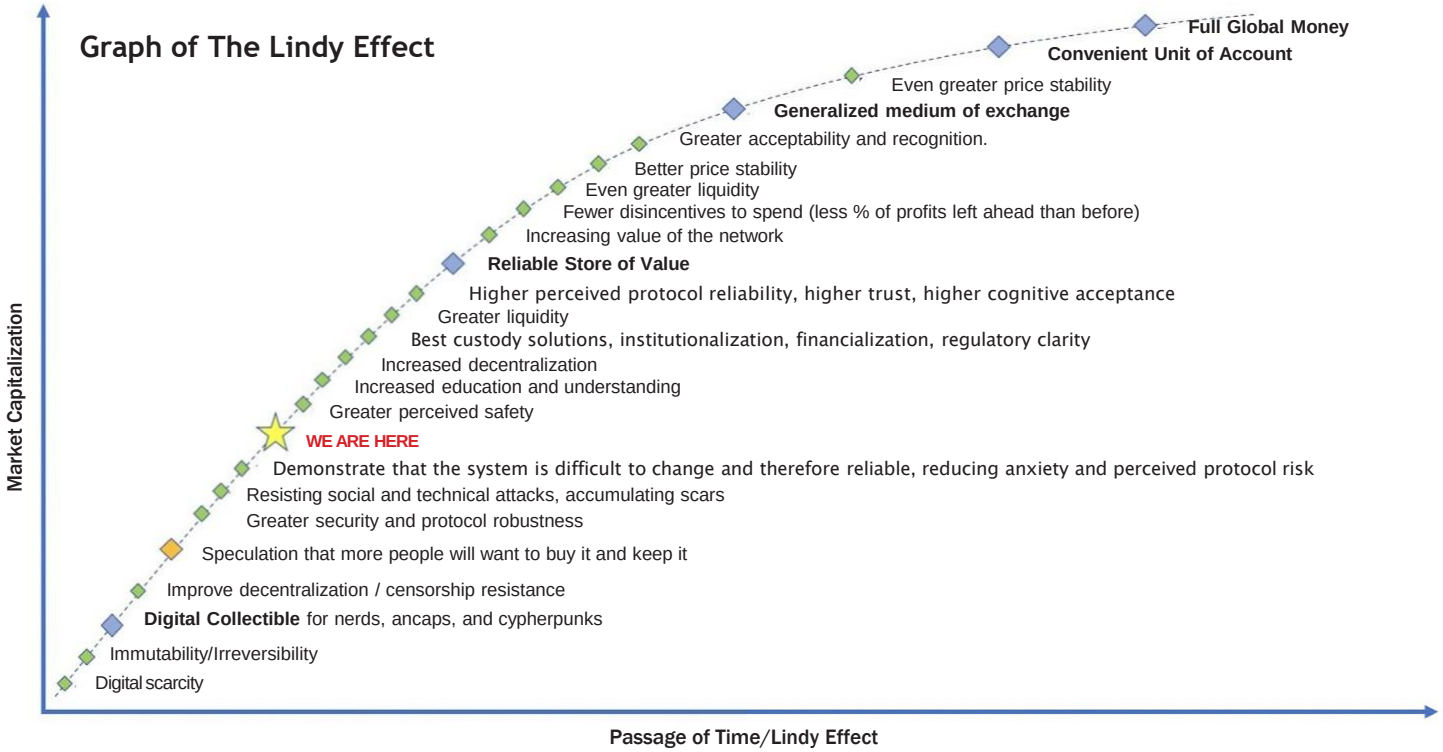
○ This chart gives us valuable information to determine buying and selling strategies for ***bitcoin***.

○ Some very successful investors wait patiently:

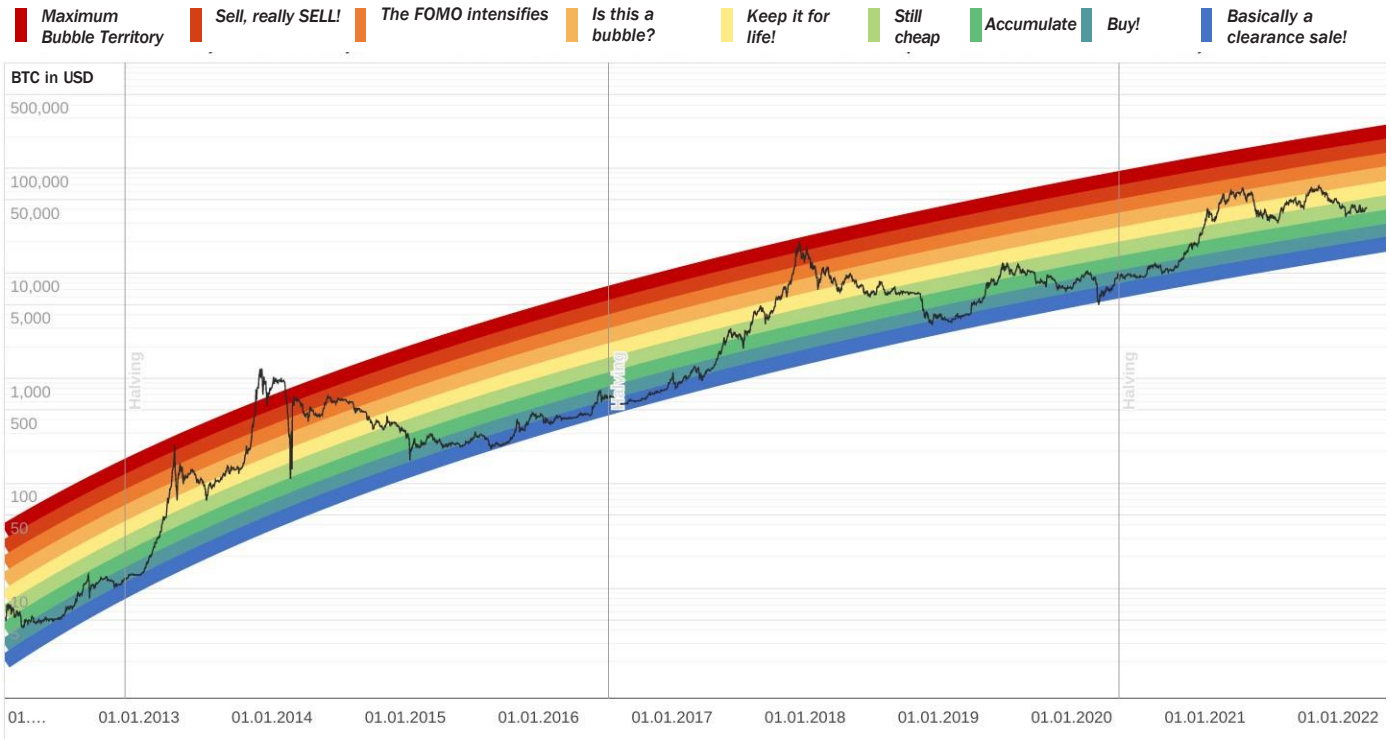
-They buy when the price reaches the blue/green zone.

-They sell little by little, while the price approaches the red band.

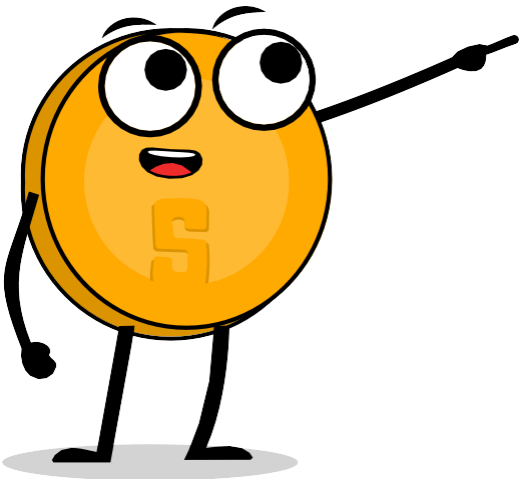




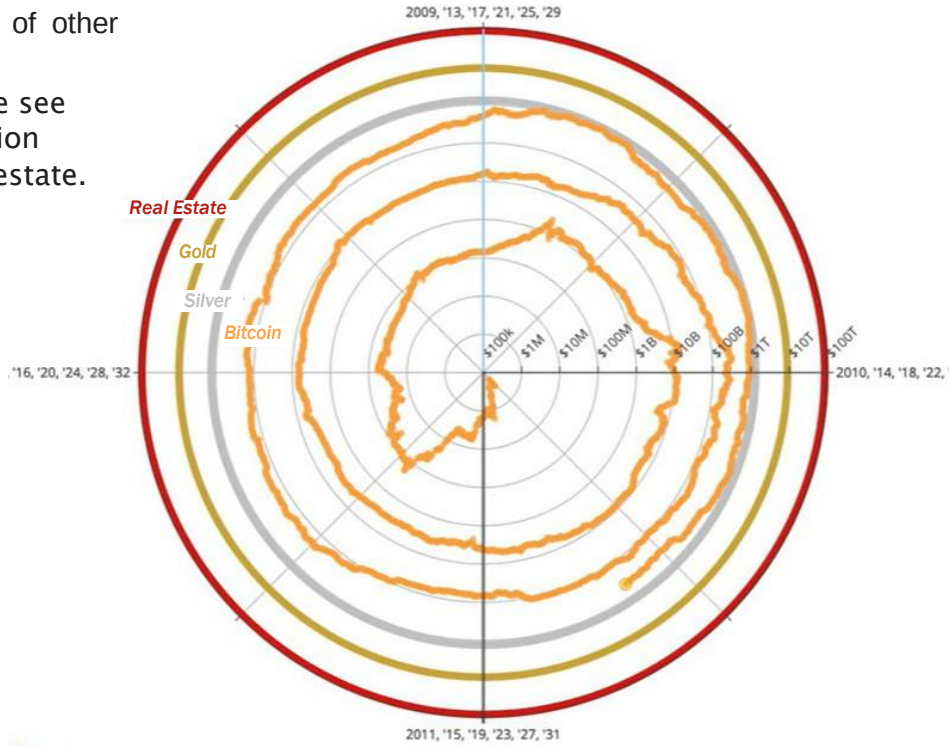
Rainbow Chart



- Let us see in perspective, and through four-year cycles, the growth in the capitalization of bitcoin in relation to the capitalization of other global monetary assets.
  - In the graph on the right, we see the Bitcoin market capitalization against gold, silver, and real estate.



Crossed Asset Spiral



8.4 The Rewards to Miners

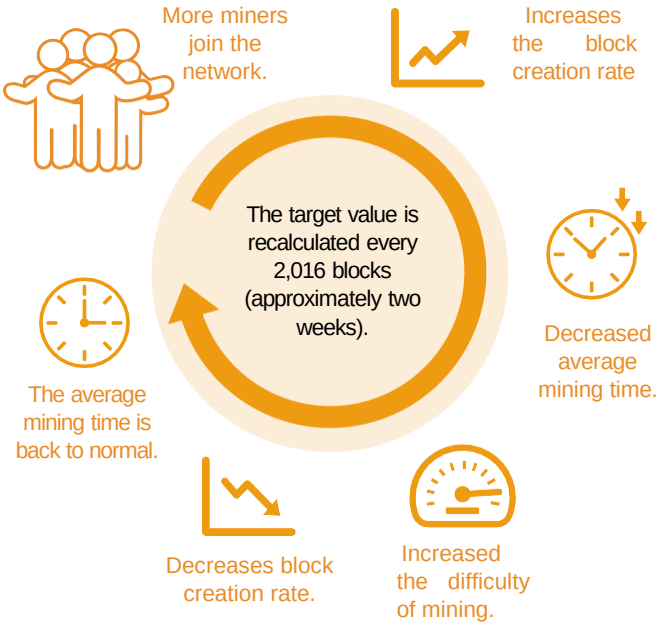
- Let's see how the rewards and monetary incentives to miners have changed over time and observe that there are times that are more profitable than others.
  - •The miners' incentive still remains, regardless of the smaller rewards, as the value of bitcoin increases in the long run.

Total Income of Miners
$34,688,409.61

The Difficulty

- Difficulty is a measure of how hard it is to mine a block of **Bitcoin**.
  - •Or to find a hash below the proposed "target value."
- Difficulty adjusts every 2016 blocks (approximately every 2 weeks).
  - •So that the average time between each block is kept at 10 minutes.
- Difficulty setting is directly related to the total mining power.
  - •It is estimated in terahashes/second (TH/s). (Tera = trillion)
    - Today's network has the capacity to compute trillions of hashes per second.

- The higher the difficulty, the more computing power to mine the same number of blocks, which makes the network more secure against attacks.



8.5 What are who do I have to take care of?

Although Bitcoin can offer much greater protection than the traditional financial system, scamming money from unsuspecting victims is becoming more sophisticated. For example:

- Identity Theft.
  - •The attacker can force the recipient to reveal sensitive information.
    - -They steal your credentials after inducing you to change your password.
    - -They steal your private keys and therefore your bitcoin.
    - -They lure you into visiting a malware website and take control over your computer.

- DNS or browser extension hijacking:
  - •Attackers hijack legitimate websites.
    - -They replace them with fraudulent interfaces.
    - -They trick users into entering their private keys on these fake sites.

- A hacker can exchange the SIM cards of two mobiles and steal all the data.
  - •Cybercriminals seek to take advantages of any situation. Businesses and security teams are struggling to keep up.

Attacks on Bitcoin

The physical attacks that are known to Bitcoin.

- None of these attacks have managed to disrupt the Bitcoin network.

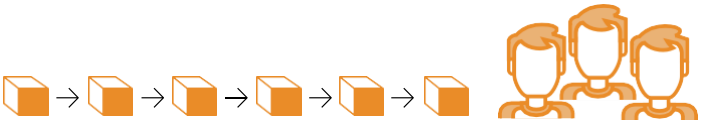
- If the private keys remain in a safe place:
  - •Heists become practically impossible.

- Still, there is the tiny chance of a 51% attack.

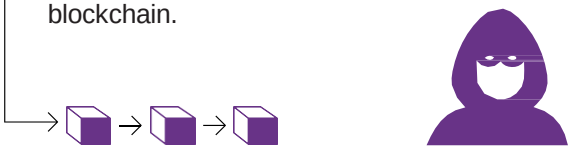
Scarcity, Cost, Price, and Volatility

What is a 51% attack?

- To achieve this, it would take work, energy, and centralized computing.



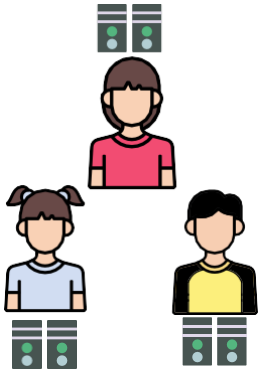
Most miners are adding and streaming blocks to the public blockchain.



An attacker is adding blocks to a private blockchain and not transmitting them to the public blockchain.

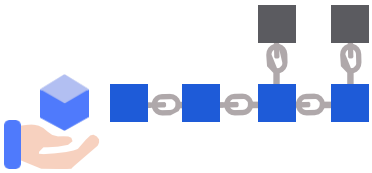
- A malicious miner would have to amass more than 50% of the computational power of the network.
  - •The network would no longer be decentralized, but controlled and manipulated by said miner.
  - •A new chain tied to the original chain is created.
    - -This would end up tricking some of the participants into adding their blocks to the new chain.
    - -You can easily manipulate, alter, or trigger the chain to your advantage.
    - -You can steal money through double spending and/or censoring transactions.

- This type of attack has never happened with **Bitcoin**.



In PoW-based networks, there are multiple participants (mining nodes) that add new blocks and confirm the information in the blockchain..

Miners compete with each other to win the right to have their version of a new block confirmed by a majority of the participants.



Class #9

Bitcoin – Today and the Future

1. Energy Consumption
2. Innovation
   - Software- Bitcoin Core
   - SegWit, Taproot, and Schnorr Signatures
   - Taro
3. Bitcoin and the future of El Salvador

Bitcoin – Today and the Future

9.1 Energy Consumption

Does Bitcoin really consume as much energy as believed?

To increase earnings:

- Miners connect a large numbers of computers.
  - In order to increase your chances of getting ***bitcoin***.

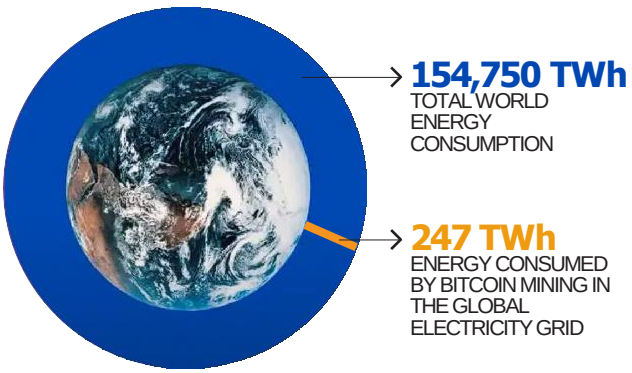
- Computers work almost day and night to win the "lotteries",
  - Therefore, the electrical consumption is considerably high.

- The technology used for mining Bitcoin is getting cleaner every day,
  - So much so that the adoption of sustainable energy rose to 59.5% in April 2022.

- Although the Bitcoin hash rate has grown by 23% compared to the beginning of 2021,
  - The electricity consumption of BTC mining is 25% lower than it was back then.

- Current ASICs are 100 billion times faster than 2009 CPUs.

- The energy consumed by Bitcoin represents 0.16% or the energy worldwide.

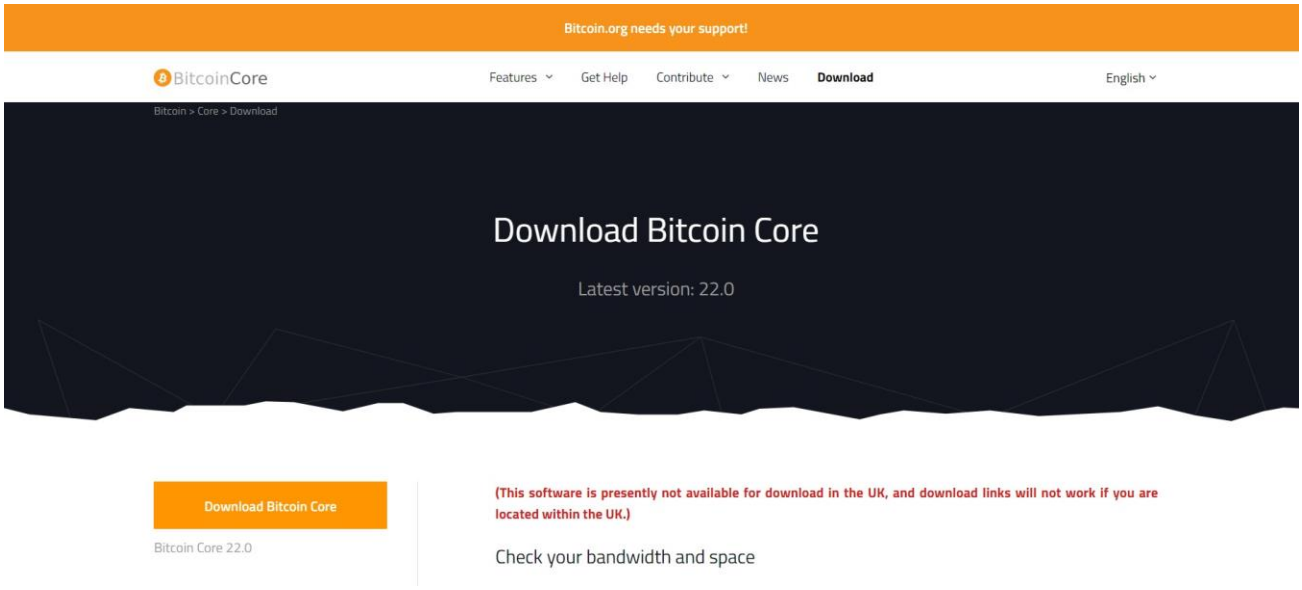


9.2 Innovation

Software- Bitcoin Core

- Bitcoin Core is the original software created by Satoshi Nakamoto.
  - Designed to connect to other people running the same program,
  - Creating a network of computers that communicate with each other.
  - Its purpose is that when downloading it, everyone works with the same set of rules.
    - To validate transactions.
    - And contribute to the security and decentralization of the system.
  - Whoever runs it can install it like any other program.
    - Download and create an additional copy of the entire blockchain.
    - It can help transmit transactions to other computers.
  - As long as there is no internet access, no permission is needed to:
    - Download and/or use it freely.
    - Transfer bitcoin to another wallet or receive from someone else.
    - Demonstrate verification of the issuance of the offer.
    - Know the transaction history and the owners of each ***bitcoin***.

- Dozens of experts in software and cryptography work on its maintenance and improvement.
  - Who proposes an update in the software, requires the consensus of the majority of those to implement it.



Open Source Code

Anyone can view, propose changes, modify, and distribute as they see fit. It's comparable to going to a restaurant and having access to the recipes of your favorite foods (the code)… but then you can make them and add or subtract any ingredients you want and refine them.

SegWit, Taproot, and Schnorr Signatures

Bitcoin has improved through consensus, through Bitcoin Improvement Proposals, BIPs. This has made it safer and more efficient over the years.

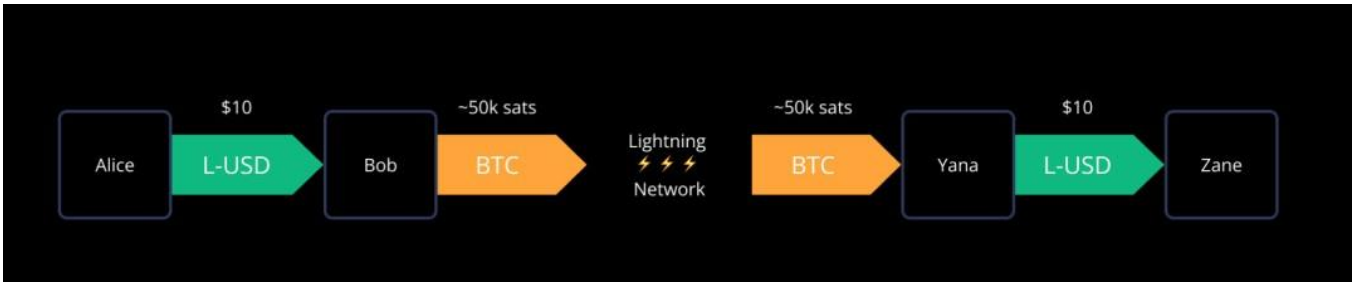
- First, ***SegWit***, a soft fork that was implemented in 2017,
  - •Increased block size limit by removing portions of transactions.
  - •Improved the processing speed of Bitcoin transactions.
  - • Fixed a protocol weakness which allowed nodes to:
    - -Handle transaction malleability problems (TXID) in the network.
    - –Transaction malleability is when an attacker can modify or alter the hash of a transaction within the blockchain.

- Second, ***Taproot*** was created to improve privacy and increase anonymity on the web.
  - •Taproot, can "camouflage" transactions.
  - •Reduce transaction validation times.
    - - Which could help promote bitcoin as a means of payment.
  - ·Transaction fees could be significantly reduced.

- The substitution to Schnorr firms; replaces the current elliptic curve digital signature (ECDSA).
  - •Integrate several keys within a complex transaction and generate a unique signature.
  - Simplify smart contracts on the blockchain.
  - •It helps scale second layer payment channels, such as the ***Lightning Network***.

Taro

- With the new Taro protocol, the aim is to take bitcoin technology to another level.
- It will enable the issuance of stablecoins and other assets on the Lightning Network.
- You will be able to exchange any currency for another instantly, practically for free.



9.3 Bitcoin and the future of El Salvador

- The originality and possibilities of Bitcoin has caught the attention of:
  - The world of investment.
  - The corporate world.
    - -Both public and private companies are subject to the same impacts of inflation and interest suppression for savers.
    - They seek to strengthen their balance sheets.
    - -They have large cash reserves.
    - -They are adopting bitcoin as a long-term store of value.

- El Salvador is likely to have a giant advantage over the world in the future.
  - It has become the first country to make Bitcoin legal tender, paralleling the US dollar.
    - Bitcoin Beach is already a robust and solid project. You have managed to create a circular economy within a coastal community.
  - •The IMF and the World Bank have spoken out against this decision.
    - Meanwhile, El Salvador continues to accumulate satoshis.

- Who will be the next to make Bitcoin legal tender?
  - •Countries that encourage adoption sooner are likely to benefit the most.

- The US dollar appears to be on the verge of collapse, with the ruble (Russia) and the yuan

(China) taking a bigger role in geopolitics.

- Both are fiat currencies, with a common denominator pitting against *bitcoin*.

- Several countries are trying to implement central bank digital currencies (CBDC's):
  - Attempts to create fiat currencies with digital benefits.
  - It implies that the government can monitor every transaction.

Who is buying Bitcoin?

- Russia is willing to accept oil and gas in *bitcoin*.
- Rio De Janeiro is willing to accept property taxes in *bitcoin*.
- Some US cities are willing to accept taxes in *bitcoin*,
- Some government officials in the US accept their salaries in *bitcoin*.

- Bitcoin in the future:
  - It will allow massive innovation in Layer 2 solutions.
  - It will modernize contracts, assets, and credentials in the private and public spheres.
  - It will encourage countries to cooperate rather than compete.
  - The desire to manipulate economies by printing money will cease.
  - It may even be that countries and nation states no longer exist, and something new replaces them, with the help of **Bitcoin**... Who knows?

"Whether you think you can, or think you can't– you're right."

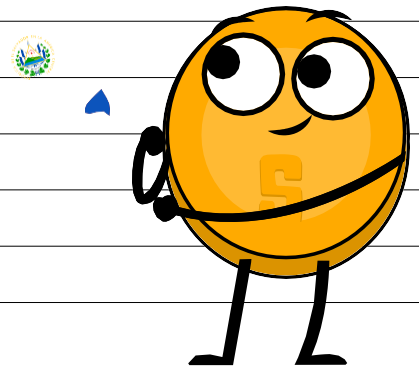
- Henry Ford

Class Activity. Answer the following questions according to what you have learned in the last classes.

What do you think are the most important benefits of **Bitcoin**?

What do you imagine could happen in El Salvador I the next ten years?

Do you think Salvadorans will become more familiar with Bitcoin and find it an essential technology?



9.4 Activity: Bitcoin Simulator

Class Activity. Follow the instructions below:

Create a new wallet.

We have already created a wallet - ***MiPrimerBitcoin***.

The private key is:

e17a9fe1f9cade3f1f8b6426f9fdabe27d0378d931fc8bb5bbb1d25d7c33e6e5

Which has mined 2 blocks (2830,2831) and made a transaction.

So what you can do now:

1. Mine a block to receive your first bitcoin as a reward.
2. Sign transactions and send bitcoins to other wallets.
3. Create your own private blockchain and use the simulator with non-public groups or school classes.
4. Create fake transactions under a fake name and try to obtain bitcoin through fraud.
5. Carry out a 51% attack to later manipulate the blockchain.
6. Tell other people.

The more you understand how Bitcoin works, the better!

Class #10

Final Project

- Why Bitcoin?

Why Bitcoin?

Practical Exercise. Write a one to two page argumentative essay and be sure to cover all of the following points:

- Explain what **Bitcoin** is.
- Explain how **Bitcoin** works.
- In your opinion, what are at least two ways that **Bitcoin** changes the way that the world operates today? Justify your answer.

Additional Class

The Magic of Digital Signatures

- Public and Private Keys
- Digital Signature
- Valid Transactions

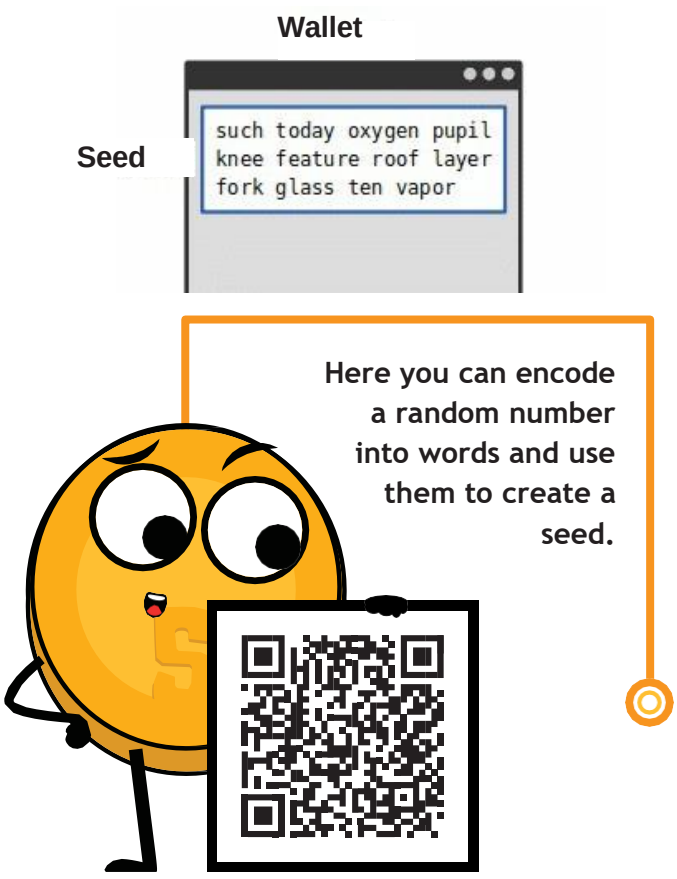
The Magic of Digital Signatures

Public and Private Keys

Now that we understand the security challenges, let's get back to wallets and transactions.

Most secure wallets provide:

- A "**master private key**" or a "*seed*"
  - It is a randomly generated list of 12 to 24 words.
    - -No one else in the world has ever seen.
    - -It is the unique key that allows access to the user's bitcoin on any device.
    - -It is used as genesis to create each of the private keys.



- Cada **clave privada** genera una **clave pública**.
- Cada **clave pública** nos permite *firmar* digitalmente una *transacción*.
- Cada *transacción* tiene una **firma digital** única.
- Cada **firma** permite transferir ***bitcoin*** a una *dirección* en particular.

Entremos en detalle:

- Private Key = Clave Privada
- Public Key = Clave Pública
- Address = Dirección
- Generate = Generar

- **Clave Privada**:
  - •Comparable con una contraseña y debe mantenerse a salvo de cualquier tercero.
  - •En caso perder el monedero, es una forma de recuperar el ***bitcoin***.
  - • A menos que se tengamos una "*semilla*"

- Las claves privadas son números completamente aleatorios y grandísimo entre 1 y 1157920892373161954235709850086879078528375642790749043826051631415161816494336.

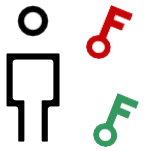
  - • Cualquier clave privada se convierte a una estructura hexadecimal:
    - -Un número de 0-9, A-F, donde A=10, B=11, etc.
  - •Es prácticamente imposible generar la misma clave privada dos veces.

Practica generar una llave privada en el siguiente enlace.

Learn Me a Bitcoin

- **Clave Pública**:
  - •Usando la **clave privada** como dato de entrada,
    - Se usa una multiplicación matemática muy avanzada para generar la clave publica.
  - •La operación es unidireccional- no se puede reversar.

Ejemplo de Clave Privada

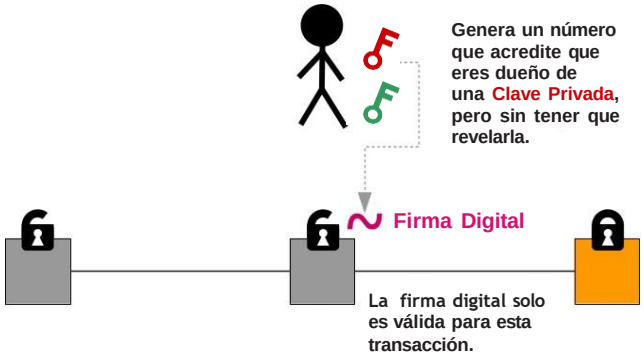


4587174879024769426368125614121805096254055807352815765611711325736666848711182816555669389162077347747757455942375279210720318921963088098868880628247002254

La Clave Pública se calcula a partir de la Clave Privada

La Firma Digital

- Se usa para demostrar que conocemos la clave privada sin revelarla públicamente.
- Se calcula a partir de la clave privada y de la información incluida en la transacción,
- Es única, irrepetible e imposible de falsificar.
- Es obligatoria para desbloquear el ***bitcoin*** que el emisor va a trasladar.



Detengámonos un momento...

Si un hacker intercepta tu transacción, ¿crees que sea capaz de descifrar tu clave privada y robarte tus fondos? Es decir, suponiendo que una persona maliciosa tenga acceso a la dirección a la cual vas a enviar bitcoin, ¿crees que puede redirigirlo a su propia caja de seguridad?

Transacciones Válidas

El objetivo de una firma digital es poder demostrar que se es propietario de una clave pública.

- Los mineros verifican la firma con la clave pública del emisor.
- La verificación criptográfica es similar a:
  - -Evidenciar que la última pieza en un rompecabezas encaje correctamente.
  - –Si la transacción se modifica en lo más mínimo.
  - –El hash de la firma automáticamente cambia, haciéndola falsa y obsoleta.
  - -Es extremadamente fácil detectar las transacciones que se deben rechazar.

Sources

1. The Free Silver Movement, Scott Wolla, Federal Reserve Bank of St. Louis. https://www.stlouisfed.org/-/media/project/frbstl/stlouisfed/education/lessons/pdf/the-free-silver-movement-and-inflation.pdf,

2. Video -Econ Vids for Kids: What is Money? https://youtu.be/AjTwcQYgISA

3. https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/functions-and-characteristics-of-money-lesson.pdf, Functions and Characteristics of Money, Chapter 3, Segment 301, Federal Reserve Bank of Philadelphia

4. https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/money-grades-6-8.pdf, "Why Money", Bonnie T. Meszaros, Federal Reserve Bank of Philadelphia

5. https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf Federal Reserve Bank of Kansas

6. ¡Historia de 1870 a 1971 en 10 minutos!, Robert Breedlove. Para la sección de 1870-1914: https://www.forbes.com/sites/nathanlewis/2013/01/03/the-1870-1914-gold-standard-the-most-perfect-one-ever-created/?sh=5e0ab9864a6a

7. Economía Desde Cero: Dinero-Video, https://youtu.be/zcYw8a4RJC4, Canal Encuentro, Argentina.

8. https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf, Activity 5, Auction, Federal Reserve Bank of Kansas.

9. Video -Qué es la Inflación, https://youtu.be/gkDQGribCfc](https://youtu.be/gkDQGribCfc, Banco de la República de Colombia

10. Video - ¿Cómo Nos Vigilan en Internet?, Magic Markers https://youtu.be/-sWgOuFIaws](https://youtu.be/-sWgOuFIaws,

11 McDonalds Menú Picture 1973. https://muddyrivernews.com/opinion/daily-dirt-where-were-you-in-72-or-once-upon-a-time-when-a-big-mac-was-65-cents/20220323091958/

12. McDonalds Menú 2022. McDonalds El Salvador, Twitter.

13. Causas de la Inflación, Video, Banco de la República, Colombia.

14. Declining purchasing power of the US dollar strengthens Bitcoin, https://cryptopotato.com/is-there-a-pattern-between-usd-dow-jones-and-bitcoin/, Toju Ometoruwa.

15. Ejemplo de Estado de Cuentas, https://www.ejemplode.com/59-finanzas/4274-ejemplo_de_estado_de_cuenta.html

16. Video -MagicMarkers.TV,Colombia. ¿Qué es Bitcoin y Cómo Funciona?, https://youtu.be/S2HxMK7iO4c,

17. Nodos Completos -Visualización de una Transacción http://beautifuldata.net/2015/01/querying-the-bitcoin-blockchain-with-r/

18. Video -(https://youtu.be/lD8WQbS8-T8), *Que es La Red Relámpago*, Whiteboard Crypto en Español

19. Bitcoin en Números, Nick Carter, Bitcoin Demystified.

20. Bitcoin, Will the Price of Bitcoin Rise or Fall?, Capital.com Research Team, 08:00 (UTC), 31 March 2022. https://capital.com/de/bitcoin-prognose,

21. U.S. dollar inflation visualized at the top versus bitcoin's deflation at the bottom: Lark Davis @TheCryptoLark.

22. https://www.bitcoincharts.com

23. https://www.blockchaincenter.net/en/bitcoin-rainbow-chart/

24. https://www.blockchain.com/charts/miners-revenue

Mi
Primer
Bitcoin
EL SALVADOR