My First Bitcoin
EL SALVADOR

Bitcoin Diploma

Financial Education for the Bitcoin Era

Student Workbook

English Version | April 2023

Bitcoin Diploma

Financial Education for the Bitcoin Era

Student Workbook

English Version | April 2023

My First Bitcoin has created this work and made it freely available under **Creative Commons**.

This work is licensed under
Creative Commons
Attribution-ShareAlike
4.0 International (CC BY-SA 4.0)

DONATE NOW:

My First Bitcoin
EL SALVADOR

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.

Dalia Platt is the curriculum development lead and the driving force behind our content from the start. She is a rockstar. She has had great help for this edition from some amazing contributors, including Arel Edelkamp, Madelyn Hereford, Greg Foss, Ronny Avendano, Alejandro Galán, Evelyn Lemus, Gerardo Linares, Marc Platt, Jim Platt, Napoleón Osorio, Victor Yasbek, and Robert Malka. Gloriana Solano, Raul Guirola, Giacomo Zucco, Gerson Martinez, Vriti Saraf and others supported earlier editions. Gerardo Apostolo and Enrique Jubis, with ACTIVA, also contributed their incredible work.

The Bitcoin Diploma story began in February 2022 at a meeting at *La Pacheco*, a public school in San Marcos, El Salvador. Among those present were the school's innovative director, Asael Rodriguez, bitcoin education advocate and congressman, Rodrigo Ayala, and the community builder for Ibex Mercado, Carlos Toriello, who invited other Bitcoiners, myself included, to come tour the school and discuss education.

The first Bitcoin Diploma students began in April, with early support from Ibex as well as hundreds of individual donors. By June, the first group of 38 students graduated at *La Pacheco* and we began to expand. With tremendous support from new donors and sponsors, including Bitfinex, local mayors, and Bitcoin Beach, enrollment has continued to more than double in size every ten weeks, a trend which will allow us to reach thousands of students all over the country this year. In February 2023, delivery of the curriculum began in Guatemala with plans to bring it to many more nations before the year's end, including Colombia, Honduras, South Africa, Ecuador, and the United States. Donations from those programs will subsidize even more students in El Salvador.

The Bitcoin Diploma workbook has been made open source. It is freely available and has been translated, printed out, and independently taught to communities around the world, from South Korea to Uruguay.

Mi Primer Bitcoin is a non-profit with a singular mission—to provide quality, independent and impartial, community-based Bitcoin education to everyone in El Salvador as fast as possible. As the first nation to adopt Bitcoin, El Salvador will be an example to the world; we get to decide what sort of example that will be. Our vison is to teach a nation and change the world. I know that sounds crazy, but I think we are well 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

Chapter #1 - The Power of Money ***11***

1.0 Ready? 12
1.1 Class Discussion: What is Money? 12
1.2 The Limited World-Navigating Scarcity in a Growing Economy 13
1.3 Definition of Money 16
1.3.1 We Can Use It, but Can We Define It? 16
1.3.2 Functions of Money 18
1.3.3 Money Characteristics 19
1.3.4 Types of Money 22

Chapter #2 - From Barter to Bitcoin and CBDCs: A History of Money ***25***

2.0 Introduction 26
2.0.1 Class Exercise: Barter Game 26
2.1 Early Forms of Money 28
2.2 Commodities to I.O.U's 29
2.3 Transition from Sound Money to Unsound Money 30
2.4 Tracing the Evolution: From Plastic to Digital 33
2.5 The Rise of a Cashless Society 33

Chapter #3 - Discovering the Dark Side of Fiat ***39***

3.0 Drawbacks of the Fiat System 40
3.1 The Biggest Threats to Your Money: Inflation, Debasement, and Purchasing Power Loss 42
3.1.1 The Effects of Inflation: An Auction Activity 42
3.1.2 Saving Money In Hard Times 47
3.1.3 The Time Value of Money and Its Role in Economic Growth 48
3.2 Centralized Control: How the Government and Banks Manipulate the Money Supply 49
3.3 The Magic of Money Creation 50
3.3.1 Fractional Reserve Banking 50
3.3.2 Class Exercise: Fractional Reserve Banking 52
3.4 Debt: The Burden That Crushes the Middle and Lower Classes 54
3.5 Addressing Wealth Inequality: A New Approach to Money 55

Chapter #4 - The Future can be Decentralized: Empowering Communities and Individuals ***59***

4.0 The Price of Control: A Look at Surveillance, Censorship, and Regulation 60
4.0.1 Surveillance 60
4.0.2 Financial Regulations and Censorship 60
4.1 From Crisis to Innovation: The Cypherpunks and the Creation of a Decentralized Digital Currency 63
4.2 Abuse of Centralization 64
4.2.1 Centralized Sytems 64
4.2.2 The Intermediaries in a Credit Card Transaction 65
4.3 Overcoming Centralization with Decentralized Systems 67
4.3.1 Class Activity: Bank Transaction vs. Peer-Peer Transaction Simulation 68
4.4 Transactions are Just Agreements to Trade 69
4.4.1 To Trust or Not to Trust 70
4.4.2 Let's Swap Trust for Rules 71
4.5 Unlocking the Power of the Blockchain: A Technology Revolutionizing the Future 72
4.5.1 Class Activity: Consensus Building in a Peer-to-Peer Network 73
4.6 Emphasizing the Importance of True Decentralization in Blockchain Projects for Achieving Freedom and Empowerment 74

Chapter #5 - Unveiling the Future of Money: An Introduction to Bitcoin ***77***

5.0 The Enigma of Satoshi Nakamoto: A Glimpse into the Mind Behind Bitcoin and the Freedom Revolution 78
5.1 Introduction to Bitcoin and bitcoin 80
5.1.1 What is bitcoin? What is Bitcoin? 80
5.1.2 What is the difference between Bitcoin and bitcoin? 81
5.1.3 Why learn about bitcoin when I can't afford It? 81
5.1.4 What is bitcoin made of? 81
5.1.5 Why is bitcoin good money? 82
5.1.6 Why should I care? 82
5.1.7 How do you **use** bitcoin? 83
5.1.8 How do you **send** or **spend** bitcoin? 83
5.1.9 How do you **receive** bitcoin? 83
5.1.10 Can Bitcoin be shut down? 83
5.1.11 How does the blockchain keep track of who spends which bitcoin? 84
5.1.12 How do new bitcoin enter the network? 84
5.1.13 What is a bitcoin transaction? 84
5.1.14 Are bitcoin transactions secure? 86

5.2 Who's Who and What's What in the Bitcoin World? 89
5.3 Walk Me Through an Actual bitcoin Transaction 91
5.3.1 Class Exercise: Bitcoin Transactions in Action 95
5.4 What Gives bitcoin Its Value? 97

Chapter #6 - Bitcoin Wallets: Navigating Self-Custody and the Lightning Network for Secure Transactions ***101***
6.0 From Novice to Pro: Navigating the World of the Bitcoin Wallet 102
6.1 The Process of Onboarding and Securing your bitcoin 105
6.1.1 Class Exercise: Mastering Self-Custody and Using Your Wallet With Confidence 106
6.1.2 Class Exercise: How do I Receive bitcoin (in detail) 107
6.1.3 Class Exercise: How Do I Send bitcoin and Pay for Goods and Services (in detail) 107
6.2 On-Chain vs. Off-Chain 108
6.3 The Lightning Network 109
6.3.1 A Lightning Transaction 111
6.3.2 Class Exercise: Lightning Wallet Relay Race 114
6.3.3 Class Exercise: Lightning Online Interactive Demo 114

Chapter #7 - Unlocking the Secrets of Bitcoin's Inner Workings: The Math, Mempool, and UTXOs ***117***
7.0 Putting the Double Spend Issue to Rest: Understanding Bitcoin's Solution 119
7.1 Tracking Your Coin's Journey 121
7.2 Security and Secrecy 124
7.3 The "Mempool" or Memory Pool: Understanding the Holding Tank of Bitcoin Transactions 128
7.3.1 Class Exercise: On Hold: Examining the Unconfirmed Transactions of the Bitcoin Network 130
7.4 Behind the Blocks: The Mystery of Bitcoin Scripting 131
7.4.1 A Technical Dive into Bitcoin Transactions 133

Chapter #8 - Building the Chain of Security: Understanding the Process of Bitcoin Mining and its Role in the Blockchain ***137***
8.0 Uncovering the Gems of the Blockchain: Meet the Miners and the Mining Process 138
8.1 The Dynamic Rewards System of Bitcoin Mining: Block Rewards, Transaction Fees, and Halvings 138
8.2 The Vital Task of Bitcoin Mining: Securing the Blockchain 141
8.3 Dissecting the Block 144
8.4 Rehashing the Hashes-No Pun Intended 147
8.5 The Step-by-Step Process of Mining a Block 150
8.5.1 Class Exercise: Mining Interactive Exercise 152
8.5.2 Summary of the transaction from start to finish 153
8.5.3 Don't Trust, Verify 154
8.6 Class Exercise: Transaction with UTXO's 155

Chapter #9 - Why Bitcoin's Intrinsic Value Is Anything but Hollow ***159***
9.0 Why Bitcoin? 160
9.1 The Future of Bitcoin 160
9.1.1 The Lindy Effect 161
9.2 Using Bitcoin for More Than Just Digital Money 162
9.3 The Challenges 163
9.3.1 The Regulatory Environment for Bitcoin 163
9.3.2 Understanding the Energy Usage of Bitcoin Mining 164
9.4 The Risks 165
9.5 Trading and Investing in bitcoin 167

Chapter #10 - From Bits to Bitcoin: Piecing Together the Puzzle ***175***
10.0 Just Some Facts, a Few Jokes... and the Lingo 176
10.1 My First Bitcoin Final Project Submission and Evaluation Guidelines 178

Additional Resources ***181***

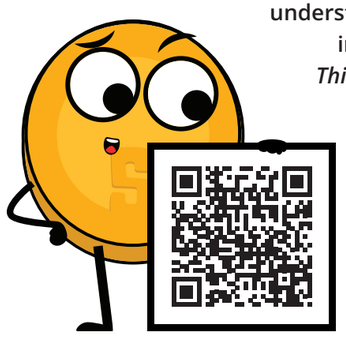
Glossary ***187***

Why Bitcoin?

Critical Thinking. Why is ***Bitcoin*** important to you and how do you think it will change humanity?

Bitcoin Diploma

A Ten Week Transformational Journey Through Independent, Impartial, Quality, and Free Education



Whatever **Bitcoin** may be; most people do not yet understand what this controversial and influential innovation is about and how it works.
This is a documentary that helps you answer those questions.

It is essential to have a firm grasp on the basics of money, its history, and the current financial system before studying ***Bitcoin***. Understanding these concepts provides a strong foundation for comprehending the unique and disruptive nature of ***Bitcoin***. By learning about the evolution of money, you will be able to better understand the potential and limitations of the current financial system and how ***Bitcoin*** aims to address them. Without this foundation, it may be challenging to fully appreciate the significance and potential impact of ***Bitcoin***. Trust the process of learning and stay focused, as the reward of a deeper understanding and appreciation of this cutting-edge field will be well worth it.

A Message from Our Founder

Chapter #1

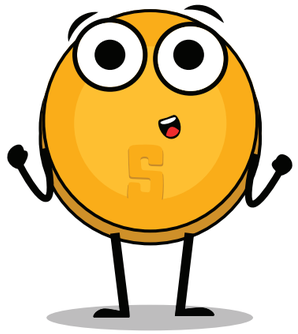
The Power of Money

1.0 Ready?
1.1 Class Discussion: What is Money?
1.2 The Limited World-Navigating Scarcity in a Growing Economy
1.3 Definition of Money
- **1.3.1** We Can Use It, but Can We Define It?
- **1.3.2** Functions of Money
- **1.3.3** Money Characteristics
- **1.3.4** Types of Money

1.0 Ready?

Bitcoin has been called many things - a fad, a scam, "magic internet money." But behind the hype, there is a powerful technology that has the potential to change the way we think about and use money; the potential to change the world in a way that "normal people" like you and me have the opportunity to build wealth, become truly free and live the lives we want to live. In this course, we will explore the flaws and limitations of our current financial system and how ***Bitcoin*** offers a potential solution. So, if you're ready to go beyond the headlines and learn about the real possibilities of ***Bitcoin***, let's dive in!

Hi! I'm Satoshi, an interactive assistant who will help you throughout the *Bitcoin Diploma*. I will give you data and recommendations to better understand.

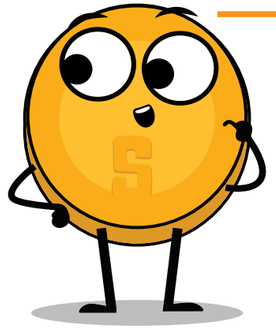


1.1 Class Discussion: What is Money?

- Please do not eat the piece of candy placed on your desk yet.
- Who would be willing to trade their candy for a US$1 bill?
- Now, keep your hands up if you would still be willing to do the trade your candy for a $1 monopoly bill instead for your piece of candy?
    - Why or why not?







The only difference between these two notes, is *your belief that one has more value than the other*.

- What makes one bill so desirable and another one as good as trash?
- What gives money it's "value"?
- Where does money come from and who decides how much of it to print?
- Why not print more money and distribute among everyone equally?
- Is money backed by gold? Or, by any other commodity?
- How many people still use cash anyways?

1.2 The Limited World: Navigating Scarcity in a Growing Economy

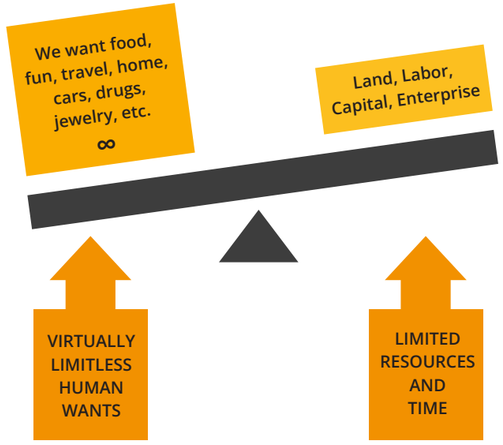
Imagine you are stranded in a desert and you only have one bottle of water left. You are thirsty and desperate for a drink, but you also know that you will need the water to survive until you can find more. This is a classic example of scarcity - you only have a limited amount of a resource (water) and you must make a choice about how to use it.

In this situation, you might decide to ration it and take small sips over a longer period of time, in order to make it last as long as possible. Alternatively, you might decide to drink as much as you can in one go, hoping that the burst of hydration will give you the energy you need to find more water. Regardless of which choice you make, you are faced with a difficult decision.

Scarcity forces us to weigh the pros and cons of how we use our resources and make trade-offs.

In this case, the choice is between quenching your *immediate* thirst and conserving the water for *later*.

This concept of *scarcity* applies to all kinds of resources, not just water. Whether it's money, time, or even love and attention, we are constantly faced with choices about how to allocate our limited resources.



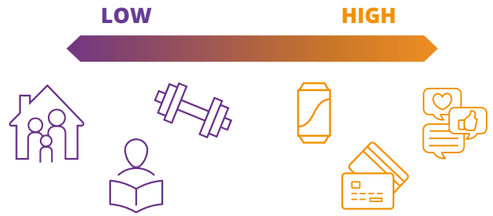
- There are two types of scarcity: **human-made scarcity** and **natural**.
    - **Human-made scarcity**, also known as *centralized scarcity*, includes things like limited edition designer bags, rare sports cards, and numbered art pieces. These can be easily replicated or counterfeited.
    - **Natural scarcity**, also known as *decentralized scarcity*, includes things like salt, shells, and precious metals like gold. These are harder to replicate or counterfeit.

- The main difference between the two is control. Centralized scarcity is controlled by a single entity, like a company or government, while decentralized scarcity is not controlled by anyone.
    - An example of centralized scarcity that disproportionately affects the poor is the control of essential resources like clean water. In some regions, access to clean water is managed by private companies or government entities that may limit its distribution, leading to a scarcity of this vital resource. This centralized control can result in price increases or unequal access to clean water, with

impoverished communities often bearing the brunt of the impact. Limited access to clean water not only affects their health and well-being but also perpetuates poverty as they may be forced to pay higher prices for water or travel long distances to obtain it.

Scarcity affects our choices. Understanding it can improve our decision-making. We often have to choose between immediate gains and long-term benefits, and these trade-offs shape our path to achieving our goals.

Time preference refers to the idea that people generally prefer to have something NOW rather than later.



- Another example: Let's say you have the option to receive $100 today or $110 in a year. If you have a high time preference, you might choose to receive the $100 today, because you value having the $100 now more than the benefits of waiting a year for the extra $10. On the other hand, if you have a low time preference, you'll prefer to wait for the larger reward, because you are more focused on long-term planning and less concerned with immediate gratification.

Class Activity. High Time Preference vs Low Time Preference

1. Listen to the teacher's explanation of the candy choice.
2. Decide whether you would like to receive a small candy or marshmallow now, or wait until the end of the class to receive two candies or a larger, more desirable candy.
3. Commit to your decision and let the teacher know your choice. Receive your candy either immediately or at the end of the class, based on your decision.
4. Participate in the class discussion about the activity, reflecting on your decision-making process and the concept of time preference.

Conclusion and Discussion:

- What factors influenced your decision to take the candy now or wait for a larger reward later?
- How do you feel about your decision now that the activity is over?
- Can you think of real-life examples where high time preference might be harmful and where low time preference might be beneficial?
- What are some potential consequences of choosing high time preference over low time preference?

- In the context of the desert example, this means that you might be more inclined to drink all of the water right away, even if it means that you won't have any left for later. This is because the thirst you feel right now is more pressing than the potential thirst you might feel in the future.
- On the other hand, if you choose to ration the water and drink it slowly over time, you are demonstrating a lower time preference. This means that you are willing to wait to satisfy your thirst and improve your chances of survival.

The concept of ***opportunity cost*** is closely related to the idea of **scarcity** and **time preference**.

Opportunity cost refers to the value of the next best alternative that you give up when you make a decision. **Every decision involves trade-offs:**



- In the desert example, the opportunity cost of drinking all of the water right away is the survival benefits you would have gained from rationing the water and using it over a longer period of time.
- Let's say that you decide to ration the water and take small sips over a longer period of time. As a result, you have the energy and hydration you need to search for more water.
- However, while you are searching, you come across a cactus that has a small amount of water inside. It's not a lot, but it's enough to quench your thirst for the moment. If you had decided to drink all of your water at once, you might not have had the energy to search for more water and come accoss the cactus. In this case, the **opportunity cost** of drinking all of your water at once would have been the chance to find the cactus and get more hydration.

This example illustrates how opportunity cost involves not just the immediate **trade-off** between two options, but also the potential future opportunities that may be gained or lost as a result of our choices. Our willingness to give up a larger reward in the future in exchange for a smaller reward now is influenced by our **time preference**, or how much we value immediate gratification versus long-term planning.

Corporations, Governments, and Societies also have to make choices.

CORPORATIONS	GOVERNMENTS / SOCIETIES
Firing 200 Employees vs. Freezing Wages	Building a New Highway vs. Increasing Teacher Salaries
Asking for a Loan vs. Bringing in more Shareholders	Funding Cancer Treatment Research vs. Clean Energy

1.3 Definition of Money

1.3.1 We Can Use It, but Can We Define It?



Have you ever stopped to think about what money really is? Ever even wonder what makes money, well, money? Most of us know how to use it, but not many of us understand where it comes from or how it works.

Money is essentially a way to exchange goods and services. It represents the value of these items in a form that can be easily traded.

This can take many different forms, such as paper notes, metal coins and electronic payments. Governments or other authorities typically issue and control money.

But money is so much more than just a physical or digital medium of exchange. It's like a universal language that allows us to trade with people all around the world, even if we don't speak the same language or have the same culture. For example, you can be on the other side of the world and still "speak" money by placing a product on the counter and exchanging it for the local currency or using a credit card. Money is like a social contract that allows us to make exchanges without having to rely on bartering or finding someone who specifically wants what we have to offer. If a group of people started accepting chocolate as payment for most goods and services, chocolate would become money. (Although, since it would melt in some parts of the world, we might consider it bad money.)

As French economist Jean Baptiste Say pointed out, "Money performs but a momentary function in an exchange; and when the **transaction** is finally closed, it will always be found that one kind of commodity has been exchanged for another."

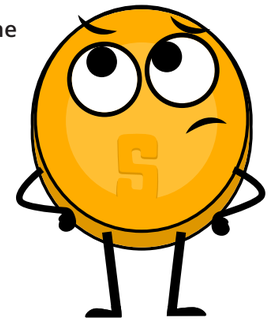
In other words, money itself doesn't have the power to satisfy human wants. It's just a tool that allows us to trade one commodity for another.



Without money, how easy or feasible would this trade be?

Would you trade one cow for 1,000,000 strawberries?

Or is it 600,000 strawberries? How about 50,000?



Transaction is an exchange or transfer of goods and services. It is a way of exchanging value between two or more parties.

There are many different types of transactions, ranging from simple exchanges (such as buying a sandwich at a deli) to more complex financial transactions (such as buying a house or investing in stocks or bonds). Transactions can be conducted in person, over the phone, online, or through other means, and they can involve a wide range of parties, including individuals, businesses, and financial institutions.

Money **IS** the value **BY** which goods are exchanged.

Money **IS NOT** the value **FOR** which goods are exchanged.

In summary, **money**:

- **Facilitates trade** because **everyone accepts it as final payment.**
- Allows us to **measure** the **value** and to **make comparisons** between different goods and services.
- Lowers our time preference, as it allows us to **save** and **spend it in the future**.

Check out this short video!



1.3.2 Functions of Money

When it comes to buying and selling goods and services, money is the key player. It has several important jobs, like:

- **Making exchanges easier**: With money, you don't have to find someone who wants exactly what you have to trade. Instead, you can use money to buy and sell anything you want.This makes trading and commerce much more convenient and efficient.

Medium of Exchange



- **Being a unit of account**: Money provides a universal standard of value that allows people to express and compare the price of different goods and services. This allows for a more efficient and transparent market, where people can make informed decisions about what to buy and sell.
  - Think of it like this: if you wanted to buy a new car, you could compare prices from different dealerships and make an informed decision about which one to buy based on the price in dollars. Without a unit of account, you'd have to try to compare the value of one car to another using something else, like the number of cows it was worth or the length of time it took to make the car.



Unit of Account

Consumers know the value of something when you assign a price (monetary value) to it.

$29.00 ***$129.00***



- **Being a store of value**: Money should maintain its value over time, making it useful as a way to save and invest the value of human labor. This lets people use money to plan for the future and to borrow and lend money.

What's your store of value?

	BTC (USD)	Gold (USD)	USD (EUR)	ETH (USD)
March 14, 2019	$3,846	$1,293	€0.8817	$136.86
March 14, 2020	$5,258	$1,529	€0.90056	$127.76
Gain/Loss	+36.71%	+18.25%	+2.14%	-6.65%

So next time you're saving up for something special, remember that money is more than just a way to pay for things - it's a tool to help you plan and invest in your future.

These three functions are what allow economies to become complex and dynamic. Without money, it would be much harder to buy and sell goods and services, and our economy would be much less developed.

Class Exercise. What function of money is this an example of?

1. Roby decided to save a portion of his weekly paychecks to buy a puppy. _____
2. Jim buys two slices of pizza for $8.30 at Ray's Pizza. _____
3. Marc can't decide whether to buy concert tickets for $75 or buy a ski pass for $95. _____

1.3.3 Money Characteristics

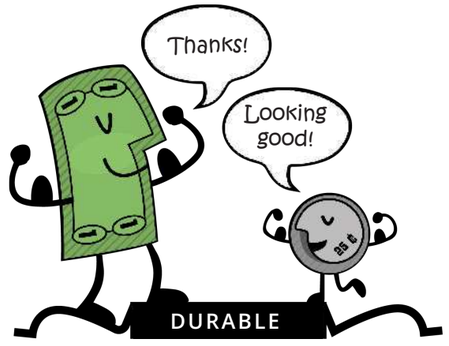
Over time, people ultimately have realized that money must possess certain qualities in order to be effective as a medium of exchange. These characteristics include durability, portability, divisibility, fungibility, scarcity, and acceptability.

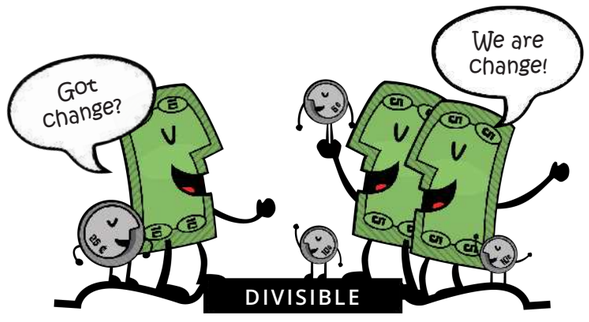
- ***Durability*** refers to the ability of money to resist physical deterioration and last over time. This ensures that money can circulate in the economy in an acceptable and recognizable state.

Gold is a durable material that can withstand wear and tear, making it a good representation of the durability characteristic of money.

- ***Divisibility*** refers to the ability of money to be divided into smaller units, so that people can use it to make purchases of varying amounts.

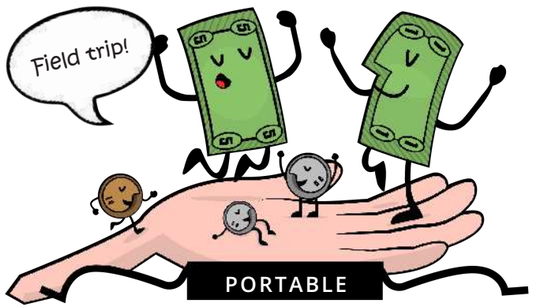
Paper bills can be easily divided into smaller denominations, making them a good representation of the divisibility characteristic of money.





- ***Portability*** refers to the ease with which money can be transported and carried around. This allows people to use money to buy and sell goods and services without difficulty.

Credit cards are portable, as they can easily be carried in a wallet or purse, making them a good representation of the portability characteristic of money.



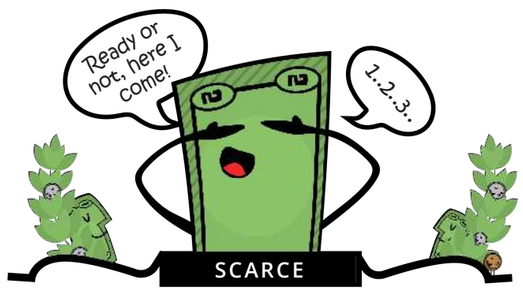
- ***Acceptability*** refers to the widespread acceptance of money as a form of payment, so that people can use it to buy and sell goods and services with confidence.

The US dollar is widely accepted as a form of payment, making it a good representation of the acceptability characteristic of money.



- ***Scarcity*** refers to the limited supply of money, which helps to maintain its value and prevent us from having to spend more money to buy the same amount of goods.

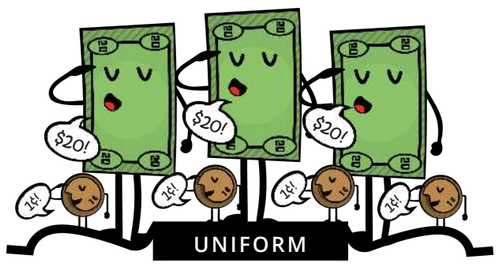
Collectible stamps, especially rare and valuable ones, can be a good form of money because they are scarce and can appreciate in value over time. Stamp collectors often use their stamps as a way to invest their wealth and to diversify their portfolio.



- ***Fungibility*** refers to the interchangeability of money, so that one unit of money is equivalent to another unit of the same value.

Money should be **uniform**.

Copper coins are uniform in size and weight, making them a good representation of the uniformity characteristic of money.



Overall, these characteristics make money a useful and effective tool for facilitating trade and commerce, and they are essential for the development and stability of economies.

Class Exercise. Different assets have different properties and perform the functions of money to varying degrees. Society ultimately determines which asset is used as money based on factors such as its stability, scarcity, divisibility, transferability, and acceptance as a medium of exchange.

To determine how well different items meet the specific characteristics of money, you can score each item on a scale from 1 to 5 for each characteristic. By tallying up the scores for each item, you can determine which one is best suited to be a form of money.

[0 = Terrible; 3 = Okay; 5 = Excellent]

*** Please do not fill in the column for *Bitcoin*; we will return to it later in the course.**

Use the following questions to help you determine how well the different items in the table meet the characteristics of money.



- ***Durability***: Can the money withstand wear and tear over time?
- ***Fungibility***: Is the money interchangeable with other forms of money?
- ***Acceptability***: Is the money widely accepted as a form of payment?
- ***Scarcity***: Is the money scarce and not too abundant?
- ***Portability***: Can the money be easily transported and used in different locations?
- ***Divisibility***: Can the money be divided into smaller units for transactions?

Characteristic of Good Money	Cows	Cigarettes	Dimonds	Euros	Bitcoin
DURABLE					
PORTABLE					
UNIFORM					
ACCEPTABLE					
SCARCE					
DIVISIBLE					
TOTAL					

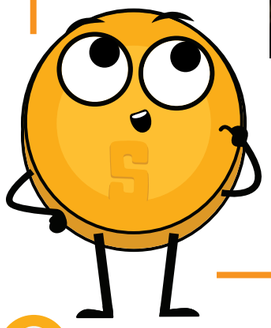
1.3.4 Types of Money

Money can be divided into two main categories: **physical and digital**.

Physical money includes:

- **Fiat money,** which is the paper bills and coins issued by governments and accepted as a medium of exchange.
- **Representative money,** which represents a claim on a physical commodity.
- **Commodity money,** which is a physical object that has intrinsic value and is widely accepted as a medium of exchange. For example, gold and silver.

Not all money is the same!



Commodity Money



Objects like this gun powder once served as commodity money.

Representative Money



Representative Money like this silver certificate could be exchanged for silver.

Fiat Money

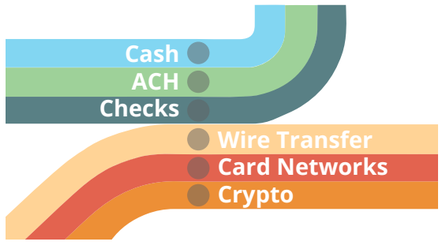


Today, Federal Reserve notes are fiat money, decreed by the federal government to be an acceptable way to pay debts.

Digital currencies, on the other hand, can be used for online transactions and include electronic currencies, stablecoins, and cryptocurrencies.

Electronic currencies are digital versions of regular money, like dollars or euros, and can be used to buy and sell things online via digital **payment rails**.

Payment rails are the infrastructure that enables the movement of electronic currencies and other digital assets from one place to another. However, in the traditional financial system, there is always a middleman, such as a bank or financial institution, that charges a fee and has the authority to accept, cancel, revert, or delay transactions.



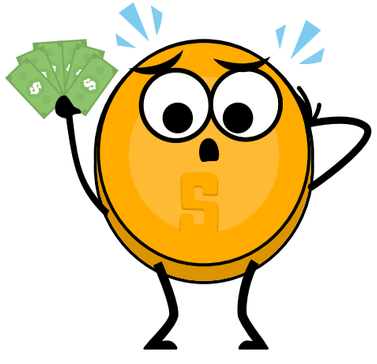
In the intermediated financial system, the main types of digital payment rails include card networks, which facilitate the transfer of funds between financial institutions and merchants when a customer makes a purchase using a debit or credit card, and digital wallets, which are online accounts that allow users to store and manage their electronic currencies and make payments by transferring funds from their account to the recipient's account.

Central Bank Digital Currencies (CBDCs): are digital versions of a country's fiat currency, which are issued and backed by the central bank and intermediated by the government. CBDCs are not cryptocurrencies, as they are issued by a central authority and do not use decentralized payment rails.

Stablecoins are cryptocurrencies that are designed to maintain a stable value relative to an asset, like the US dollar. Some stablecoins are intermediated, meaning they require a middleman like a bank to operate, while others are decentralized and do not require intermediaries.

Cryptocurrencies are a type of digital currency that use decentralized payment rails to move from one place to another online. They can be transferred and exchanged directly, without the need for a middleman like a bank. Cryptocurrencies are not intermediated, meaning they do not require a central authority or intermediary to operate.

Ultimately, a currency that operates without intermediaries is more efficient and beneficial for society, as it prevents a few individuals from controlling the money supply and concentrating their power. However, creating such a currency that facilitates secure transactions without relying on trust between parties has been a challenge throughout history. To achieve this, a currency must be created that operates like the internet, where control is distributed among everyone and no one at the same time. This requires the agreement of all parties, including those who hold power, to relinquish control for the greater good.



Chapter #2

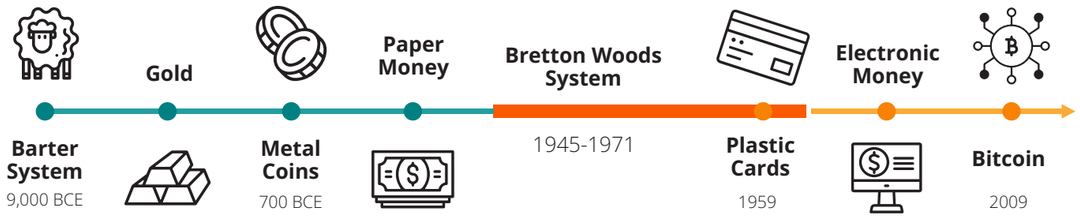
From Barter to Bitcoin and CBDCs: A Travel Through Time

2.0 Introduction
    2.0.1 Class Exercise: Barter Game
2.1 Early Forms of Money
2.2 Commodities to I.O.U's
2.3 Transition from Sound Money to Unsound Money
2.4 Tracing the Evolution: From Plastic to Digital
2.5 The Rise of a Cashless Society

2.0 Introduction

The concept of money has evolved over time. In its early forms, money was used to facilitate trade and exchange of goods and services.

- In ancient civilizations, people relied on bartering, a system of direct exchange of goods and services without the use of a medium of exchange.
- Later, metal coins and paper currency were introduced as more convenient forms of money, paving the way for the sophisticated financial systems we have today.



In this chapter, we will embark on a journey through time, experiencing the evolution of money firsthand. We'll trace its origins and observe how it has changed and adapted through history.

2.0.1 Class Exercise: Barter Game

Your teacher has given you a small piece of paper. Your goal is to trade what you "have" with what you "want" in a game of commerce throughout history. Please write your name on the top of the paper in small legible letters.

Round #1- Barter

It is the year 6000 B.C.E. Needless to say, money as we know it has not been invented. You are in Mesopotamia and directly exchange goods and services with one another through **bartering**.

As a side-note, many businesses still accept non-monetary payments for their services, and governments treat these bartered transactions the same as currency transactions for tax-reporting purposes.

Cut your sheet of paper at the dashed line. Your goal is to trade away your "have" as many times as you need to finally get your original "want". You cannot change your original "want". You will have 5 minutes to accomplish the goal of this exercise.

When your new "have" matches your original "want", return to your seat. After the time is up, if you have not found a trading partner, return to your seat anyway.

Raise your hand if you were able to get what you wanted after one trade. Two? Three?

Questions. Answer the following questions briefly but substantially.

1. Why were some of you able to get someone to trade with and others were not?

2. What are the benefits of barter?

3. Based on your experience with this exercise, what are the drawbacks to using barter?

Round #2- Commodity Money

Fast forward and travel to the western coast of Africa sometime around the 14th century BCE. Bartering has become tedious and inefficient. We have evolved as a civilization and are now using **commodity money**.

Cowry Shells to Coins



FUN FACT
Cowry shells were accepted as legal tender in some parts of Africa until the 20th century.

These proto-coins were oval-shaped, made from "electrum" (a gold/silver alloy), and had a design on one side only.

1,300 BCE
Cowry shells are the predominant form of payment in most of Asia, Africa, Oceania, and some parts of Europe.

1,000 BCE
China's Western Zhou dynasty begins using metal coins.

687 BCE
King Alyattes of Lydia (present-day Turkey) orders the first metal coins to be minted in the Western world.

Your teacher has given you one macaroni (for simplicity purposes). Let's assume that by convention, the price of each good is worth one macaroni. Your goal again is to obtain what you "want". But now, our species has smartened up a bit and found a way to solve certain problems.

- Why do we consider macaroni commodity money?
- How do we get the things we want now?
- Was the macaroni round easier?
- Why do you think money has replaced commodities?
- In what ways is using commodity money more efficient than bartering?
- What are the drawbacks to using macaroni as money?

What do you think happened when Spain started to bring back boatloads of macaroni into your community (gold and silver from the Americas back to Spain)?

2.1 Early Forms of Money



Watch this short video to learn about the Origins of Exchange, in the series "The History of Paper Money."

In **barter economies**, people trade with each other based on the relative value of the goods and services that they have to offer. **Barter economies** are *inefficient* and can be difficult to manage, especially in complex societies.

A situation, known as the **double coincidence of wants**, is necessary in any bartering system since people must always find someone who has what they want but also wants what they have to offer.



I'll give you shoes for your wheat.

I don't need shoes. I need clothes.

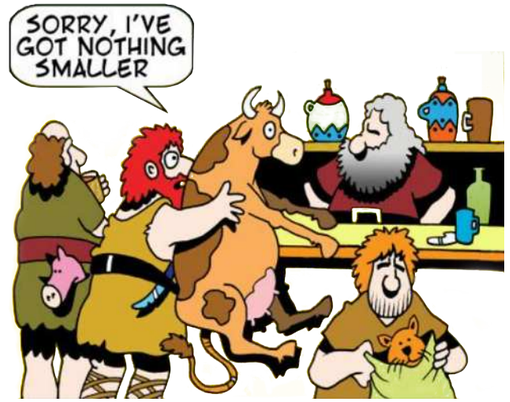
I want shoes but I don't have wheat.

Let's suppose:

- Joseph wants to trade his banana for Yael's coconut.
- But Yael only wants to trade her coconut for Tammy's mango.
- And Tammy only wants to trade her mango for Joseph's banana.
- They are stuck in a never-ending cycle of fruit trading without a double coincidence of wants.
- Joseph suggests they just trade their fruits for a nice cold soda, but they realize they are on a remote island and there is no soda.
- They decide to just sit on the beach and enjoy their fruits in silence.

Using a **common unit of account**, such as a "soda", makes trade and commerce much more efficient. In ancient times people began by using beads, shells, and other items that had value in their society as **mediums of exchange**.

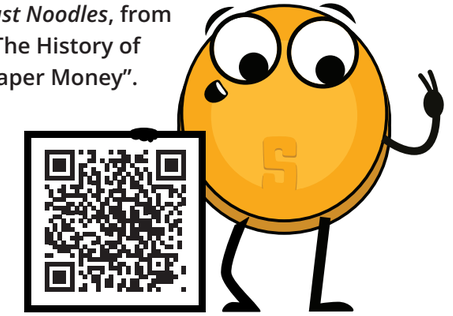
Why Money was Invented



2.2 From Commodities to I.O.U's

As you and your community become more involved in trade and commerce, you realize the limitations of using bartering and other forms of non-monetary exchange. You decide to adopt the use of **metal coins as a form of money**.

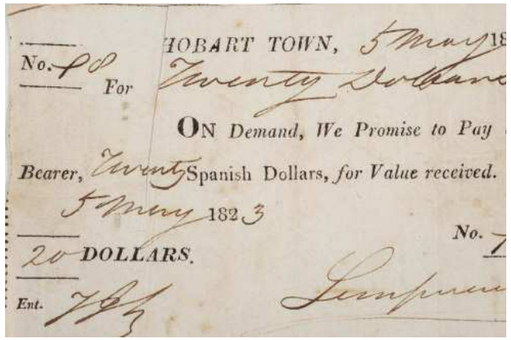
This is the second episode, called *Not Just Noodles*, from "The History of Paper Money".



These metal coins are made of valuable materials like gold and silver, and they serve as a medium of exchange and unit of account to facilitate trade and commerce: **commodity money.**

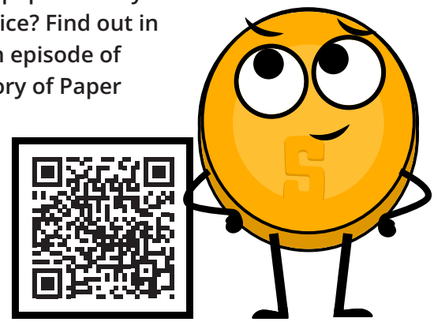
However, as you ***begin to use metal coins more frequently***, you encounter some drawbacks. They can be heavy and inconvenient to carry in large transactions, and you notice that some people are taking advantage of the system by melting down the coins and creating new ones by mixing them with cheaper metals, which causes prices to rise and undermines trust in the system.

In an effort to address these issues, you and your community start to use paper receipts as a form of money. These paper receipts, which have their origins in ancient China, are a convenient and easily exchangeable form of currency. They are backed by gold and other valuable metals, and can be converted into these metals during the seventeenth through the nineteenth century. This allows you to have a more portable and easily transferable form of money, while still maintaining the value and security of precious metals.



2.3 Transition from Sound Money to Unsound Money

What happens when you really try to put paper money doctrine into practice? Find out in the fourth episode of "The History of Paper Money".



Fast forward to the 17th century in Sweden. Now you are completely dependent on banks to store your valuable assets. However, you start to notice something fishy going on with these bankers. It seems they are issuing more paper receipts than they have gold in storage, allowing them to create more money than they have assets to back it up. This sneaky practice allows the bankers to profit from the difference between the value of the paper receipts and the value of the gold they are holding for their customers.



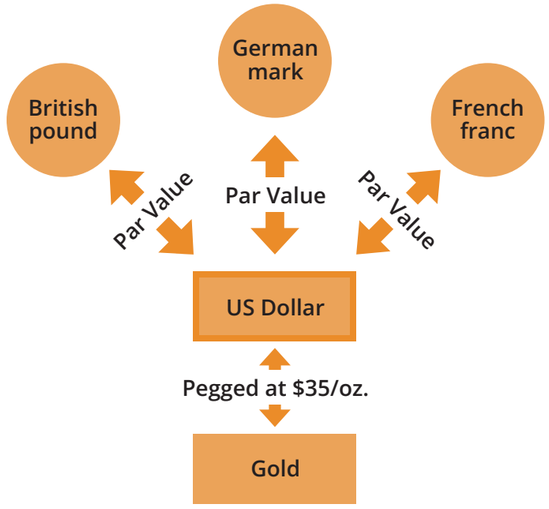


You realize that this marks a major shift in the way money works. You are moving from a system of sound money (i.e. money backed by precious metals) to a system of unsound money (i.e. fiat currency not backed by a physical commodity). This transition didn't happen overnight, but rather was a gradual process influenced by several factors. The Industrial Revolution, with its mass production and urbanization, played a role, as did the growth of advanced financial systems like banks and stock markets. The emergence of central banks and other monetary authorities contributed to the centralization or the control of money, leading to the issuance of fiat currencies to support economic growth.

However, you also begin to see the **downsides of this centralization**, including irresponsible consumption, an **increase in debt**, and manipulation of citizens through economic incentives.

Until World War I, you were able to convert your paper money into a preset amount of gold. But the two world wars and the 1929 economic crisis put an end to that. In 1944, the Bretton Woods agreement is signed, establishing the U.S. dollar as the world's reserve currency and fixing the value of the U.S. dollar to the price of gold at a rate of $35 per ounce. Other countries' currencies are pegged to the dollar, which helps to stabilize international financial markets.

Bretton Woods System
(1945-1972)



Unfortunately, the system begins to break down in the late 1960s, leading to the Nixon Shock in 1971, when the U.S. government suspends the convertibility of the dollar into gold. This marks the end of the gold standard and the beginning of a world driven by the creation and accumulation of debt.

As you go about your daily life, you begin to notice that the value of money is no longer as stable as it used to be. Just like a flexible ruler makes it difficult to accurately measure the length of a table, living in a fiat world where the value of money is subject to the unpredictability of those in power can also make it difficult to accurately measure the value of goods and services. You feel confusion and unease adjusting to a world where the value of money is no longer tied to a physical commodity like gold.

You see the impacts of this shift on the global economy and start to question the stability and reliability of fiat currencies. You realize that in this modern world, the dollar is no longer fixed and consistent as it was when it was pegged to gold, but instead becomes subject to fluctuation. This makes it more difficult to use the dollar as a unit of account, as its value is affected by various factors including inflation (rising prices), interest rates, the strength of the country's economy, political events, market speculation, and demand in international trade. It can be a confusing and unpredictable time, as you try to navigate the constantly shifting value of the dollar and its impact on your daily life.

Despite efforts to improve quality of life through modern monetary systems, increased efficiency, greater access to information, and enhanced communication, the majority of people's standards of living begin to decline due to:

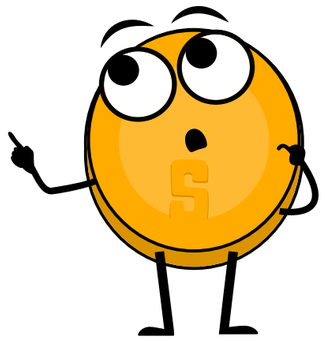
- Abuse of centralization.
- Rising prices.
- Stagnated real wages.
- Weakening currencies.
- The need to spend more money for fewer things.



This has challenges for those with lower economic resources, who may have limited access to education, credit, resources, social networks, and political representation, leading to potential disadvantages in their ability to succeed.

As a result, the rich seem to keep getting richer and the poor seem to keep getting poorer.

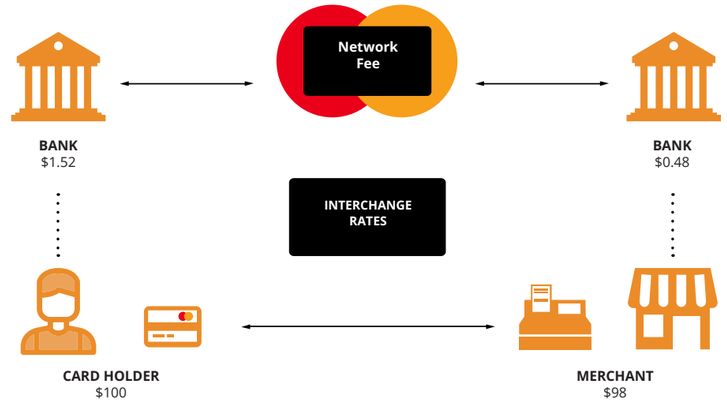
> *"I don't believe we shall ever have good money again until we take the thing out of the hands of government... all we can do, is by some sly, roundabout way, introduce something that they can't stop."*
>
> ***Friedrich Hayek***,
> Nobel Prize Winner of Economics



2.4 Tracing the Evolution: From Plastic to Digital

Today, we've come a long way from the introduction of the first credit card back in the 1950s. With a simple swipe of plastic, we can buy whatever we want, whenever we want, without any hassle. It's like opening up a world of endless possibilities, and the excitement of discovering what it holds is palpable...or so we thought. Little did we know that our reliance on credit would have painful aftereffects — like raising the overall cost of goods, and incentivizing a certain economy doomed to fail.

As technology advances, so does the way we handle money. The internet becomes a major player in the financial world, with online banking and e-commerce websites making it possible to manage and spend money entirely online.



Then, in 2009, the first decentralized cryptocurrency, ***bitcoin***, is created. As its popularity grows, it inspires the creation of new technologies and unknown frontiers for the future of money. And so, as we'll learn, we've come full circle from sound money to unsound money and back again, sound money finding new wind in its sails for the first time in almost a hundred years.

2.5 The Rise of a Cashless Society

When the first credit card was introduced in the 1950's and people rejoiced at the thought of never having to carry around actual cash again. No more fumbling for loose change or awkward check-writing moments at the checkout counter. All those pesky intermediaries can now take their cut without you even realizing it, just like a toll on a network. Ah, the convenience of modern finance.

But with the rise of digital currencies like CBDCs, it's like we've gone from paying a fee for using the network to having to ask permission. Worse, now we expect to be searched, scanned, and

scrutinized by the government every time we pass through. Control and surveillance has taken the place of convenience. And just like the fee from the network, these intrusions into our financial lives come with a cost, whether it's monetary, a violation of privacy, or the loss of autonomy.

The question is, are we willing to pay the price for the convenience of modern finance, or will we seek out alternative options that prioritize our freedom and privacy?

As more of our daily transactions move online, the use of cash declines. Governments and financial institutions around the world are promoting the use of electronic payments and cracking down on the use of physical money. This trend has sparked a debate about the future of cash and the potential consequences of a cashless society.

In this infographic, we will provide an overview of the war on cash and explore all sides of the debate. We will look at the reasons behind the push for a cashless society, the challenges and concerns that it raises, and the potential impacts on individuals, businesses, and society as a whole.

The **war on cash** is a term that refers to the various efforts to reduce the use of physical money, remove high-denomination bills and promote the use of electronic payments.

Proponents of the war on cash argue that it will make transactions faster, more convenient, and more secure. Critics, however, fear that it could lead to a loss of privacy and financial inclusion and increased risks of fraud and cyber-attacks.

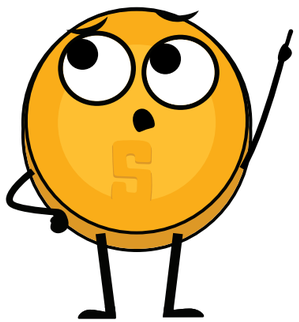
Q: How do traditional banking methods put individuals' financial data at risk?

A: With credit cards, debit cards, wire transfers, and other centrally controlled payment networks, individuals are giving their private financial transaction data to a third party and potentially sacrificing their rights to privacy.

The Global War on Cash

There is a global push by lawmakers to eliminate the use of physical cash around the world. This movement is often referred to as "***The War on Cash***", and there are three major players involved:

- The Initiators
- The Enemy
- The Crossfire



Desjardins, Jeff. "The Global War on Cash." Visual Capitalist, 27 Jan. 2017, https://www.visualcapitalist.com/global-war-cash/.



WHO?
Governments, central banks

WHY? The elimination of cash will make it easier to track all types of transactions, including those made by criminals.



WHO?
Criminals, terrorists

WHY? Large denominations of banknotes make illegal transactions easier to perform, and increase anonymity.

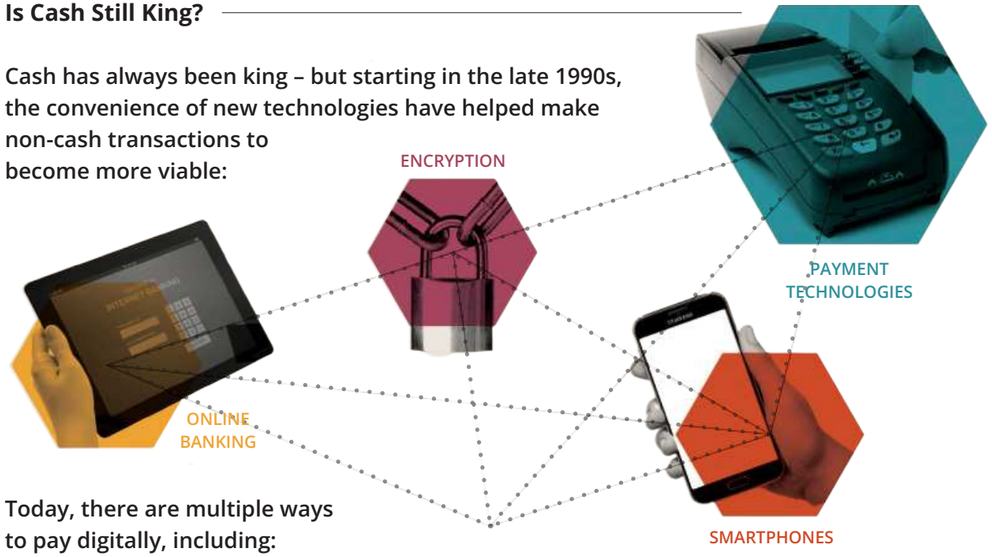


WHO?
Citizens

WHY? The coercive elimination of physical cash will have potential repercussions on the economy and social liberties.

Is Cash Still King?

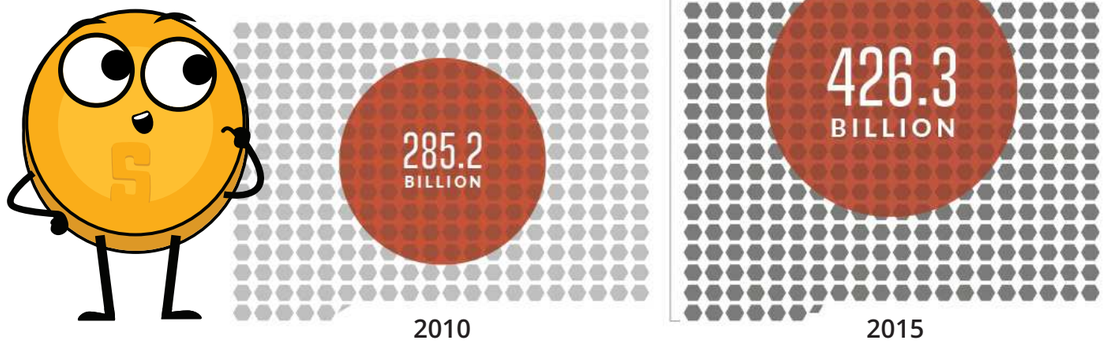
Cash has always been king – but starting in the late 1990s, the convenience of new technologies have helped make non-cash transactions to become more viable:



Today, there are multiple ways to pay digitally, including:



By 2015, there were 426 billion cashless transactions worldwide - a 50% increase from five years before.



The First Shots Fired



The success of these new technologies has prompted lawmakers to posit that all transaction should be now digital. **Here is their case for a cashless society:**

Removing high denominations of bills from circulation makes it harder for terrorists, drug dealers, money launderers, and tax evaders.

1

- $1 million in $100 bills weighs only ten kilograms (22lbs).
- Criminals move $2 trillion per year around the world each year.
- The U.S. $100 bill is the most popular note in the world, with 10 billion of them in circulation.

2

- Money that is traceable means higher tax revenues.
- It also means there is a third-party involved with all transactions.
- Central banks can dictate interest rates that encourage (or discourage) spending to try to manage inflation. This includes ZIRP or NIRP policies.

This gives regulators more control over the economy.

Cashless transactions are faster and more efficient.

3

- Banks would incur less costs by not having to handle cash.
- It also makes compliance and reporting easier.
- The "burden" of cash can be up to 1.5% of GDP, according to some experts.

For this to be possible, they say that cash, especially large denomination bills, must be eliminated.



After all, cash is still used for about 85% of all transactions worldwide.

Caught in the Crossfire

The shots fired by governments fighting the war on cash may have several unintended casualties.



- Cashless transactions would always include some intermediary or third party.
- Increased government access to personal transactions and records.
- Certain types of transactions (gambling, etc.) could be barred or frozen by governments.
- Decentralized cryptocurrency could be an alternative for such transactions.



- Savers could no longer have the individual freedom to store wealth "outside" of the system.
- Eliminating cash makes negative interest rates (NIRP) a feasible option for policymakers.
- A cashless society also means all savers would be "on the hook" for bank bail-in scenarios.
- Savers would have limited abilities to react to extreme monetary events like deflation or inflation.



- Rapid demonetization has violated people's rights to life and food.
- In India, removing the 500 and 1,000 rupee notes has caused multiple human tragedies, including patients being denied treatment and people not being able to afford food.
- Demonetization also hurts people and small businesses that make their livelihoods in the informal sectors of the economy.



- With all wealth stored digitally, the potential risk and impact of cybercrime increases.
- Hacking or identity theft could destroy people's life savings.
- The cost of online data breaches is reached $2.1 trillion by 2019, according to Juniper Research.

Chapter #3

Discovering the Dark Side of Fiat

3.0 Drawbacks of the Fiat System
3.1 The Greatest Threats to Your Money: Inflation, Debasement, and the Loss of Purchasing Power
- **3.1.1** The Effects of Inflation: An Auction Activity
- **3.1.2** Saving Money In Hard Times
- **3.1.3** The Time Value of Money and Its Role in Economic Growth

3.2 Centralized Control: How the Government and Banks Manipulate the Money Supply
3.3 The Magic of Money Creation
- **3.3.1** Fractional Reserve Banking
- **3.3.2** Class Exercise: Fractional Reserve Banking

3.4 Debt: The Burden That Crushes the Middle and Lower Classes
3.5 Addressing Wealth Inequality: A New Approach to Money

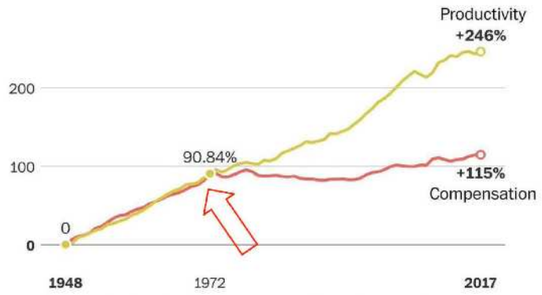
3.0 Drawbacks of the Fiat System

In this chapter, we will explore the drawbacks of the traditional fiat system and how it benefits those in power at the expense of the majority.

The fiat system is a monetary system that is based on government-issued currency that is not backed by a physical commodity like gold or silver. Instead, the value of fiat currency is based on the faith and credit of the government that issued it.

Although the fiat system has its benefits, such as stability and flexibility, it also has significant drawbacks. One of the most significant of these is the way it perpetuates power dynamics and wealth inequality.

Growth in Productivity and Hourly Compensation (1948-2017)



NOTE: Compensation includes wages and benefits for production and non-supervisory workers.

History often echoes through time, revealing patterns that are strikingly familiar.

For instance, during the 2008 financial crisis, the US government bailed out large corporations such as AIG, Citigroup, and Bank of America. These bailouts were paid for with taxpayer money, but they disproportionately protected the interests of the wealthy while leaving ordinary citizens to bear the burden of economic hardship. In fact, a study by the Congressional Budget Office found that the top 1% of income earners received 95% of the income gains from the recovery after the 2008 crisis, while the bottom 90% of income earners experienced a decline in their income.

Furthermore, the manipulation of the money supply by governments and central banks can exacerbate the problem of wealth inequality. **Inflation** and **debasement** of currency pose significant threats to the value of money in a fiat system, often disproportionately affecting the middle and lower classes.

Inflation occurs when the general level of prices of goods and services in an economy increases over time. It reflects a reduction in the **purchasing power** of money and results in a loss of real value in the medium of exchange and unit of account within an economy.

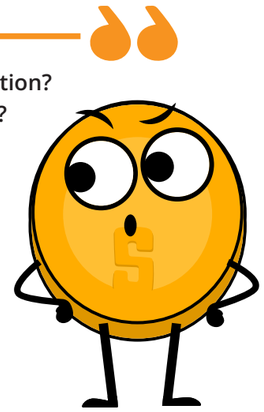


Purchasing power refers to the amount of goods or services that can be purchased with a certain amount of money. In other words, it's a measure of how much you can buy with your money.

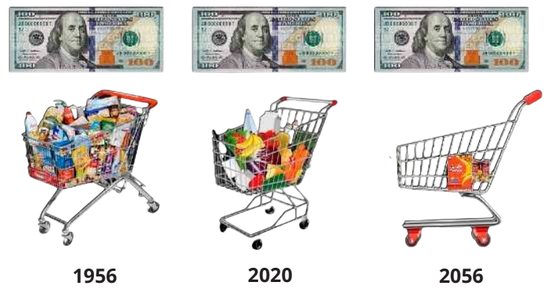
- For example, if you have $100 and the price of a loaf of bread is $2, you can purchase 50 loaves of bread with your money. However, if inflation occurs and the price of bread increases to $4, your purchasing power decreases and you can only purchase 25 loaves of bread with your $100.

In addition, **debasement** of currency occurs when the government reduces the value of its currency by increasing the money supply or decreasing the quality of the currency.

So what exactly is inflation? Why is it so dangerous? Steve Forbes breaks it down.



To better illustrate the impact of inflation and debasement on the middle and lower classes, let's look at some statistics. According to a report by the Economic Policy Institute, the top 1% of income earners in the US have seen their income grow by 205% since 1979, while the bottom 90% have seen their income grow by only 62%. This means that the rich are getting richer while the poor are getting poorer. Inflation and debasement only serve to exacerbate this problem by decreasing the purchasing power of the middle and lower classes, who are already struggling to make ends meet.



1956 **2020** **2056**

In addition to wealth inequality, the fiat system can also perpetuate power dynamics by giving governments and central banks control over the money supply. This control can be abused to benefit those in power at the expense of the majority. For example, the government and central bank can manipulate interest rates to favor certain groups or industries over others. They can also use monetary policy to stimulate economic growth or control inflation, but these policies can have unintended consequences that disproportionately

affect the middle and lower classes.

Furthermore, the fiat system allows for the accumulation of debt on a massive scale. Governments and corporations can borrow money with relative ease, but this debt must be paid back with interest. This interest can become a significant burden on the economy and future generations, who may be left to bear the consequences of decisions made by their predecessors.

While the fiat system has its benefits, it is important to recognize its drawbacks and consider alternatives like Bitcoin. By understanding the power dynamics and wealth inequality perpetuated by the fiat system, we can work towards creating a more equitable and transparent financial system for all.

3.1 The Biggest Threats to Your Money: Inflation, Debasement, and the Loss of Purchasing Power

3.1.1 The Effects of Inflation: An Auction Activity

Objective: To understand the concept of the **money supply** and how it affects the prices of goods and services in an economy.

Definitions:

- The **money supply** is the total amount of money in circulation within an economy at a specific time. This includes:
  - Physical currency, such as coins and bills
  - Electronic money held in bank accounts
    + The money supply is an important concept in economics, as it can affect the overall health of an economy.
- **Auction**: A public sale in which goods or property are sold to the highest bidder.

Class Exercise. Follow the instructions below:

1. You will receive a random amount of monopoly money from the teacher. This represents the money supply in a society.
2. Write down the total money supply in the chart provided.
3. The teacher will auction a candy bar to the students. To win the candy bar, you will need to make the highest bid using your monopoly money. Record the winning bid next to the money supply.
4. The teacher will then add a significant amount of monopoly money to the total money supply. This represents an increase in the money supply in an economy. Later, you will learn how money supply is added or reduced in an economy.

Societies can often be unpredictable and unjust, exemplified by the simulation of a teacher randomly giving a significant amount of money to only a select few students. This mimics real-life situations where unequal distribution of resources and opportunities can occur, highlighting the inherent randomness and unfairness in many situations.

5. The teacher will auction a second candy bar to the students using the same process as before. Record the winning bid next to the money supply on the chart.
6. The teacher will repeat the auction a third time.

Round	Money Supply	Winning Bid
1		
2		
3		

Conclusion:
1. How did the increase in the money supply affect the winning bids for the candy bars?
2. What is the relationship between the money supply and inflation?
3. How is the money supply relevant in the real world?
4. Can you think of any other factors that can affect the prices of goods and services?

Understanding how inflation impacts not only individuals, but entire communities, can help people make informed decisions about saving and spending, while recognizing the challenges posed by economic conditions. Let's begin with an example.

Jaime is a college student who lives in a small apartment. He works part-time at a coffee shop to pay for his living expenses and tuition. As soon as he began living independently, Jaime became a pro at managing his own **ledger**.

A **ledger** is a detailed record of all of your monetary transactions. Whether it's money you're earning or spending, a ledger helps you keep track of it all.

At the beginning of the year, he budgeted $10,000 for his living expenses, including rent, food, and other necessities.

These were his transactions for January:

Date	Description	Amount	Type	Balance
01/01/2023	**Starting Balance**			**$1,600.00**
01/01/2023	**Rent for January**	$800.00	Debit	**$800.00**
01/05/2023	**Groceries**	$100.00	Debit	**$700.00**
01/15/2023	**Part-time paycheck**	**$500.00**	**Credit**	**$1,200.00**
01/20/2023	**Gas for car**	$350.00	Debit	**$850.00**
01/30/2023	**Textbooks**	$150.00	Debit	**$650.00**

This ledger shows that Jaime's starting balance on his checking account on January 1st was $1,600, out of which he spent $800 to pay rent for the month. He then spent (a **debit**) $100.00 on groceries and received $500.00 (a **credit**) in pay from his part-time job, bringing his balance to $1200.00. He then spent money on gas and textbooks, bringing his balance down to $650.00 at the end of the month.

Twelve months later, while having lunch with his grandfather, Jaime notices that his budget is not stretching as far as it used to. He realizes that the prices of the goods and services he needs have increased significantly over the past year, and wondered why. Then he saw this image and could not believe his eyes.

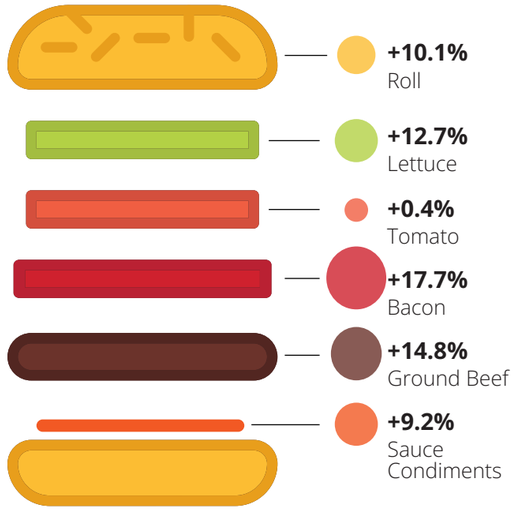
When he brought it up to his grandfather, he was told: "In 1956, I was just a young man starting out in the world. I remember that I used to earn $100 a month as a factory worker. It may not seem like much by today's standards, but it was a decent wage at the time. In fact, I was able to save up enough money to buy a small house in the suburbs."

As we can see, the cost of each item in the **basket** has increased, leading to an overall decrease in his purchasing power.

Thankfully, Jaime has mastered the use of a ledger, for it clearly showed him how his annual purchasing power has decreased.

How Inflation Changed the Price of a Hamburger

Year-over-year change in the price of selected ingredients of a hamburger (April 2021 – April 2022)

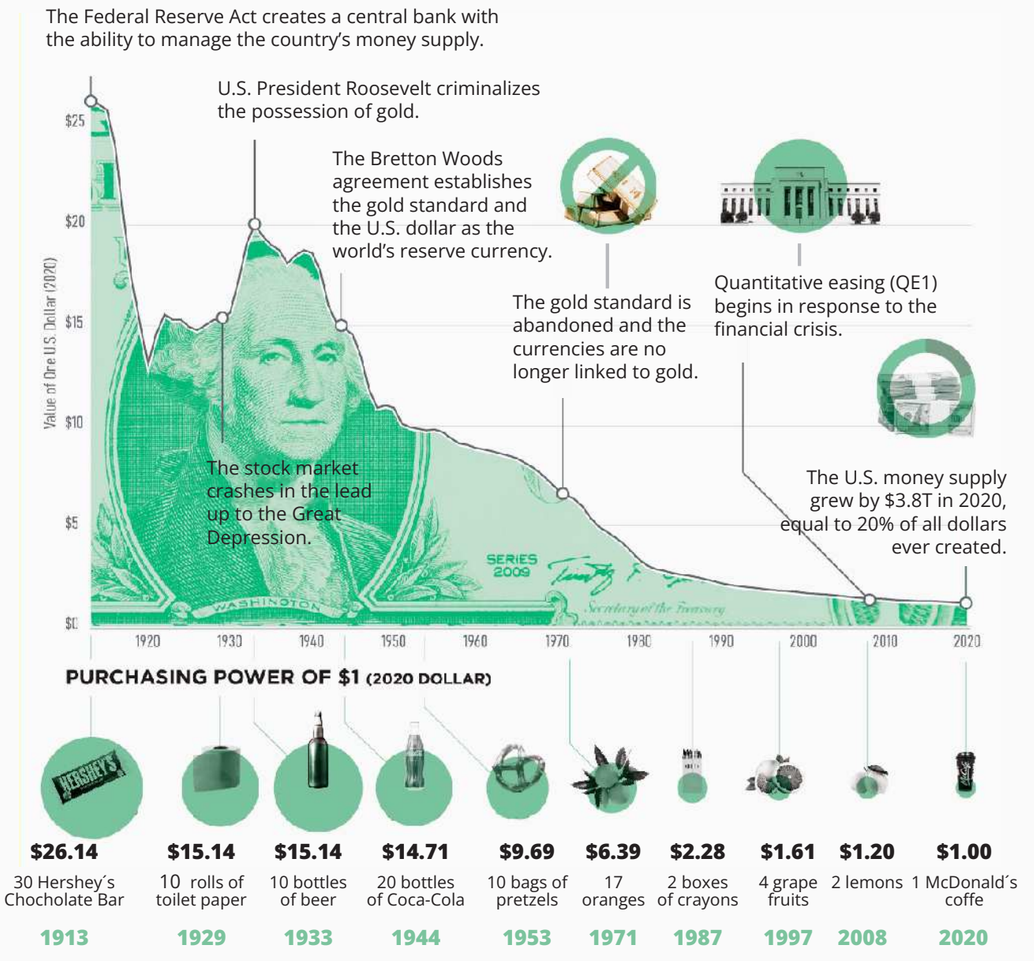


** Based on retail prices, urban consumers.*

A Dollar's Worth

Purchasing Power of the U.S. Dollar

The purchasing power of the U.S. dollar has fallen sharply over the last century, due to rising inflation and money supply.



In 2020, purchasing 30 Hershey's Chocolate bars would cost you $26.14. However, if we go back in time to 1913, the cost for the same quantity of bars would only be $1. This significant difference in price highlights the change in purchasing power over time and demonstrates how the value of currency has shifted over the years due to inflation.

Jaime: "What? That's crazy. I can't even imagine what my rent would have cost back then."

Grandfather: "Well, let me see. If we take inflation into account, $1USD would have bought me about 10 bags of pretzels back then."

Jaime: "Wow, that's really interesting, Grandpa. But how much would that be worth today?"

Grandfather: "Oh, things were much cheaper! A loaf of bread would only cost a few cents, and you could buy a gallon of gasoline for just a quarter. It is unbelievable how much the cost of living has gone up."

- Jaime needs to budget an additional $1,000 for the same basket of goods and services that he purchased the previous year.
    - This means that his purchasing power has decreased by $1,000, as he *now has to spend more money to buy the same goods and services*.
- The basket of goods and services includes rent for his apartment, groceries, and other necessities.
- The following table shows the cost of each item in the **basket** in the first year and the second year, as well as the percentage increase in price:

Item	Cost Year #1	Cost Year #2	% Increase
Rent	$4,000	$4,500	**12.5%**
Groceries	$2,000	$2,300	**15%**
Necessities	$4,000	$4,200	**5%**
Total	**$10,000**	**$11,000**	**10%**

Actually, according to the US Bureau of Labor Statistics, today's prices are 30.39 times as high as average prices since 1913 meaning that a dollar today only buys about 3% of what a dollar bought back then. Now, imagine someone gave Jaimie a time-travel choice: either take $100 in 1913 or wait till 2023 and receive a mere $3. It's like deciding between a shopping spree in the past or grabbing just a couple of small treats today. The difference is huge, and it really highlights how much the value of money has changed over the years!

Jaime earns more in a year than his grandfather ever did, but this also disincentivizes saving. It's more advantageous to spend money now since its value decreases. This hinders the ability to plan for the future. As shown in a previous graph (in section 3.0), salary growth year over year in the United States has remained stagnant for the average citizen, meaning most people aren't receiving raises at the same rate as the decreasing value of their money, despite working harder.

It could have been worse for Jaime. For example, Zimbabwe experienced hyperinflation in the late 2000's, when the country's economy was hit by a combination of political instability, economic mismanagement, and external factors such as drought and sanctions. As a result, the value of the Zimbabwean dollar (ZWD) plummeted, and the government was forced to print more money.

- The 100,000,000,000,000 ZWD bill was introduced in Zimbabwe in 2008. Because of hyperinflation, it was worth only a few US dollars at the time.

- Despite its high face value, the 100,000,000,000 ZWD bill was not enough to buy basic necessities like food or fuel, and people had to carry large bundles of cash to make everyday purchases.

The 2008 financial crisis exemplified the failure of a fiat system. Irresponsible lending practices, lack of oversight, and excessive money creation by banks led to a collapse in the housing market, massive job losses, and global economic turmoil.

Another example is the hyperinflation crisis in Venezuela. Poor economic policies, mismanagement, and excessive money printing caused the Venezuelan bolivar to experience severe inflation, leading to widespread poverty, food shortages, and political instability.

3.1.2 Saving Money in Hard Times

The current global economic situation, which was negatively affected by the pandemic, has brought about challenges such as high inflation and low interest rates on savings accounts. These conditions can make it tough to effectively save money, as inflation eats away at the value of currency over time. Even if you save today, you may end up with less purchasing power in the future.

But don't worry! There are still ways to save money and be financially secure. Here are a few ideas to try:

- **Make a budget**: A budget is a plan for how you will use your money. It can help you see where you are spending too much money and where you can save. Set aside some money each month for saving, and look for ways to cut back on your expenses.
- **Start investing**: Investing is a way to make your money grow over time. There are many types of investments to choose from, and you can find one that fits your budget and your level of risk.
- **Get creative**: There are many creative ways to save money. You can try cutting your own hair or bartering with others for goods and services. Be open to trying new things and

The 50/30/20 Spending Plan



looking for non-traditional solutions to your financial problems.

- It is **generally acceptable** to **take on debt as long as the money is used to generate income and increase purchasing power in the future**. This is because borrowing money can allow an individual or business to make investments that increase their productivity and efficiency, ultimately leading to greater profits and financial stability.
- For example, if a farmer takes out a loan to purchase new equipment that allows them to harvest their crops more quickly and efficiently, they may be able to generate more income and increase their purchasing power as a result. On the other hand, if the money is used to waste resources or make unproductive investments, it can lead to financial difficulties and wouldn't be a wise decision.

By taking charge of your finances and being flexible, you will be better able to weather the storm of a tough economy and come out on top.

3.1.3 The Time Value of Money and Its Role in Economic Growth

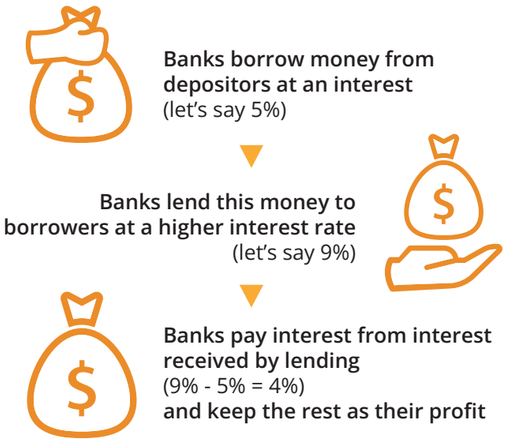
Have you ever wondered why banks offer so many services to their customers? While it may seem like they are being generous, it's important to remember that banks are businesses, and their primary goal is to make a profit. But how do they make a profit if they are giving away money in loans?

In addition to earning interest on deposits, banks generate revenue in other ways, including:

1. Charging interest on loans they give out
2. Charging fees for services like ATM usage and account maintenance
3. Earning money through investments, like buying and selling securities or investing in real estate
4. Keeping a percentage of loans in reserve and investing or lending out the rest
5. Paying interest on deposits and charging fees on checking and savings accounts

By borrowing money at low interest rates and lending it out at higher rates, banks are able to turn a profit. They also generate income through fees and investment activities.

But why should this matter to you as an individual? Well, have you heard the phrase "a dollar today is worth more than a dollar tomorrow"? This concept is known as the **time value of money**, and it's all about the idea that money is worth more in the present than in the future. This is because ***money can be invested to earn interest and because money can lose value over time due to inflation***.



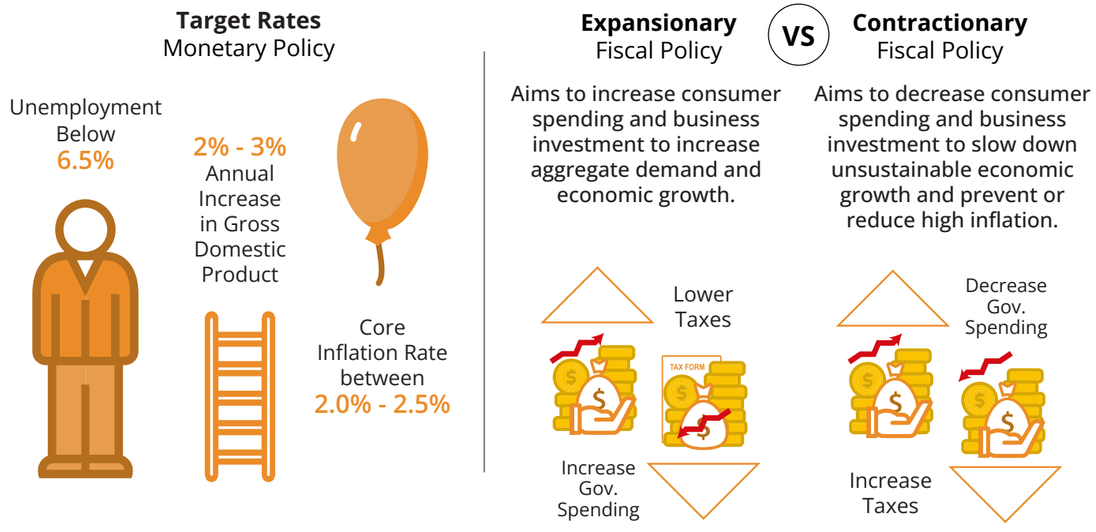
In other words, if you have money sitting in a savings account earning a low interest rate, it's not going to be worth as much in the future as it is today. On the other hand, if you invest your money in something that has the possibility of earning a higher return, you might come out ahead.

To ensure that your money retains its value over time, the goal of investing is to earn a return that is higher than the rate of inflation. This way, your money will be worth more in the future than it is today.

3.2 Centralized Control: How the Government and Banks Manipulate the Money Supply

Understanding where trillions of dollars in stimulus funds come from, and who gets to decide their allocation, is critical for comprehending the broader financial system. Governments use several tools to manage the money supply at specific moments in time.

Central banks and governments can use monetary and fiscal policy tools to influence the money supply and the economy. For example, the United States Federal Reserve (The Fed) uses monetary policy to adjust interest rates, affecting the amount of money in circulation. Fiscal policy, on the other hand, involves using spending and tax policies to influence economic activity.



Exchange rate policies, supply shocks, and price controls are additional tools that can be used to manage the money supply and influence trade and the economy. These policies can help stabilize prices and manage inflation.

Example: **"Too big to fail"** refers to financial institutions so large and interconnected that their failure would have catastrophic repercussions on the entire financial system. During the 2008 financial crisis, several large banks were deemed "too big to fail," leading the U.S. government to intervene and provide bailouts to prevent their collapse.

- One of the most prominent examples of a "too big to fail" institution during the financial crisis was investment bank Lehman Brothers. When Lehman Brothers filed for bankruptcy in September 2008, it set off a domino effect of events, including the near-collapse of insurance giant AIG and a massive drop in the stock market. The U.S. government had to intervene and provide bailouts to other major financial institutions to avert further chaos and safeguard the broader economy.

Grasping how these policies function is vital for understanding the limitations of centralized monetary systems and the context in which ***Bitcoin*** emerged. As a decentralized currency, ***bitcoin*** addresses some of the issues associated with centralized control over the money supply by offering a system that operates independently of central banks and governments.

3.3 The Magic of Money Creation

3.3.1 Fractional Reserve Banking

In the previous sections, we discussed how central banks like the Federal Reserve manage the money supply, how banks earn profits, and some strategies to save money. However, we haven't yet talked about how new money is created and introduced into an economy. It may seem like magic, but there is an interesting process behind it.

So, how does new money actually enter circulation and fuel economic growth? Unlike physical resources like food or water, money has no fixed limit. The government, the central bank, and private banks all play a role in this process.

Let's take a closer look at how the Federal Reserve (Fed) can add $100 million into circulation:

1. The Fed decides to increase the money supply by $100 million based on its **monetary policy goals**, such as boosting economic growth or stabilizing prices.

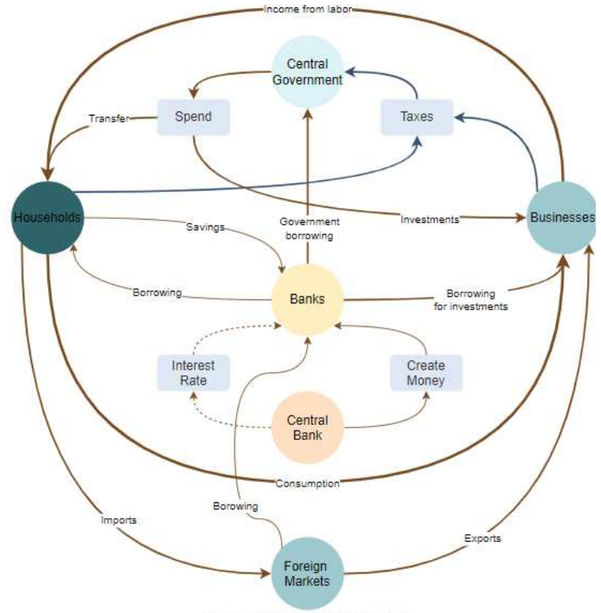
2. The Fed instructs a commercial bank to create a $100 million deposit in its account at the Fed. This deposit is created out of thin air and not backed by any physical assets.

- When a commercial bank creates a deposit at the Fed, it essentially borrows money from the Fed. The Fed provides the bank with funds for the deposit, and in return, the bank pays interest on the loan and eventually pays the loan back.

3. The bank uses the new $100 million deposit to make loans to businesses, individuals, or purchase securities such as government bonds.

4. The businesses or individuals who receive these loans can then use the money to make purchases, pay bills, or invest in other assets. This increases the overall supply of money in the economy.

5. The circulated money eventually ends up in other banks, which can then use it to make their own loans and investments. This process continues until the $100 million has been fully injected into circulation.



It's important to note that banks create new money every time they lend to customers or make investments. When a bank makes a loan, it creates money by adding new funds to the borrower's account for the loan amount. The borrower can then use this money to make purchases or pay bills, effectively increasing the overall supply of money in the economy.

Overall, the Fed's ability to add new money into circulation through the banking system helps to stimulate economic growth and achieve its monetary policy goals. The process of creating new money can be complex, but it is sometimes essential for the economy to function and grow. Other times, it can lead to dire consequences, such as excessive money printing and growing wealth inequality.

Excessive money printing can foster wealth inequality in several ways. For example, the **Cantillon effect** suggests that when new money is created, it primarily benefits those who receive it first—usually large corporations and wealthy individuals. These early recipients can spend or invest the new money before prices rise, accumulating more wealth. In contrast, those further down the chain, like the middle and lower classes, experience the negative effects of inflation without reaping any direct benefits from the newly created money.

The COVID-19 pandemic provided a recent example of the Cantillon effect. Central banks worldwide, including the U.S. Federal Reserve, implemented large-scale quantitative easing measures,

purchasing government bonds and other financial assets to increase the money supply and stimulate the economy.

As a result, a significant amount of newly created money flowed into the hands of large corporations, financial institutions, and wealthy individuals. They could obtain low-interest loans or invest in assets like stocks, bonds, and real estate. The increased demand for these assets drove up their prices, leading to substantial gains for those who could invest early.

Conversely, the middle and lower classes, without the same access to capital or investment opportunities, dealt with the consequences of inflation. As the newly created money trickled down through the economy, it led to higher prices for goods and services, reducing the purchasing power of those unable to benefit directly from the central banks' actions.

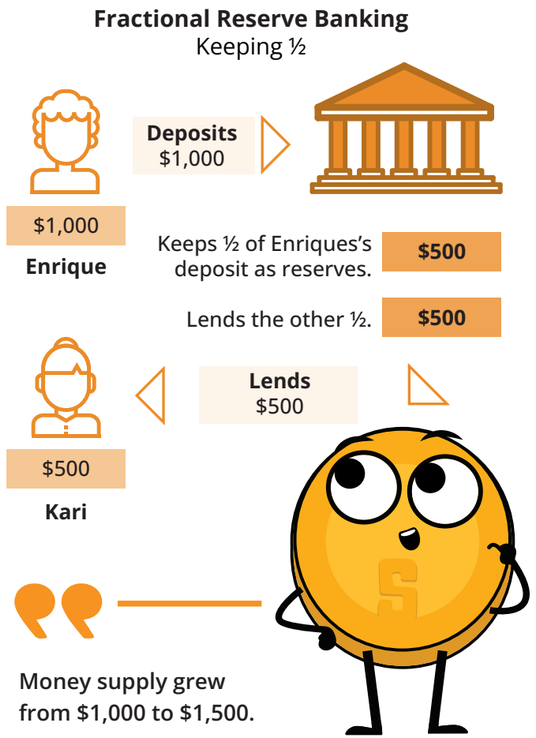
This example demonstrates how the Cantillon effect can exacerbate wealth inequality, disproportionately benefiting those closest to the source of new money while leaving the majority to grapple with the negative consequences of inflation.

3.3.2 Class Exercise: Fractional Reserve Banking

Fractional reserve banking is a system where banks maintain only a fraction of their deposits as reserves and lend out the remainder. As long as they adhere to the reserve ratio set by the central bank, they can create more money than they have on hand. However, this ability to create new money carries the risk of excessive borrowing and financial instability if not managed carefully.

The reserve ratio is a regulation that dictates how much money banks must keep in reserve and how much they can lend out. It is established by the central bank, which is responsible for ensuring a healthy economy.

In the following exercise, we'll explore how fractional reserve banking can lead to currency debasement, inflation, and a decrease in purchasing power. We'll use a simplified example involving six participants, one of whom will act as a bank, and a reserve ratio of 10%.



1. **A** just won $100,000 from the lottery and deposits it in the bank (**B**). With a 10% reserve ratio, **B** must keep $10,000 in its vault and can lend out the remaining $90,000.

2. **C** borrows the maximum amount ($90,000) from B and uses it to buy a house from **D**.

3. D deposits the $90,000 received from **C** into the bank (**B**). The total deposits in the bank are now $190,000.

4. **E** requests a loan from **B**, and the bank lends out 90% of the new deposit, which is $81,000.

5. **E** uses the $81,000 loan to buy an art piece from **F**, who then deposits the money in the bank (**B**). The total deposits recorded are now $271,000.

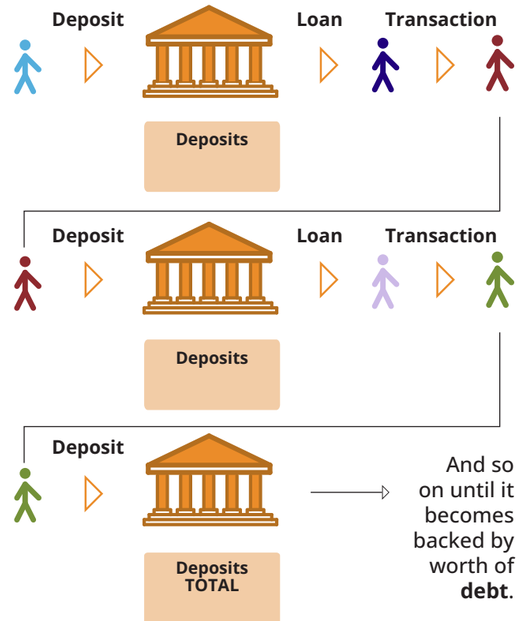
In this scenario, the initial $100,000 deposit has resulted in a total of $271,000 in deposits after circulating through the economy. If the reserve ratio were lowered to 1%, the amount of money created would be significantly higher ($100,000 / 0.01 = $10,000,000).

It's important to note that as of 2020, the Federal Reserve (the Central Bank of the USA) reduced reserve requirement ratios to zero percent in order to stimulate the economy.

Through this exercise, we can see that fractional reserve banking has the potential to fuel economic growth by increasing the availability of credit. However, it also carries risks that need to be carefully managed to avoid inflation and financial instability.

We need the following volunteers:

A = Depositor (Lottery Winner) (Light Blue)
B = Bank Cashier (Bank)
C = Debtor #1 (Dark Blue)
D = Property Owner/Depositor (Red)
E = Debtor #2 (Light Purple)
F = Art Gallery Owner/ Depositor (Green)



The formula is: *Money Created = Total Amount of Money in the Economy ÷ Reserve Ratio*

So, how much money is actually created with those 100,000 USD if the money continues to circulate throughout the economy?

Just out of curiosity, how much money would be created in an economy if its reserve ratio was lowered to 1%? (Make sure you divide $100,000/0.01). Surprised?

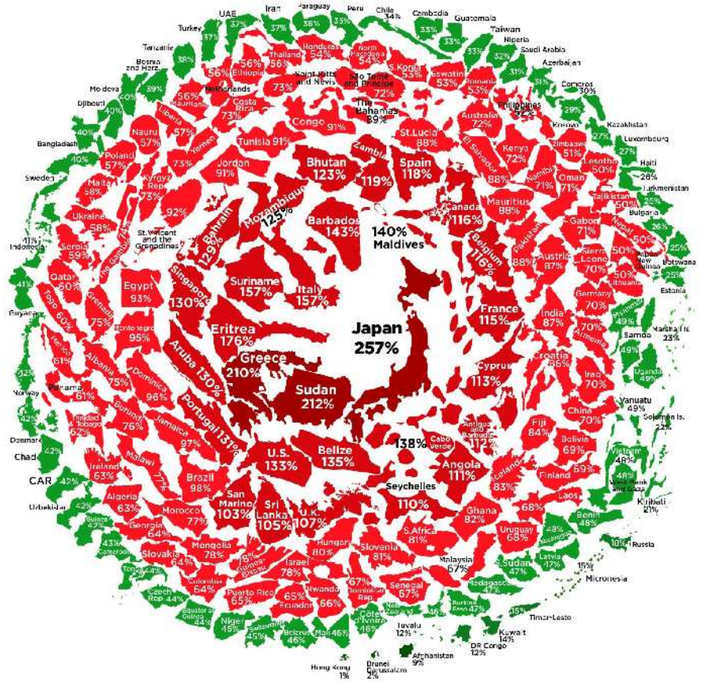
- As of 2020, the Federal Reserve (the Central Bank of the USA) **reduced reserve requirement ratios to zero percent** in order to stimulate the economy.

3.4 Debt: The Burden That Crushes the Middle and Lower Classes

Debt is money that is owed by one person or organization to another. When you have debt, you are required to pay back the money you owe, usually with interest, by a certain date.

Debt is a double-edged sword. It's true that borrowing money can provide a much-needed financial boost, whether it's for individuals making a big purchase, businesses investing in their growth, or governments funding important services. But borrowing too much can lead to financial ruin. When you can't pay the interest on your debts, it becomes harder to pay your bills and stay afloat. This is especially true when an entity takes on more debt

The State of the World´s Government Debt



to pay off existing debt, and gets caught in a vicious cycle known as a "debt spiral."

The debt crisis is a worldwide problem, including in the United States. Currently, the government is spending more money than it is earning. To pay its bills, it has been borrowing more and more money. However, this cycle of debt and higher borrowing costs can soon harm the government's credit rating. If the debt becomes too much, the government may have financial difficulties and potentially go bankrupt, just as many other countries have in the past.

- Debt taken on by the government can have long-term effects on future generations.
- Printing more money to fund expenses can result in currency devaluation and a possible collapse of the monetary system.

In the late 2000s, Greece faced a severe debt crisis when it was revealed that the government had been hiding the true extent of its debt. As a result, the country was unable to repay its creditors, leading to austerity measures, skyrocketing unemployment, and a significant decline in economic growth.

But how can we measure the risk of a country taking on too much debt? One way is through the **debt-to-GDP ratio**, which shows the amount of a country's total debt as a percentage of its GDP.

- It's important to remember that the debt-to-GDP ratio is only one part of understanding a country's money situation.
    - The **debt-to-GDP ratio** is a way to see if a country can pay its debts.

- If the ratio is high, the country may have trouble paying its debts in the future.
- If the ratio is low, the country may be able to pay its debts easily and be in good financial shape.

Gross Domestic Product (GDP) is a measure of the total value of goods and services produced within a country over a specific period of time, typically a year. It is often used as a measure of the size and health of an economy.

3.5 Addressing Wealth Inequality: A New Approach to Money

The transition from commodity-based currencies to the modern fiat system has brought about several challenges. Issues with the current monetary system include inflation, debasement, excessive debt, and wealth inequality, as well as concerns about privacy, control, and financial censorship. The need for a viable alternative is increasingly urgent in today's digital, interconnected world.

Bitcoin was invented as a potential solution to these issues with traditional money. Operating independently of central banks, Bitcoin enables peer-to-peer transactions without intermediaries,

making it a groundbreaking innovation in the financial industry. Key features of ***Bitcoin*** include its decentralized network, which makes it resistant to government interference and manipulation, and its finite supply. These attributes make ***bitcoin*** scarce and valuable, similar to gold, contributing to its growing popularity as a store of value and investment opportunity.

It's important to note that one of the key benefits of Bitcoin is that it operates without a central authority or boss. Nobody controls ***Bitcoin***, and it has been operating perfectly fine since January 3, 2009, without any major crashes or shutdowns. This decentralized nature of ***Bitcoin*** means that it is not subject to the same vulnerabilities as traditional financial systems, which can be manipulated or controlled by governments, banks, or other centralized institutions. This lack of control has also been a major factor in addressing wealth inequality, as Bitcoin is accessible to anyone with an internet connection, regardless of their socioeconomic status.

In the following sections, we'll explore ***Bitcoin's*** origins, technology, and how it addresses the concerns of the current monetary system.

Chapter #4

The Future can be Decentralized: Empowering Communities and Individuals

4.0 The Price of Control: A Look at Surveillance, Censorship, and Regulation
- **4.0.1** Surveillance
- **4.0.2** Financial Regulations and Censorship

4.1 From Crisis to Innovation: The Cypherpunks and the Creation of a Decentralized Digital Currency

4.2 Abuse of Centralization
- **4.2.1** Centralized Sytems
- **4.2.2** The Intermediaries in a Credit Card Transaction

4.3 Overcoming Centralization with Decentralized Systems
- **4.3.1** Class Activity: Bank Transaction vs. Peer-Peer Transaction Simulation

4.4 Transactions are Just Agreements to Trade
- **4.4.1** To Trust or Not to Trust
- **4.4.2** Let's Swap Trust for Rules

4.5 Unlocking the Power of the Blockchain: A Technology Revolutionizing the Future

4.6 Emphasizing the Importance of True Decentralization in Blockchain Projects for Achieving Freedom and Empowerment

4.0 The Price of Control: A Look at Surveillance, Censorship, and Regulation

4.0.1 Surveillance

Surveillance is a tricky business. On the one hand, it helps catch people doing bad things like money laundering. But the more fraud that happens, the more surveillance is needed, which can lead to invasions of privacy through technology. Private companies may also collect and trade your personal information for their own benefit, and the risks of this surveillance can include scams, harassment, extortion, identity theft, and even tracking your card purchases. Plus, with the rise of AI and machine learning, it's becoming even easier for governments and companies to invade our privacy. Moreover, it's often the people who are already disadvantaged or underprivileged who are hit the hardest.

The Impact of AI and Technology on Future Privacy and Surveillance

Future Effect	The Rich	The Poor
Access to personal information.	May have access to extensive personal information and can use it to make informed decisions.	May lack this information and may have to rely on outdated or unreliable sources.
Ability to shape the world in their own interests.	May use their access to data to shape the world in their own interests.	May have little influence on what happens.
Control over others.	May exert control over the poor through their access to data, leading to a loss of individual freedom.	Little control; are often the controlled.
Vulnerability to digital scams, online harassment, extortion, and identity theft.	Likely less vulnerable to these issues with more information and more protection from such scams.	May be more vulnerable to these issues due to a lack of access to resources and information.

4.0.2 Financial Regulations and Censorship

Financial regulations, censorship, and prohibitions can be an emotionally and financially taxing reality for society and its citizens. They come in many forms, such as:

- **Capital Controls or Sanctions**: When spending gets out of control, governments may impose price controls to try and fix the problem. But sometimes these controls make things worse. Governments may also limit how much money citizens can transfer, exchange, or take out of the country. Examples:

- How does China's Social Credit Score system work? In China, financial transactions and other data of all citizens are centrally collected, and used to create a Social Credit Score system that can be used to control citizens.

- Consider what happened in Greece in 2015 — citizens were only able to withdraw 60 euros per day by government mandate. Similarly, the Chinese are only able to send limited amounts of Renminbi out of the country.



Check the following article: "What You Need to Know About Moving Money In and Out of China".

- There have been several instances in Argentina when the government imposed strict currency controls to try to stabilize the peso. One such instance was in 2011, when the government implemented capital controls to stem the flow of dollars out of the country and to prevent further devaluation of the peso. Another instance was in 2019.



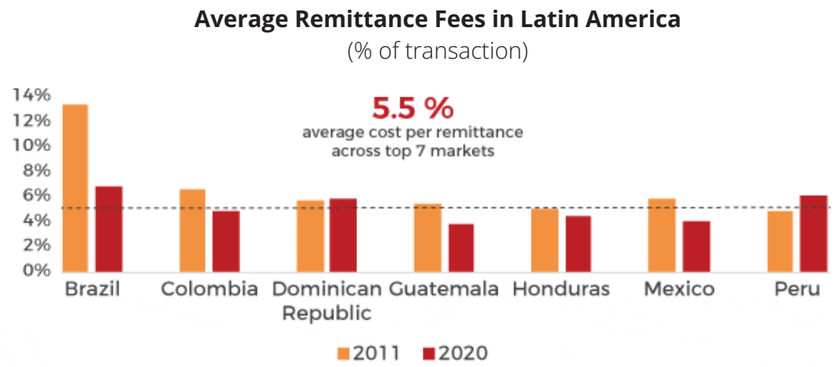
- **Restrictive Banking Policies**: Have you ever tried to withdraw cash from an ATM only to find out you've reached your daily limit?

Or maybe you've tried to transfer money to a friend only to be told there's a maximum amount you can send. These are just a few examples of restrictive banking policies that can make it tough to access your own money and do what you like with it.

Banks can also charge fees for most transactions and may only be open during certain hours, making it hard to get to your cash or make financial decisions. Carrying around lots of cash increases your risk of getting robbed. On top of all that, banks sometimes offer lower-interest loans to the wealthy, while opening up the poor to loan sharks and higher-interest loans. In so doing, the financial system often profits from the gap between the rich and the poor.

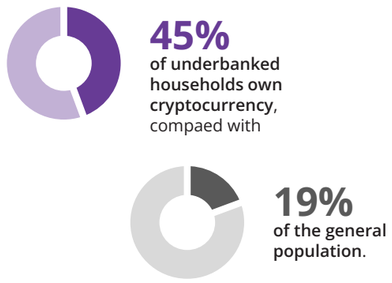


- **Expensive Remittances**: Sending money to other countries can be expensive due to fees from banks and other financial institutions. Many low-income families in developing countries rely on money from relatives living abroad to get by. But high fees for international money transfers can eat into how much money is actually received by the recipient. This can make it hard for families to afford basic necessities like food, housing, and education.

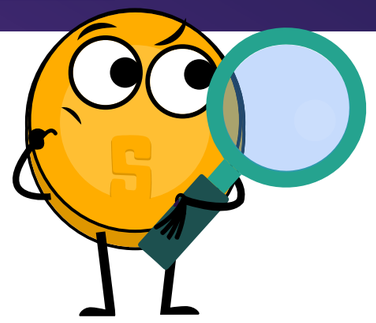


- Imagine a family in a rural village in Brazil that relies on money from a relative working in the US. If the relative sends $100, but the bank charges a $7 fee for the transfer, the family only gets $93. This may not seem like a lot, but for a family living on a tight budget, losing $7 can make a big difference.

- **The Unbanked and Underbanked**: Unfortunately, **not everyone has access to traditional banking services**, whether it's because they don't meet the requirements to open an account or because they live in areas where banking services aren't available. This can make it difficult for people to access financial services and participate in the global economy.



- But wait, there's more! Governments may also control the exchange rate of their currency, which can make it hard for people to exchange money between countries or lead to **unfavorable exchange rates**. Financial institutions may **block donations** to certain organizations or individuals, or take away your bank account altogether. Social media platforms and financial institutions may remove certain content if they believe it is spreading misinformation or violating their community standards or policies. This is sometimes referred to as **censorship** and can include a wide range of activities, such as blocking or suppressing content, limiting access, or removing information altogether.

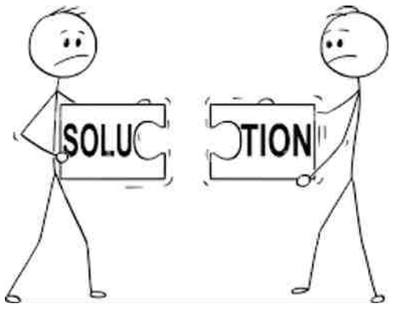


Surveillance, control, and hidden fees are only the political downsides of the current system we live in. Unfortunately, there are a series of hidden economic costs as well — ones that we often never get to learn about.

4.1 From Crisis to Innovation: The Cypherpunks and the Creation of a Decentralized Digital Currency

Before the creation of ***Bitcoin***, people were searching for ways to address the problems of traditional finance, such as fraud, corruption, and a lack of trust in financial institutions. These issues were made even more pressing by the global financial crisis of 2008. In response, a group of tech-savvy and forward-thinking individuals known as the Cypherpunks set out to create a **digital currency** that could be used for online transactions **without the need for intermediaries** like banks.

The Cypherpunks were rebels and visionaries who believed in the power of technology to bring about positive change and challenge traditional power structures. Many of them were involved in activism and civil liberties issues, and they were united by a shared passion for technology and a desire to use it to shape the future.



Q: How can individuals regain their financial self-sovereignty?

A: The Cypherpunks movement aims to create a new financial system that respects individuals' security, privacy, and freedom, as a solution to regain financial self-sovereignty.

And so, they set out to create ***bitcoin***, a digital currency that would revolutionize the way we think about money and financial transactions. To do this, they needed to find a way to record transactions that was more secure and transparent than traditional centralized ledger systems. Why did they feel this way?

4.2 Abuse of Centralization

4.2.1 Centralized Sytems

Centralization of power often leads to corruption, which can result in the mismanagement of resources, including financial resources. This can disproportionately affect those lower in the hierarchy and without as much influence or power, causing them to bear the greatest burden of the consequences of corruption and mismanagement.

The modern fiat system is characterized by centralization of control, with a small group of banks and other financial institutions holding significant weight over the economy.

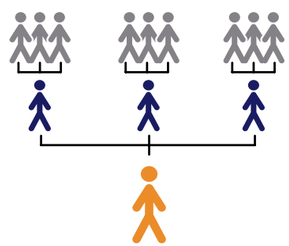
A centralized system can be thought of as a tree with a single trunk. The trunk represents the central authority or point of control, and the branches represent the various parts of the system that are controlled by the central authority. In this analogy, the tree is vulnerable if the trunk is damaged or diseased, because the entire tree relies on the trunk for support.





There are many **drawbacks to centralized systems** including:

- **Vulnerability**: A centralized system relies on a single point, so if that point fails, the whole system can fail.
- **Control and power**: Those in control of centralized systems have a lot of power and influence over how they work.
- **Inefficiency and intermediaries**: Centralized systems often use intermediaries, which can make them slow and add extra costs.
- **Lack of autonomy**: People may not be able to make their own financial decisions.
- **Censorship and restriction**: There is a risk of being blocked from accessing certain financial resources in centralized systems.

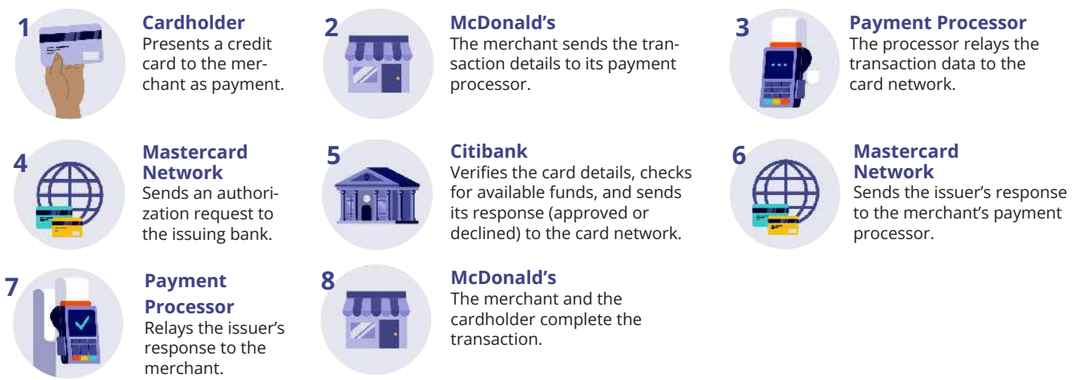


- **Scaling challenges**: Centralized systems may struggle to keep up with increasing demand for financial services and resources.
- **Security risks**: Centralized systems can have weaknesses that hackers can use to gain access or cause damage.
- **Lack of transparency and trust**: It can be hard to understand how centralized systems work and to make informed decisions about them because they may *not be transparent or trustworthy*.

4.2.2 The Intermediaries in a Credit Card Transaction

A credit card transaction, such as buying a hamburger, might appear simple but involves multiple intermediaries. Let's break down the process concisely to reveal its complexity and hidden costs.

1. You order a hamburger at **McDonald's** using your **Citibank MasterCard** card.
2. **McDonald's** sends an authorization request to its payment processor.
3. The processor forwards the request to **Mastercard**.
4. **Mastercard** sends the request to the issuing bank, **Citibank**.
5. **Citibank** sends an authorization code back to **Mastercard**.
6. **Mastercard** returns the authorization to the processor.
7. The processor sends the authorization back to **McDonald's**.
8. You receive your hamburger.



In this process, each intermediary adds fees, which are ultimately passed on to the consumer. These fees remain hidden in the cost of the hamburger.

Real-world Examples of Centralized and Decentralized Systems

Centralized System: **Facebook**

Facebook is a centralized social media platform where users' data is stored and controlled by the company. In 2018, the Cambridge Analytica scandal revealed that personal data of millions of Facebook users had been harvested without their consent, leading to questions about privacy and security.

Decentralized System: **Tor**

Tor (The Onion Router) is a decentralized network that allows users to browse the internet anonymously. Instead of relying on a central authority, Tor routes users' data through multiple nodes, protecting privacy and security. This has made it popular among journalists, activists, and others seeking to evade censorship and surveillance.

Research, Data, and Statistics

1. A study by the Federal Reserve Bank of Kansas City found that the average interchange fee for credit card transactions in the United States was 2.04% in 2019 [1]. This means that for every $100 spent, $2.04 goes to intermediaries in the credit card transaction process.

2. According to the International Data Corporation (IDC), global spending on blockchain solutions is expected to reach $15.9 billion by 2023, a compound annual growth rate of 60.2% between 2018 and 2023 [2]. This indicates that investment in decentralized systems is growing rapidly.

3. Research by GlobalWebIndex showed that 40% of respondents were concerned about how Facebook uses their personal data [3]. This highlights the potential drawbacks of centralized systems when it comes to privacy and security.

Modern banking. Simple, right? Take something as seemingly simple as buying a hamburger with a credit card. At first glance, it may seem undemanding and harmless. But if we break down the steps and see the intermediaries involved, you might be surprised at what we discover. Are there inconveniences, inefficiencies, maybe even hidden dangers lurking in the shadows? Let's find out.

At this point, no actual funds have changed hands, except perhaps a small authorization fee. The transaction only exists on "paper." McDonald's needs to close or batch-out its sales for the day. The closing process might look like this:

1. **McDonald's** terminal or point-of-sale (POS) system sends the day's transactions to the processor.

2. The **processor** sends the transaction information to **Mastercard**.

3. **Mastercard** sends the transactions to **Citibank**.

4. **Citibank** confirms the authorizations, **holds back their interchange fees** (there are over 900 possible fee codes in North America), and transfers the funds back to **Mastercard**.

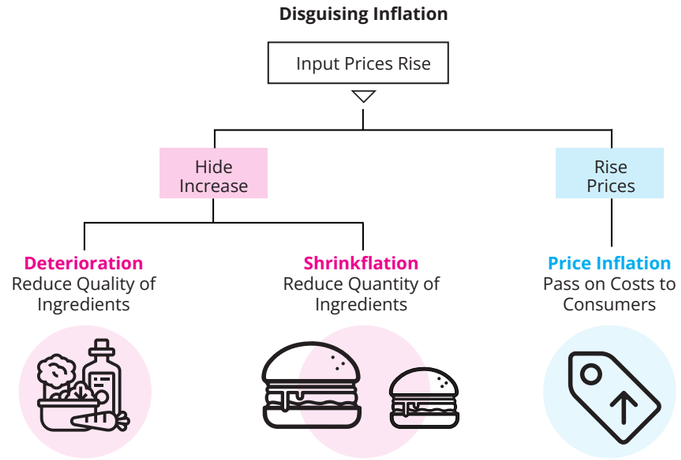
5. **Mastercard takes its assessment fee** and sends the funds to the **processor**.

6. The **processor takes its cut**, as set out in the merchant agreement, and deposits the funds to **McDonald's** bank account.

Who do you think paid for the fees? Of course YOU. But, did anybody inform you of this? Oh, no! They were hidden in the cost of the hamburger.

And all of this happens believe it or not because we rely on centralization.

The modern banking world comes with various risks, including accidental double swipes, credit card fraud, human and computer errors, and potential hacks.



4.3 Overcoming Centralization with Decentralized Systems

Decentralized systems resemble a forest, where each tree represents an independent participant, and the forest symbolizes the entire system. In this analogy, the forest is more resilient than a single tree as it does not rely on a single point of failure. If one tree is damaged, the forest can continue to thrive. Decentralized systems, like forests, are more effective with diverse and collaborative participants, instead of a single central authority dictating the rules.





Advantages of decentralized systems:

- Enhanced resilience and reliability due to no single point of failure
- Increased security with the right encryption, as there's no central point of control for hackers
- Greater sovereignty for participants, who have more control over assets and decisions
- Improved transparency, as all nodes access the same information

A **node** is a *computer connected to a network* that can *share and/or receive information* and communicate with the other nodes.

- Permissionless and limitless nature, allowing anyone to join or participate
- Equal opportunities for all nodes to contribute and influence the network

A **network** is a group of **nodes** that are connected to each other in some way. This connection allows the devices to exchange information and communicate with each other.

- Enhanced privacy and security through the use of pseudonyms or nicknames

Challenges of decentralized systems:

- Increased effort required to achieve consensus among nodes
- Greater vulnerability to malicious nodes that could harm the network

In a centralized financial system, a small group of entities or individuals has control over the entire system, making decisions that impact all participants. In contrast, a decentralized system can empower each participant to be in charge of themselves, eliminating the influence of a central authority. This power shift restores financial control to the people, fostering a more equitable and democratic financial landscape.

4.3.1 Class Activity: Bank Transaction vs. Peer-Peer Transaction Simulation

Objective: To understand the underlying concepts and mechanics of a bank transaction through a hands-on simulation using checks, and compare it to a **peer-to-peer transaction like *Bitcoin***.

1. Understand your role: You have been assigned one of the following roles: sender, receiver, or a member of the bank staff (teller, manager, clearance officer) OR sender, receiver, or a member of the Bitcoin network (node, miner).
- Senders will be responsible for initiating the transaction.
- Receivers will be responsible for verifying and confirming the transaction.
- Bank staff or Bitcoin network participants will be responsible for facilitating the transaction.

2. ***As a sender (bank simulation):*** Create a check by following these steps:
- Take a check template and fill in the date, payee (receiver's name), the amount in words and numbers, and sign the check.
- Hand over the completed check to the receiver.

3. ***As a sender (Bitcoin simulation):*** Create a ***Bitcoin*** transaction by following these steps:
- Open your ***Bitcoin*** wallet and create a new transaction by entering the receiver's address and the amount of ***bitcoin*** to send.
- Verify the transaction details and confirm the transaction.

4. ***As a receiver (bank simulation):*** Deposit the check by following these steps:
- Verify that the check is properly filled out, signed, and has no alterations.
- Deposit the check at the bank by handing it to the teller.

5. ***As a receiver (Bitcoin simulation):*** Receive the Bitcoin by following these steps:
- Open your ***Bitcoin*** wallet and wait for the transaction to be confirmed on the blockchain.
- Verify that the correct amount of ***bitcoin*** has been received.

6. ***As a member of the bank staff (bank simulation)***: Verify, approve, and clear the check by following these steps:
- **Teller**: Verify the check's information and pass it to the bank manager for approval.
- **Bank Manager**: Verify the check and, if everything is correct, approve the transaction and pass it to the clearance officer.
- **Clearance Officer**: Finalize the transaction by transferring the funds from the sender's account to the receiver's account.

7. ***As a member of the Bitcoin network (Bitcoin simulation):*** Facilitate the transaction by following these steps:
- **Node**: Verify the transaction and broadcast it to the network.
- **Miner**: Confirm the transaction by including it in a block and solving the cryptographic puzzle.
- Wait for the transaction to be confirmed on the blockchain.

4.4 Transactions are Just Agreements to Trade

Welcome to *The **Decentralized** Micronesian island of Yap!* It is a bit remote, but fascinating because people use a special kind of currency called "Rai stones." A feature that makes them a great form of money is their **scarcity**. The total number of Rai stones is *limited*, which means that *they cannot be easily reproduced or inflated* like fiat currencies. This fixed supply helps to maintain the purchasing power of the Rai stones over time and makes them a reliable store of value. These Rai stones are like giant coins that are used to purchase stuff on the island. The thing is, they can weigh a *ton*. Rai stones can actually crush you, so they're a bit impractical to carry around. How then, can people

conveniently use Rai stones as mediums of exchange without having to physically take them from one place to another?



4.4.1 To Trust or Not to Trust

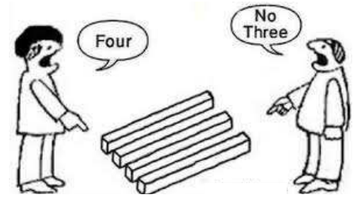
While the US Dollar is now the official currency of Yap Island, Rai stones still are a type of money. Unlike the dollars, the Rai stones on Yap Island are not controlled by a single authority or stored in banks. Instead, the transactions are based on oral history and trust, with people keeping track of their own records of who owns which stones.

This system has both benefits and drawbacks. On the one hand, it allows for a certain degree of independence from one central authority. On the other hand, it can also lead to disagreements and potential for cheating. Why?

Decentralization is easy to achieve in small groups. Life is simple as there are fewer people to coordinate; it is often possible for everyone to have a say in decision-making processes and for those decisions to be implemented relatively quickly. As a group gets larger, it becomes more difficult to reach an agreement and for decisions to be implemented effectively.



- Imagine that you have a field full of ripe corn that needs to be harvested. You need some help, so you approach your neighbor, Raquel, and offer her a deal: if she helps you harvest the corn, you will give her a 10 kg stone in exchange. Raquel agrees, and for the next day, she works alongside you in the fields, helping to gather the corn and bring it in. At the end of the day, you both shake hands and instead of physically handing over the stone, you simply show her that her payment (the Rai stone) is in your backyard.
- From that point on, *you both agree* that the stone now belongs to Raquel. This type of **transaction**, where no currency actually is handed from one individual to the other as a form of payment, but instead a *physical object is used as a **symbol of value***, is common on Yap Island and has been used for centuries as a form of currency.
- Five years later, you decide to try and claim the Rai stone as your own. You present evidence to the community that the stone has been passed down through your family for generations, and that you are the rightful owner.
- However, Raquel remembers the agreement that you both made and provides evidence by bringing witnesses of the exchange to give a statement. She argues that the stone rightfully belongs to her, as it was given to her in exchange for her help with the harvest.
- Some members of the community might agree with your claim, citing the tradition and history of your family's ownership of the stone. However, others might side with Raquel, pointing to the agreement that was made and the fact that the stone has been in her possession (figuratively speaking) for five years without any objections from other members of the community. Factors that might be considered include the history and tradition of ownership, the terms of the agreement between you and Raquel, and any relevant evidence or arguments. Not a very solid solution, is it?



So then, how can thousands of strangers all agree on one truth without anyone having the final say? This is something that has puzzled people for a long time, and it's an important question to consider. It turns out that the internet has helped us find a solution to this problem. The solution is called the **blockchain**.

4.4.2 Let's Swap Trust for Rules

Imagine you and your friends are in a group chat where you can buy and sell things with each other. Every time a purchase is made, it's recorded in a shared document for everyone to see and each person's balance is updated. This chat uses a digital ledger to keep track of all the transactions that have happened. The ledger is like a record book that everyone can see.
In a decentralized system like this, all the participants have a copy of the ledger. This makes it hard for any one person or group to change any information without being noticed. It's like a security measure to make sure that the records are accurate and no one can cheat. This is similar to how a **blockchain** works.

Instead of relying on personal relationships and subjective interpretations of trust, a decentralized system can operate effectively if it is *based on a set of clear, transparent rules that everyone agrees to follow*. This way, *decisions can be made and conflicts can be resolved in a fair and objective manner, without relying on the trust of individual parties*. It might not be as romantic as relying on trust, but it's a much more reliable way to ensure that a decentralized system operates smoothly.

- If Yap Island had a set of unbreakable rules and a written record of all transactions between its members, the conflict between you and Raquel could have been avoided. These rules and records would have made it clear to all members of the village what their rights and responsibilities were.

But is it that simple? Not really; there was a lot of trial and error before blockchain technology was actually a success.

- What are the exact rules that must be followed?
- Who makes these rules?
- Why will people want to follow the rules?

- How do rules get distributed across the network?
- What will happen if someone breaks the rules?
- How can the rules be changed or updated later?
- How will the rules be enforced to make sure everyone follows them?
- How can the rules be made clear and easy to find for everyone in the system?

4.5 Unlocking the Power of the Blockchain: A Technology Revolutionizing the Future

Despite numerous setbacks, one very enigmatic person (or group of people) finally found the key to developing a game-changer methodology for the world of trade and finance. This masterpiece made it incredibly easy to track and verify transactions, streamlining the process of exchanging money, goods, and other assets. With its innovative approach and advanced technology, this system revolutionized the way we think about economic transactions, making them faster, safer, and more efficient than ever before.

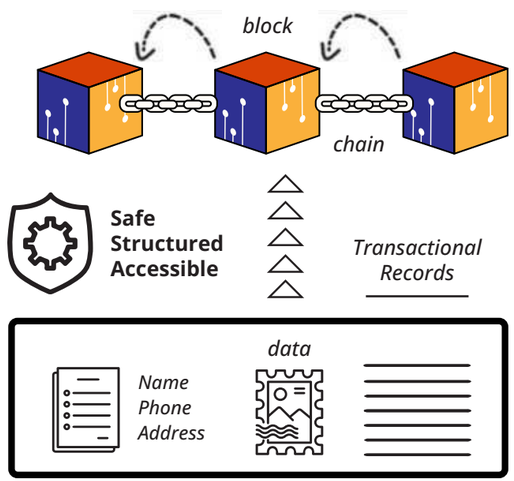
A ***blockchain*** is a decentralized digital ledger that securely records and verifies all transactions across multiple computers in a transparent manner.

A **blockchain** is like a history book. Each page (or "**block**") has a list of things that happened (**transactions**). As more things happen, we need to add new pages (blocks) to the book. Anyone can read the book for free, but only special helpers (**miners**) can add new pages. They make sure that what's written is true. Once something is written in the book, it can't be changed or erased. It's a permanent record of all the **transactions** that have happened on the **blockchain**.

- A **blockchain** does not have a central authority (like an author, a publisher or an editor) that can edit, delete or change the information recorded in it, hence it's considered a more secure and reliable method of record keeping compared to a traditional central database.

What is a blockchain?

All records of actions on the blockchain are called transactions.



If the helpers (**miners**) are not in **consensus** about the validity of the pages (**blocks**), they will be rejected and will not be added to the **blockchain**.

4.5.1 Class Activity: Consensus Building in a Peer-to-Peer Network

1. Understand your role: You have been assigned to either Group A or Group B.

2. If you are in Group A:
- Select a leader who will create a drawing on a piece of paper, which represents a **transaction** to be added to the **blockchain**.
- Pass the paper around the group until everyone has had a chance to replicate the drawing.
- Compare the original drawing to the final drawing to see if there are any discrepancies.
- If there are discrepancies, discuss and try to reach a consensus on what the correct drawing should be.

3. If you are in Group B:
- Select a leader who will create a different drawing on a piece of paper, which represents a **transaction** to be added to the **blockchain**.
- Pass the paper around the group until everyone has had a chance to replicate the drawing.
- Compare the original drawing to the final drawing to see if there are any discrepancies.
- If there are discrepancies, discuss and try to reach a consensus on what the correct drawing should be.

4. Try to complete the task as quickly as possible.

5. Discuss the similarities between this activity and the process used by nodes in a peer-to-peer network to verify **transactions** and add them to the **blockchain**.

6. Compare the activity to the concept of proof of work, where nodes compete to solve a complex mathematical problem to add a new block to the **blockchain**.

7. Discuss the benefits of consensus-building in a **blockchain** network, such as decentralization, security, and immutability.

This activity helps students to visualize the concept of consensus-building in a **blockchain** network, where nodes must agree on the validity of a transaction before it can be added to the **blockchain**. By working together to reach a consensus on the correct drawing, students can better understand the importance of collaboration and agreement in a decentralized system. Additionally, the timed aspect of the activity adds a sense of urgency, which reflects the importance of speed and efficiency in **blockchain** **transactions**.

4.6 Emphasizing the Importance of True Decentralization in Blockchain Projects for Achieving Freedom and Empowerment

Decentralization is a key principle of **blockchain** technology that eliminates the need for intermediaries and enables peer-to-peer interactions. In a truly decentralized system, there is no central authority or control, and all participants have an equal say in the decision-making process. ***Bitcoin***, the first and most well-known blockchain-based cryptocurrency, was designed with decentralization as a central principle. By creating a decentralized monetary system, ***Bitcoin*** sought to eliminate the need for intermediaries and empower individuals to take control of their financial transactions. The decentralized nature of ***Bitcoin*** makes it immune to government or institutional control, and its open-source code allows anyone to participate in the network.

True decentralization is important in **blockchain** projects because it ensures that power is distributed among all participants and that no single entity can control the system. This aligns with the principles of ***Bitcoin*** and the larger goal of the freedom and empowerment of individuals. When power is centralized, it can be easily abused, leading to unequal access to resources and control over financial transactions. Decentralization allows for a more transparent and equitable system where all participants have an equal say in decision-making.

Unfortunately, not all **blockchain** projects prioritize decentralization. Some projects create new **blockchain** and tokens, which are still controlled by a central authority or company. This defeats the purpose of **blockchain** technology, which is to create a decentralized and trustless system. These projects may market themselves as decentralized, but in reality, they are not truly decentralized by design.

Incorporating true decentralization into **blockchain** projects is essential for creating a more equitable and transparent society. By eliminating intermediaries and creating a peer-to-peer system, individuals can take control of their financial transactions and participate in a global economy in unprecedented ways. Additionally, true decentralization can help prevent abuse of power and promote fairness and equal access to resources.

As we continue to explore the possibilities of **blockchain** technology, we recognize that the true revolutionary power lies in the open source, peer-to-peer networks that implement true decentralization and unstoppable freedom in our society. This aligns with the principles of Bitcoin and the larger goal of the freedom and empowerment of individuals. By challenging traditional power structures and creating transparent and secure systems, blockchain technology has the potential to transform many aspects of our society, creating a future that is more equitable, transparent, and decentralized. While the potential of **blockchain** technology to revolutionize finance is well-known, we are only beginning to scratch the surface of its potential to transform many other industries as well. By prioritizing true decentralization and aligning with the principles of ***Bitcoin***, we can create a future that empowers individuals and promotes greater freedom and equality.

Chapter #5

Unveiling the Future of Money: An Introduction to Bitcoin

5.0 The Enigma of Satoshi Nakamoto: A Glimpse into the Mind Behind Bitcoin and the Freedom Revolution
5.1 Introduction to Bitcoin and bitcoin
- **5.1.1** What is bitcoin? What is Bitcoin?
- **5.1.2** What is the difference between Bitcoin and bitcoin?
- **5.1.3** Why learn about bitcoin when I can't afford It?
- **5.1.4** What is bitcoin made of?
- **5.1.5** Why is bitcoin good money?
- **5.1.6** Why should I care?
- **5.1.7** How do you **use** bitcoin?
- **5.1.8** How do you **send** or **spend** bitcoin?
- **5.1.9** How do you **receive** bitcoin?
- **5.1.10** Can Bitcoin be shut down?
- **5.1.11** How does the blockchain keep track of who spends which bitcoin?
- **5.1.12** How do new bitcoin enter the network?
- **5.1.13** What is a bitcoin transaction?
- **5.1.14** Are bitcoin transactions secure?

5.2 Who's Who and What's What in the Bitcoin World?
5.3 Walk Me Through an Actual bitcoin Transaction
- **5.3.1** Class Exercise: Bitcoin Transactions in Action

5.4 What Gives bitcoin Its Value?

Bitcoin is a fascinating and revolutionary digital system that has the potential to transform the way we think about money. But to understand its impact and potential, we need to delve deeper into what it is and how it works. In this chapter, we'll explore the basics of ***Bitcoin*** and ***bitcoin***, including how they differ, why they're valuable, and how transactions work. We'll also take a look at the key players in the ***Bitcoin*** network and walk through a sample transaction. By the end of this chapter, you'll have a solid understanding of ***Bitcoin's*** foundational concepts and be ready to explore its potential for the future.



Watch the following video: "What is Bitcoin? A Simple Explanation" by 3Blue1Brown. You can come back to the key moments anytime, as it is segmented.

5.0 The Enigma of Satoshi Nakamoto: A Glimpse into the Mind Behind Bitcoin and the Freedom Revolution

Satoshi Nakamoto, a mysterious and brilliant innovator, dreamed of a future where financial transactions were borderless, transparent, and secure—free from the grasp of governments and banks. With this vision, Satoshi sparked a Freedom Revolution by creating Bitcoin, the first practical implementation of blockchain technology. ***Bitcoin*** emerged as a symbol of hope and resilience in a world plagued by financial crises and eroding trust in centralized institutions. Driven by a desire to establish a decentralized financial system, it sought to return power to the people, igniting a global movement that challenges the status quo and champions financial freedom.

By harnessing the power of blockchain technology, ***Bitcoin*** marked a turning point in history, catalyzing a revolution with the potential to redefine money and transform the global economy. Satoshi's legacy lives on, despite remaining anonymous, and the impact of their creation is felt around the world. The enigma of Satoshi Nakamoto has only added to the intrigue surrounding the creator of ***Bitcoin***. While some speculate that Satoshi is a group of people, others estimate that they possess a fortune of 1 million ***bitcoin***, making them one of the wealthiest individuals in the world.

Bitcoin Conspiracy and Mystery

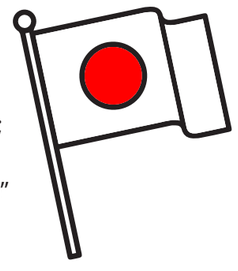


Bitcoin is the brainchild of a mysterious unknown person or group known as **'Satoshi Nakamoto'**.

To this day, nobody knows who the person(s) behind ***Bitcoin*** is.

In Japanese

- "*Satoshi*" translates into "clear-thinking; quick-witted; wise."
- "*Naka*" can mean "inside" or "relationship".
- "*Moto*" is defined as the origin; the cause; the foundation; the basis."



Because of this, some believe that the translation points to ***Bitcoin*** being created by the CIA (Central Intelligence Agency).

Yet more conspiracy theorists believe that four companies are behind things:

Satoshi = **Sa**msung & **Toshi**ba
Nakamoto = **Naka**michi **& Moto**rola

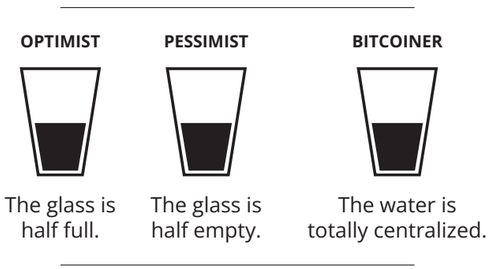
Despite challenges, skepticism, and technical hurdles, ***Bitcoin*** has persevered, inspiring numerous innovations and gaining widespread adoption. Today, it continues to be a symbol of hope, resilience, and the potential to transform the global economy. Satoshi Nakamoto may have vanished from the public eye, but their creation continues to empower individuals and challenge the traditional financial system, offering transparent, equitable, and secure transactions that are permanently recorded on a distributed ledger. The Freedom Revolution, sparked by Satoshi's vision, continues to unfold as a testament to the power of decentralized technology and the unyielding human spirit.

« previous topic next topic »

Pages: [1] print

Author	Topic: Added some DoS limits, removed safe mode (0.3.19) (Read 24633 times)
satoshi (OP) Founder Sr. Member Activity: 364 Merit: 5530	**Added some DoS limits, removed safe mode (0.3.19)** December 12, 2010, 06:22:33 PM *Merited by EFS (100), OgNasty (50), fillippone (50), bumbacoin (50), cloverme (50), sukamasoto (30), yahoo62278 (25), notaek (25), Welsh (20), mindrust (20), legendster (10), dragonvslinux (10), harrymmmm (10), ETFbitcoin (8), aTriz (7), Betwrong (5), Lauda (5), MicroGuy (5), Mrpumperitis (5), TMAN (5), minorman (5), Steeley (5), FrueGreads (4), Danslip (3), finist4x (3), Ryu_Ar1 (3), Yaunfitda (2), Bthd (2), casperBGD (2), Anon136 (2), cinnamon_carter (2), edgycorner (2), Syke (1), LFC_Bitcoin (1), Searing (1), ralle14 (1), HI-TEC99 (1), hatshepsut93 (1), bitcoinPsycho (1), goldkingcoiner (1), crypto_trader#43xzEXrP (1), bill gator (1), famososMuertos (1), denzkilim (1), lx001 (1), akirasendo17 (1), Bardman (1), Woshib (1), ImHash (1), Scorpion (1), Rooster101 (1), dark08 (1), domoy77 (1), lesom (1), ryap12 (1), CoolWave (1), glerant (1), TheArchaeologist (1), ritaconscience (1), nikolaspaolo (1), mx12.levins (1), 1Dq (1), murrayrothbard (1), akopjpuge (1), sigri44 (1), OWZ1337 (1), zantezu (1), EKAloji (1)* #1 There's more work to do on DoS, but I'm doing a quick build of what I have so far in case it's needed, before venturing into more complex ideas. The build for this is version 0.3.19. - Added some DoS controls As Gavin and I have said clearly before, the software is not at all resistant to DoS attack. This is one improvement, but there are still more ways to attack than I can count. I'm leaving the -limitfreerelay part as a switch for now and it's there if you need it. - Removed "safe mode" alerts "safe mode" alerts was a temporary measure after the 0.3.9 overflow bug. We can say all we want that users can just run with "-disablesafemode", but it's better just not to have it for the sake of appearances. It was never intended as a long term feature. Safe mode can still be triggered by seeing a longer (greater total PoW) invalid block chain. Builds: http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/

5.1 Introduction to Bitcoin and bitcoin



On May 17, 2010, the first known exchange of ***bitcoin*** for goods took place. Lazlo Hanyecz purchased two pizzas for 10,000 BTC. How did he do this?

In broad terms, ***bitcoin*** is similar to traditional money, but instead of being physical, it exists only on the internet. To use ***bitcoin***, you have to download a program on your computer. When you run the program, it connects to other computers also running the program. They share a file called the ***blockchain*** which is a big list of all the ***bitcoin*** transactions ever made.

5.1.1 What is bitcoin? What is Bitcoin?

bitcoin (lowercase "b"): It is the digital cash that runs on the ***Bitcoin network***.

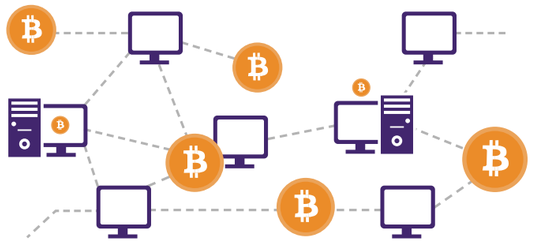
It is a ***currency "b"*** that allows people to send and receive payments online. It is called "digital" because, unlike traditional currencies such as the US dollar or the euro which are physical currencies that can be held in your hand, ***bitcoin*** can only be used with the internet.

Bitcoin (capital "B"): It's everything else; the system, the network, the software, the rules, the community... Satoshi's creation.

The ***Bitcoin network*** "B" is made up of computers from all around the world that work together to process and verify transactions. These transactions are registered on the ***blockchain***.

The rules for using ***Bitcoin*** are implemented in the software that runs the ***Bitcoin network*** and followed by all participants in the network. They are designed so that everyone uses Bitcoin in a fair and predictable way.

The community of people who use and support ***Bitcoin*** is made up of individuals, companies, and organizations all around the world. They are the ones who keep the network functional by using and supporting the currency, running the software that powers the network, and contributing to the network's development.



5.1.2 What is the difference between Bitcoin and bitcoin?



One way to think about the relationship between ***bitcoin*** and the ***Bitcoin network*** is to consider the relationship between an email and the internet. Just as an email is a message that is sent and received over the internet, bitcoin is a digital currency that is transferred and received over the ***Bitcoin network***. The internet provides the infrastructure for emails to be sent and received, while the ***Bitcoin network*** provides the infrastructure for ***bitcoin*** to be transferred and received.



5.1.3 Why learn about bitcoin when I can't afford it?

Have you ever thought about using bitcoin, but have been put off by the high price of one whole coin? Don't worry, you're not alone! The good news is that you don't have to buy a whole ***bitcoin*** to start using it. Just like you can purchase a fraction of a dollar with coins, you can also purchase a fraction of a ***bitcoin***. One ***bitcoin*** is divisible into 100 million units called *satoshis*, so you can buy any amount of ***bitcoin***, even a small amount. Now that you know you can buy as little as 1 cent worth of bitcoin, let's go ahead and explore the possibilities of using this digital currency!

Satoshi	Bitcoin
1	0.0000000**1**
10	0.000000**10**
100	0.00000**100**
1,000	0.0000**1000**
10,000	0.000**10000**
100,000	0.00**100000**
1,000,000	0.0**1000000**
10,000,000	0.**10000000**
100,000,000	**1**.00000000

The symbol for *bitcoin* is ***BTC*** or ฿ and the abbreviation for *satoshis* is ***Sats*** similar to how a dollar is USD or $.

The conversion is ***1 BTC*** = *100,000,000 sats*

- For example, let's say you want to buy an apple that costs $1.40, but you only have ***0.00008 bitcoin***. Don't let the small amount scare you! In fact, when you leave the store after paying, if you check your balance on your phone, you will most likely notice that you have a few sats left to spare.

5.1.4 What is bitcoin made of?

- Nothing that can be physically touched, such as a banknote or dollar bill. They are digital currency units that exist on the ***Bitcoin network*** as a **record of ownership.**

• Just as every dollar bill has its own ***UNIQUE*** **serial number** that is used to identify it and prevent counterfeiting, and every person has their own ID, every ***bitcoin*** **transaction** corresponds to a unique ***bitcoin*** "***fingerprint***" helping to identify the ***bitcoin*** and its **transaction** history.



Serial Number. It is a unique combination of eleven numbers and letters appears twice on the front of the note. Each note has a unique serial number.



= 79054025255fb1a2

Bitcoin Transaction. Each bitcoin transaction has a unique digital fingerprint.

• In today's virtual age, it is possible for things to be real and valuable even if they do not have a physical form.

5.1.5 Why is bitcoin good money?

Characteristic	Why **bitcoin** is good money.
Durable	It **is a** digital currency and is not subject to physical wear and tear. **Like gold**.
Portable	It can be easily stored and transferred digitally, making it convenient to carry anywhere. **Like cash, but better.**
Uniform	All ***bitcoin*** are worth the same, no matter where they are used or who owns them. **Like cash, but better.**
Acceptable	Every day more people around the world accept bitcoin as a form of payment. **Like cash, but better.**
Scarce	The total supply of ***bitcoin*** is limited, 21,000,000 to be exact, making it valuable and desirable. **Like gold, but better.**
Divisible	It can be divided into smaller units, called **satoshis**, allowing for smaller transactions. In theory, because it is digital, a ***bitcoin*** is infinitely divisible. **Like cash, but better.**

5.1.6 Why should I care?

Faster, Cheaper Payments

Send money across the globe in minutes, with extremely low fees.

Financial Inclusion

2.5 billion unbanked people can have access to money via a phone or a computer.

Increased Privacy

Bitcoin transactions are public, but your identity is not.

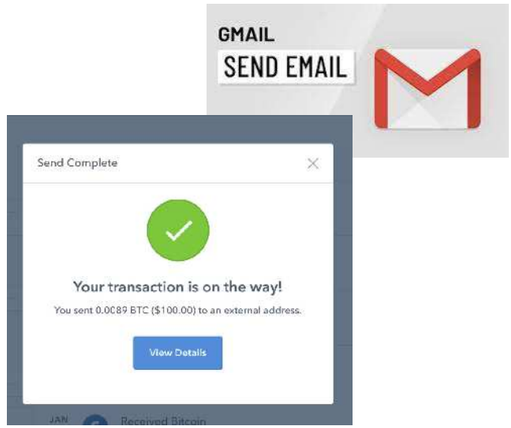
Blockchain Technology

The technology behind Bitcoin will power the future of many different industries.

*5.1.7 How do you **use** bitcoin?*

To use ***bitcoin***, you'll need to set up a digital wallet on your computer or phone. You can use your wallet to store, send, or receive ***bitcoin*** from other people, or even to buy things online.

*5.1.8 How do you **send** or **spend** bitcoin?*



All you need is an internet connection.

• The process of sending bitcoin is just like sending an email. To send an email, you open your email client, enter the recipient's email address, type a message, and click send. In a similar fashion, to send ***bitcoin*** to someone or spend ***bitcoin*** when you are purchasing something in exchange, you open your bitcoin wallet, enter the recipient's ***bitcoin*** address, enter the amount of ***bitcoin*** you want to send (or spend), and click send.

*5.1.9 How do you **receive** bitcoin?*

To get ***bitcoin***, you can either buy it online, accept it as a gift from someone or as payment for goods or services, or "mine" it (work hard for it) by using a computing device. With any of these forms, once you get it, you will store it in a "wallet".

5.1.10 Can Bitcoin be shut down?

Governments may try to make it difficult for people to **use** ***Bitcoin***, but it is difficult to completely shut down the network. This is because ***Bitcoin*** is decentralized, meaning there is no central company or organization that controls it. Instead, the software is **open-source**, which means anyone can download, use, and run the software on their own computer.

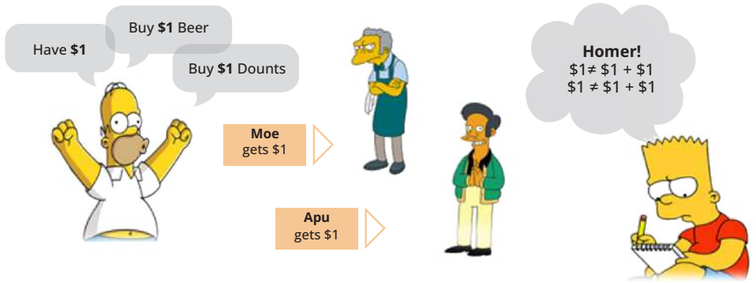
Governments may try to **restrict access** to ***Bitcoin***, but this is similar to the way governments try to control access to the Internet. People can use tools like VPNs to bypass these restrictions. Additionally, due to the digital nature of ***Bitcoin***, it can be hidden relatively easily. It is much more difficult for governments to locate and confiscate ***bitcoin*** than it is to locate and confiscate physical assets like gold or real estate.

Despite being illegal in some countries, people continue to access the ***Bitcoin network***. Additionally, some countries have attempted to control ***Bitcoin*** by creating their own central bank digital currencies, which could have varying outcomes. Some people may accept and adapt to the new centralized system, while others may reject it and further pursue decentralized solutions like ***Bitcoin***.

5.1.11 How does the Blockchain keep track of who spends which bitcoin?

You know how you can't spend the same dollar bill twice? ***Bitcoin*** similarly works to make sure that you can't spend the same digital coin twice.

You see, before ***Bitcoin***, it was possible to send transactions across a network of computers, but there was a problem: people could send conflicting transactions, like trying to spend the same coin twice. This is called "**double-spending**".



Bitcoin solves this problem by making all the computers on the network work together. When a new transaction is sent, it's sent to all the computers, and they keep it in memory before writing it to a permanent file (the *blockchain*).

This process is called "**mining**", and it makes sure that no double-spending transactions ever get written to **the file**. It's like a big competition that nobody can cheat, so your ***bitcoin*** are always safe.

This is how *Bitcoin* reaches consensus, all without a single punch being thrown!

At regular intervals, one of the computers gets to add all the transactions it has in memory to the file. Then it shares the updated file with all the other computers on the network. All the computers agree on which transactions are valid, and which aren't, and they remove any conflicting ones from their memory.

5.1.12 How do new bitcoin enter the network?

To **reward miners** for their job, every time they add a new block to the *blockchain*, they get compensated with newly minted ***bitcoin***. Currently miners get paid 6.25 BTC for every block they mine.

5.1.13 What is a bitcoin transaction?

A ***Bitcoin*** **transaction** is a record of value transfer between two parties. Each **transaction** has an **input** and an **output**. The input is the amount of ***bitcoin*** being sent, while the output is the address of the recipient's ***Bitcoin*** wallet.

Here's an analogy to help you understand ***bitcoin*** transactions: imagine you have a jar of marbles, and you want to transfer some of them to a friend. You would count out the number of marbles you want to give your friend, and put them in a separate jar with your friend's name on it. This is similar to how a ***bitcoin*** **transaction** works: you take a certain amount of ***bitcoin*** from your wallet and send it to your friend's wallet.

- Marc and Roby want to exchange 1 BTC. To understand this, it's important to know that there are no physical coins in ***bitcoin***, only updates to the *blockchain*, which then get reflected in the wallets of both parties involved.
- When Marc wants to send 1 BTC to Roby, it's called a **peer-to-peer** transaction because the ownership of the value goes directly from Marc to Roby. But Roby doesn't actually receive a "digital coin" from Marc. Instead, all the nodes in the network update their local copy of the public ledger, which changes the ownership of the ***bitcoin*** from Marc's address to Roby's address.
- A ***bitcoin*** **transaction** is simply a **signed message** that Marc sends to the network, which is then validated by many nodes. The message goes through several steps, like being picked up by some of the full nodes, being validated, and then being broadcasted, until all the nodes in the network have independently validated it.

The signature is a digital representation of the **transaction details**, including the amount of ***bitcoin*** being sent, the **sender's address (Marc)**, and the **recipient's address (Roby)**.

Purpose of a Digital Signature



A signature confirms that the message (document or email) originated from the sender and has NOT been modified.



Imagine all existing ***bitcoin*** as being stored in digital safes, each with a different amount of BTC along with a history of how they got there.

Each safe has an owner. Therefore, it has to be identifiable with an **address**. Addresses are protected by a digital lock with two different keys, like passwords to an account. If a safe has ***bitcoin***, its owner can open it with his **private key** and transfer any desired amount of ***bitcoin*** to another safe.

From Roby's perspective: To **receive** ***bitcoin***, you need to provide the sender (Marc) with your **address** where ***bitcoin*** can be deposited.

From Marc's perspective: To **spend** your ***bitcoin***, you need to access **your private key** for it to be unlocked.

5.1.14 Are bitcoin transactions secure?

The transaction details, such as the sender and recipient addresses and the amount being transferred, are publicly visible on the *blockchain*, but the ownership of the ***bitcoin*** being transferred is verified through the use of cryptography.

What is Cryptography?

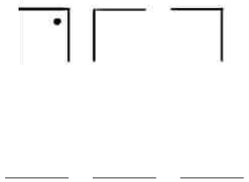
Cryptography is a way of keeping information secret by disguising it in code.

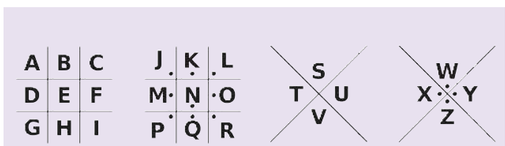


How to Solve
Pigpen Cipher

When solving the Pigpen Cipher, the player is given an encrypted message and a cipher. To decrypt the message, the player will find the symbol from the encrypted message on the cipher to find the decrypted letter.

- Example of an encrypted message:





- **Encryption** is the process of taking information and putting it in a special code, making it unreadable to anyone without the correct decryption method. This is similar to locking a safe, where only the person with the correct key or combination can open it.
- On the other hand, **decryption** is the process of taking the coded information and **making it readable again**, like unlocking the safe and being able to read the information inside.

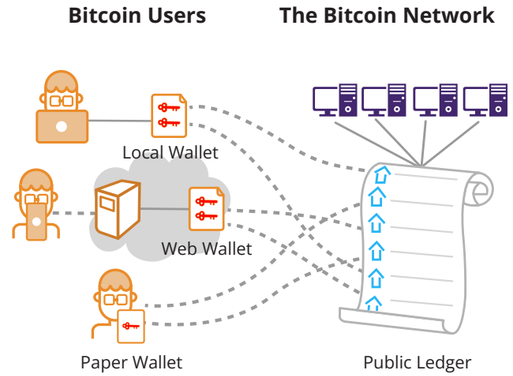
For instance, let's say Arel and John want to keep a message hidden from someone named Ronny. They agree to use a secret key to disguise the message before sending it to each other. They could use a simple method like shifting each letter of the message down the alphabet, so that A becomes B, B becomes C, and so on. Only those with the key can decrypt the message, making it unreadable to Ronny. Though this method is not considered secure today, it illustrates the principle of private-key cryptography.

How Does Cryptography Work in Bitcoin Transactions?

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

However, Ronny could also intercept the message and use the same key to unscramble it and read the message.

With **public key cryptography**, which is the type of cryptography used in bitcoin transactions, John and Arel each have two keys: a **public key** and a **private key**. John can use Arel's **public key** to scramble his own message before sending it (to Arel). Only Arel's **private key** can unscramble the message. Ronny, who does not have Arel's **private key**, would not be able to read the message even if he intercepts it.



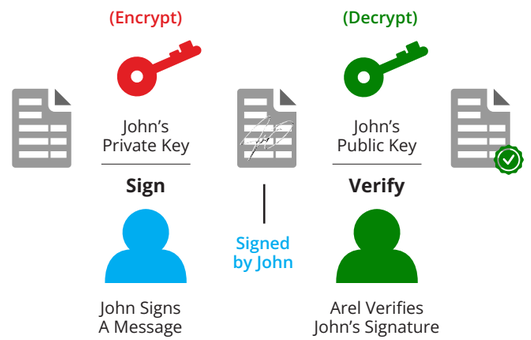
In addition to encrypting messages, **public key** cryptography can also be used for digital signatures. A digital signature is a way to prove the authenticity of a message, similar to a written signature on a physical document. In order to create a digital signature, John would use **his private key** to **encrypt his signature**. Arel then uses John's **public key** to decrypt it and verify that it was indeed sent by John.

Public Key Cryptography (For every transaction between two users):

Each user has two keys; a **private key**, which is kept secret, and a **public key** that can be shared with others.

The **private key** serves as a form of identification and proof of ownership, confirming: **"This address belongs to me and I have control over it"**

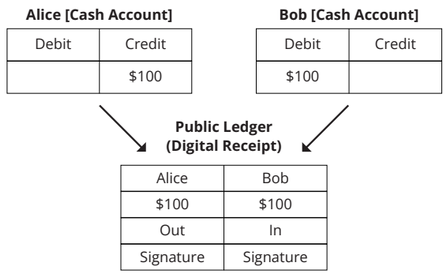
Digital signatures are created to identify unique transactions.



So the main advantage of **public key cryptography** over private key cryptography is that it allows for secure communication without the need for the sender and receiver to first share a secret key, which could be intercepted by a third party.

- ***Bitcoin*** transactions involve transferring a certain amount of ***bitcoin*** **directly** to another person's account.
    - You wouldn't want someone to just steal the money your friend sent via Venmo because the payment rail is insecure, would you?

- Encryption is a way to keep important information guarded from malicious actors as it travels through the network, some of whom, such as hackers, might deviate the funds to their account instead.



- As an additional measure of protection, to keep the **transaction details** safe and secure in ***Bitcoin***, a ***UNIQUE*** signature is added to each transaction. This signature acts like a secret code that ensures that no one can change any part of the transaction without the software detecting it and marking it as invalid.

Comparing Bitcoin Transactions to Traditional Banking

- In traditional banking, a **PIN** is used to authenticate transactions, similar to how a **private key** is used to sign transactions in *blockchains*.

A simple analogy for this process would be a person accessing their bank account number with a private pin (**private key**), and then using their own personal signature (**unique signature**) on an online check (***digital currency***) to send money (**make a transaction**) to someone else (another user). Just like how a person's signature on a check verifies their identity and authorizes the transaction, the digital signature using a **private key** verifies the identity and authorizes the transaction of digital currency.



5.2 Who's Who and What's What in the Bitcoin World? Identifying the Key Roles in the Network

There are three main types of participants in the ***Bitcoin*** network:

1. ***Miners*** are computers in the ***Bitcoin Network*** that *write and verify new transactions on the blockchain by appending new blocks to it*. Miners are rewarded with ***bitcoin*** for the work they do!

2. ***Nodes*** are computers in the ***Bitcoin Network*** that *store and verify* blockchain transactions and blocks. Nodes do not get rewarded for their work.

3. ***Developers*** are responsible for maintaining and proposing improvements to the ***Bitcoin*** software (ie. the code). They ensure that every computer on the network follows the rules and operates smoothly.

Overall, these three groups work together to keep the ***Bitcoin Network*** running and ensure that it remains secure and decentralized.

- **Users** are regular individuals who use ***bitcoin***. They send and receive ***bitcoin*** via their *wallets* and can also make purchases or exchange it for other currencies.
- **Exchanges** allow users to buy, sell, and trade ***bitcoin***, and facilitate transactions on the network. However, exchanges do not play a direct role in the operation of the ***Bitcoin Network*** itself.

Still a little confused? Going back to our analogy where the ***Bitcoin Network*** is like a transportation system, we will reintroduce the key players.

- **Miners** are like ***automated toll booths or bookkeepers***.
    - They are responsible for the bookkeeping. They register every car that passes by and charge fees. They also verify that the cars (bitcoin transactions) passing through are not stolen, have expired license plates or are driven by unlicensed or drunk drivers.
    - This process helps to ensure that the highway system (***Bitcoin Network***) is safe and efficient, and helps to prevent collisions or fraud.



● **Nodes** can be thought of as ***service plazas*** along the roads.



• Just as a service plaza is a place to stop, get food, or use restrooms, a node on a *blockchain* network is a point where transactions are processed, validated, and stored.

• Just like service plazas have rest areas and parking lots, nodes have their own waiting rooms (mempool) for verified transactions to chill before they continue on to the *blockchain*.

• Plazas do not charge for your stay or usage of the location.

● **Developers** are like the ***engineers*** who design and build the highway system.



• They are responsible for maintaining and improving the infrastructure of the network, such as fixing any issues that may arise or adding new features.



A **bitcoin wallet** is like a ***garage*** for your car. Just as a garage is a secure place to store your car when it is not in use, a **bitcoin wallet** is a secure place to store your ***bitcoin***.



• Let's say you own a ***car*** (a ***bitcoin***) and you want to keep it safe when you are not driving it. You can put it in your ***garage*** (a bitcoin wallet) and ***lock the door*** (lock your wallet with a **password**). This will protect your car (***bitcoin***) from thieves (hackers). When you want to use your car (spend your bitcoin), you can open the garage door and unlock your wallet with another **password**, which is needed to ***turn the car on*** and ***drive it out*** of the garage (make a transaction).





Exchanges can be thought of as ***car dealerships***. Just as a dealership allows you to buy and sell cars, an exchange allows you to buy and sell ***bitcoin***.

• For example, if you want to sell your car (***bitcoin***), you can take it to a dealership (exchange) and they will help you find a buyer.

Let's look at ***Bitcoin*** in terms of a car sale:

Imagine you, the user, have a valuable asset, like a ***bitcoin***, that you want to sell. You take it to an exchange, similar to a dealership, to find a buyer. Along the way, you pass through the network's nodes, similar to a service plaza, to ensure that your asset is in optimal condition before the sale. The transaction then goes through a rigorous verification process with the exchange's financial department, similar to bookkeepers in a dealership, to ensure that everything is accurate and the sale goes smoothly. Once the sale is complete, you receive payment in fiat currency and the exchange takes possession of the asset, transferring it to their wallet. The network also has a team of developers, similar to engineers in a dealership, working on improving and updating ***Bitcoin***'s features and technology. Other participants in the network, such as merchants and investors, also play a role in the functioning of the ***Bitcoin Network***.

5.3 Walk Me Through an Actual bitcoin Transaction

New ***Bitcoin*** transactions are initiated from wallets around the world, but there is no central payment processor. Instead, **miners** around the world compete to **record** transactions in the ledger.

Let's say Jim owes Eliana ***0.5 BTC*** and is ready to pay her back. Both have digital wallets.

1. Eliana shares her **address** with Jim.
2. Jim uses his wallet software to create the **transaction**, which includes Eliana's **address**, the amount to be transferred (0.5 BTC), and a fee for the miner.

When Jim clicks "send," his wallet uses his **private key** to unlock 0.5 BTC, as this is how he "signs" the transaction. He **does not actually reveal his private key** though.

- By doing this, Jim is informing the network "**I am the owner of this account and I approve the transfer of 0.5 *bitcoin* to Eliana's account**."

LEDGER

Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.50
Robert	2.00
Eliana	1.75
Daniel	5.25

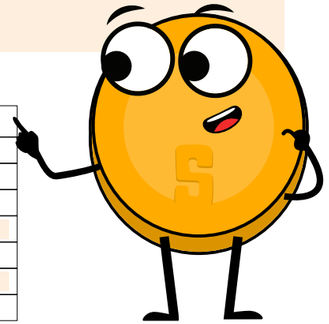
Bitcoin Transaction Request Message

Jim sends 0.50 BTC to Eilana

Jim ▸ Eilana 0.50 BTC

LEDGER

Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	**1.00**
Robert	2.00
Eliana	**2.25**
Daniel	5.25

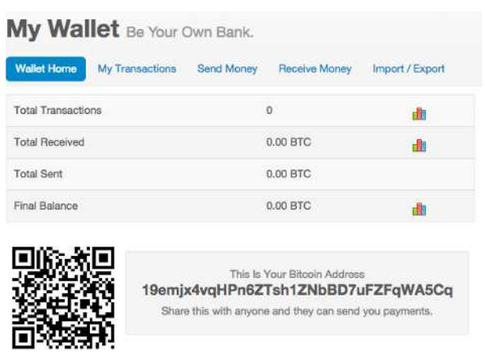


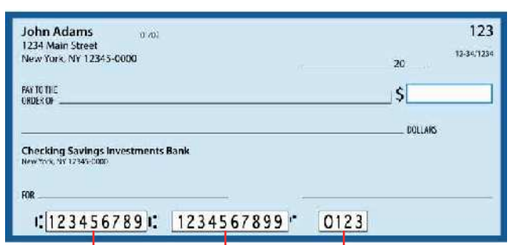
3. After signing the transaction, it is **broadcast** to the network where it is verified by nodes called miners. Miners check the transaction for validity and ensure that Jim has enough funds. If he does not, they reject the transaction immediately.
4. Once the transaction is verified and included in a block, it is added to the *blockchain*, and the funds are transferred to Eliana's address.
5. Eliana can then use her **private key** to access the transferred funds in his wallet.

It's important to note that once the transaction is complete, it cannot be reversed.

Now with a bit of detail

After opening his digital wallet, Jim, via his own **address**, initiates the transaction by requesting and including Eliana's **bitcoin address** (similar to writing a routing number for a traditional bank transfer) and the amount of ***bitcoin*** to be sent. Jim signs the transaction with his **private key** (similar to accessing an account with a private password) to validate the transfer.

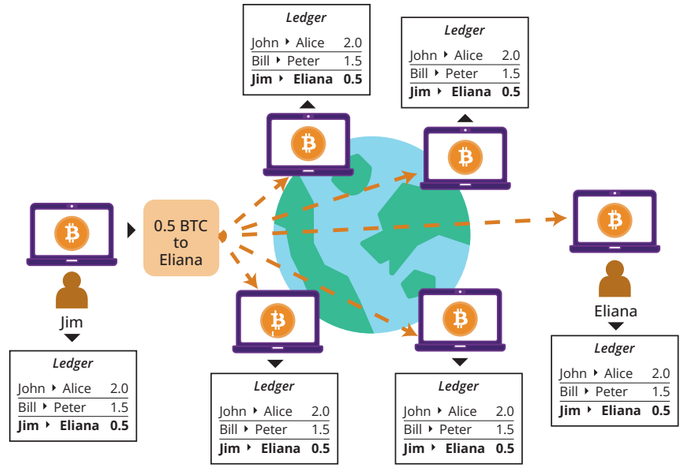




Next, the **transaction is broadcasted onto the network** with just a click of a button.

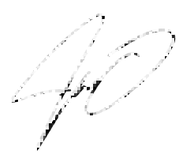
A transaction on the ***blockchain*** can be thought of as a package delivery process. When a package is first sent, it is just one package in **one** post office (one transaction sent to a first node). The post office (node) **verifies** the package's authenticity, and if it is valid, it sends it on to other post offices (nodes) for further verification. The package is passed along from post office to post office until it reaches every post office in the network (all the nodes in the *blockchain*). The package's authenticity and validity are confirmed at each stop, similar to how a transaction is verified by multiple **nodes** on the ***blockchain***.

- Eliana's unique address is generated using her **public key** to ensure that only she can access and unlock the funds, similar to solving a puzzle where only those with the correct pieces can open it.



In order to **verify** the authenticity of the transaction, a digital signature and a **public key** are used.

The digital signature and the **public key** are two important pieces of the puzzle. The **public key** acts like an identification card, making sure that Jim is the rightful owner of the ***bitcoin***. The digital signature proves that Jim has authorized the transaction, like he's signing a check.

	Handwritten Signature	Digital Signature
Concept		Digital Signature using Asymmetric Encryption // Decryption Method **732070795917431371 99** **612884145455952927 84** **330600399365338469 24**
Problem	Reusable	Impossible to Reuse



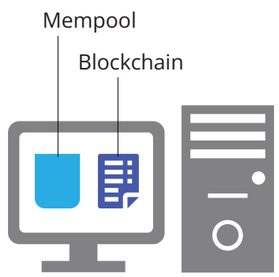


The **nodes** in the ***Bitcoin Network*** **are like puzzle checkers.** They have to verify that all the pieces fit together correctly. They make sure that Jim both owns the ***bitcoin*** and authorized the transaction.

Once a majority of the nodes are in consensus that the puzzle is solved correctly, the transaction is considered legitimate and is added to a **queue**.

This queue of pending transactions is called the "**mempool**."

A Node in the Bitcoin Network



The **mempool** is like a waiting area for puzzles that have been solved correctly, but haven't been added (chained) to the permanent puzzle (***blockchain***) yet. It is located in a different section of a node's memory storage compared to the *blockchain*, which permanently records confirmed transactions.

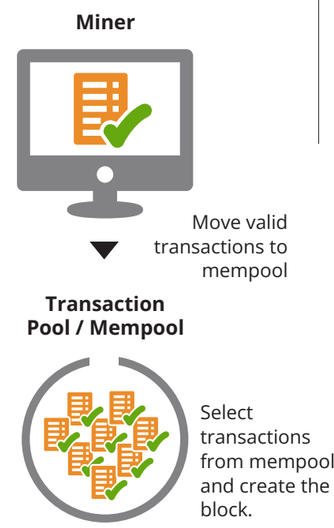
Once transactions are verified, they must be recorded permanently on the ***blockchain***. A group of **nodes** called "**miners**" compete to be the first to add them to the ***blockchain*** in order to receive a reward.

Meet the superheroes of ***Bitcoin***: **miners**! These special computers use their super-powered software to check that nobody is **double-spending**, stealing, or accidentally sending funds they don't have, and they make sure all the other miners are doing the same.

- **Miners** are like puzzle curators, they select which puzzles from the queue to add to the final puzzle exhibit, this process ensures that the same bitcoin can't be spent twice by the same person and that transactions are processed quickly.

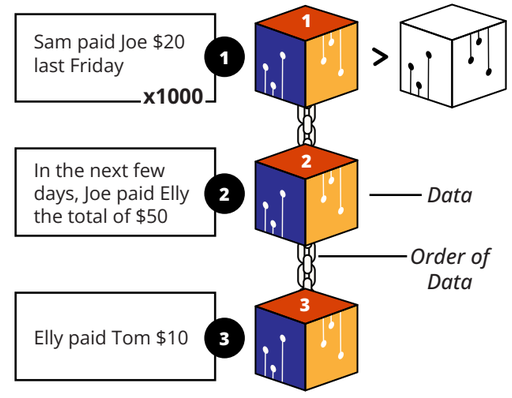
Miners keep a copy of the *blockchain*, and they check each transaction against the blockchain to **confirm** that the same ***bitcoin*** haven't been spent before. Only legitimate transactions that meet certain criteria, such as having the correct **digital signature** and enough funds, are added to the *blockchain* by the miners.

Once on the ***blockchain***, the transactions included on the block are considered complete and irreversible. The exchange of ***bitcoin*** from one address to another is settled.

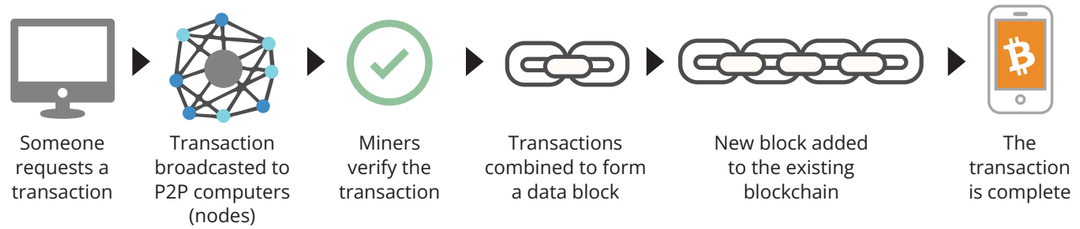


In summary, using ***Bitcoin*** involves creating a transaction, broadcasting it to the network, and validating and confirming it. This process ensures that the transaction is secure and cannot be changed, allowing people to trust the system without the need for a central authority.

Example of a Transaction on a Blockchain



How a Bitcoin Transaction Works



5.3.1 Class Exercise: Bitcoin Transactions in Action

Miners are responsible for adding new transactions to the *blockchain*. Full nodes validate transactions and store a complete copy of the *blockchain*. Light nodes let people validate transactions while using less storage and fewer computational resources.

Class Exercise. Let's assume that the sender and receiver are light nodes. In reality, not all wallets are light nodes.

Understand your role. You have been assigned one of the following roles: ***sender, receiver, node, or miner***.

• *Senders* will be responsible for creating and broadcasting transactions.
• *Receivers* will be responsible for receiving and verifying transactions.
• *Nodes* will be responsible for validating the transactions by checking that the transaction is valid. They'll do this by checking it against the rules of the protocol and the consensus mechanism.
• *Miners* will be responsible for adding the transactions to the *blockchain*.

1. **As a sender**: Create a transaction. To create a transaction, follow these steps:
☐ Take a transaction note and write the number of coins you want to send and the name or initials of the receiver.
☐ Sign the note with your name or initials, simulating a **private key**.
☐ Pass the transaction note and the corresponding number of ***coins*** to the receiver.

Both nodes and receivers have to verify transactions:

2. **As a receiver**: You are responsible for verifying the transactions. Follow these steps:
☐ Check the transaction note to ensure that the correct number of coins and the receiver's name or initials are written.
☐ Count the coins received and compare them to the number of coins written on the note.
☐ If the coins match, check the approval box.
☐ If the coins do not match or you have doubts, reject the transaction.

Coin Sent	Sender	Sender Signature	Receiver	Date & Time	Recipient Approval

3. **As a node**: Verify and validate transactions. You are responsible for checking that the transaction is valid.
☐ Verify that the sender's address is valid and that the receiver's address is valid.
☐ Check that the sender has enough funds to complete the transaction and that the transaction does not double-spend any coins.

Coin Sent	Sender	Sender Signature	Receiver	Date & Time	Node Approval

4. Add transactions to the *blockchain*: **As a miner**, you are responsible for adding the transactions to the *blockchain*. Follow these steps:
☐ Check the transactions that have been approved by the receivers and validated by the nodes.

☐ Roll the dice and compare the numbers with the other miner. The miner with the smaller number will add the transaction to the blockchain.
☐ For your time, energy, and effort, you will receive a reward. Go select a candy of your choice.
☐ Once a transaction is added to the *blockchain*, it cannot be changed or reversed.

5. Keep track of your ***coin*** balance: Throughout the activity, keep track of your coin balance by counting the coins in your digital wallet.

Coin Sent	Sender	Sender Signature	Receiver	Date & Time	Approval

6. Discuss the concepts learned with your class.

5.4 What Gives bitcoin Its Value?

Unlike traditional forms of currency, such as gold or fiat money, ***bitcoin*** is digital, decentralized, and scarce. These properties give it a number of advantages over traditional forms of money, and make it a valuable store of value and medium of exchange.

Bitcoin gets its value from a combination of factors, including:

• Its scarcity, as the total amount of ***bitcoin*** that can ever be made is limited to 21 million, which makes it different from regular money that can be printed by governments.

• Its utility as a decentralized digital currency, which means it is not controlled by any government or institution and can be used for transactions anywhere in the world.

• Perceived value by investors and users, as some people see ***bitcoin*** as a good investment, a way to store money or a protection against inflation.

What is the market demand for bitcoin and how does it influence its price?

The market demand for ***bitcoin*** refers to the amount of people who are willing to buy bitcoin at a certain price. The price of ***bitcoin*** is influenced by market demand, as well as supply and other economic factors. When demand is high and there is a limited supply, the price of ***bitcoin*** tends to increase. Conversely, when demand is low and there is a large supply, the price of ***bitcoin*** tends to decrease.

One of the main arguments against ***bitcoin*** is that it is not backed by any physical assets or government guarantees, making it inherently worthless. However, this argument misunderstands

the nature of money. **Money does not have to be backed by physical assets or government guarantees to be valuable; it simply needs to be widely accepted as a medium of exchange and a store of value. *Bitcoin* meets these criteria and then some.**

Bitcoin's virtually untouchable status, which makes it difficult to confiscate, is a major factor in its value to those who fear authoritarian or tyrannical regimes. This attribute is seen as more valuable than the physical characteristics of an asset by some.

Finally, ***bitcoin*** is also versatile, with its underlying technology blockchain has been applied to various industries such as supply chain, digital identity, and more, making it a valuable commodity in many different industries.

- ***Bitcoin*** is being seen as a solution to the world's economic problems, as it is fair, secure, and incorruptible.

- ***Bitcoin*** is being referred to as digital gold, and its demand is expected to continue to grow as more people take control of their wealth.

- While there may be ongoing debate about ***bitcoin***'s role as a medium of exchange, it's important to recognize the significant progress that has been made in recent years to increase its acceptance as a viable option for transactions. With the rise of new technologies and innovative payment solutions, ***bitcoin*** is increasingly being seen as a practical and efficient medium of exchange, particularly in the realm of cross-border transactions. As more businesses and individuals recognize the advantages of using ***bitcoin*** for everyday transactions, its potential to become a widely accepted medium of exchange continues to grow.

Satoshi Nakamoto's creation of ***Bitcoin*** was not just about developing a new technology, but about solving the root cause of the world's biggest problems. In the aftermath of the 2008 financial crisis, he saw the need for a decentralized, transparent, and secure financial system that would empower individuals and remove the control of centralized institutions. His vision was to create a better world that was more equitable, just, and peaceful, where people had greater financial freedom, autonomy, and control over their wealth. By understanding the true intention behind ***Bitcoin's*** creation, we can be inspired to continue working towards our end goal of a world where people live in freedom, abundance, and happiness together.

Chapter #6

Bitcoin Wallets Unlocked: Navigating Self-Custody and the Lightning Network for Secure Transactions

6.0 From Novice to Pro: Navigating the World of the Bitcoin Wallet
6.1 The Process of Onboarding and Securing your bitcoin
- **6.1.1** Class Exercise: Mastering Self-Custody and Using Your Wallet With Confidence
- **6.1.2** Class Exercise: How do I Receive bitcoin (in detail)
- **6.1.3** Class Exercise: How Do I Send bitcoin and Pay for Goods and Services (in detail)

6.2 On-Chain vs. Off-Chain
6.3 The Lightning Network
- **6.3.1** A Lightning Transaction
- **6.3.2** Class Exercise: Lightning Wallet Relay Race
- **6.3.3** Class Exercise: Lightning Online Interactive Demo

6.0 From Novice to Pro: Navigating the World of the Bitcoin Wallet

When Sats are purchased for the first time, they will be credited to a virtual account, similar to how funds are deposited into a bank account.

The key difference is that while a bank account is centralized and subject to government regulations, a **bitcoin wallet** is decentralized and operates on a **person-to-person** network.
- ***Bitcoin*** has no central point of failure, but it is important to be cautious as someone's ***bitcoin*** can be in the possession of a third party, who is managing it.

- This virtual account, often referred to as a "wallet," is protected by a ***master private key***, much like how a bank account is protected by a *personal PIN or password*. Just as you have control over the funds in your bank account, you can control the Sats in your wallet, and use them to make purchases or transfer them to other accounts.

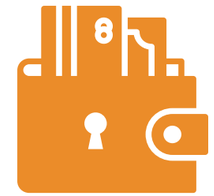
- Just as a locksmith can create any number of keys that can be used to open locks, a ***recovery or backup phrase*** (*or master private key*) can be used to generate any number of **private keys** that can be used to access your Bitcoin wallet. You could say that a ***recovery phrase*** is like a locksmith, and the **private keys** are the keys that are created by the locksmith.

This table includes the two main types of bitcoin wallets, **self-custodial** and **custodial**. You can see the benefits and risks of using each wallet type and who controls the bitcoin in each case. Self-custodial means the user holds the **private keys**, *which means they are in true possession of their **bitcoin***, while with the second type, the *third party holds them*.

Wallet Type	Who controls my bitcoin?	Benefits	Risks
Self-Custodial Wallets	The user	Complete control over funds and transactions, no approval process or account freeze, no corporate or government control, protected against arbitrary confiscation, like keeping money at home.	No recovery if ***recovery phrase*** is lost, less customer support, full responsibility falls on the user.
Custodial Wallets	The third-party provider	Easy recovery if access is lost, easier customer support	Funds are always connected to the internet, more vulnerable to hacking and breaches. Custodians control and can freeze accounts.

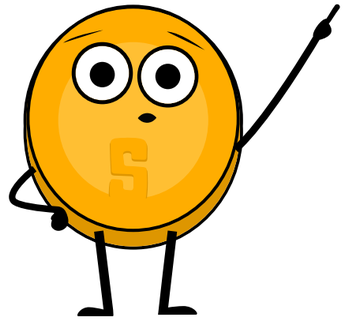
In a **self-custodial wallet** (also called **non-custodial wallet**,) you are the only one with the **keys** to the wallet and **you have full control over what goes in and out**. On the other hand, in a custodial wallet, someone else holds the key and can access and manage the contents of the wallet on your behalf.

- Self-custody is like being your own bank. Transactions are not subject to control or authority by any government or company, but it also means you bear full responsibility for keeping your ***bitcoin*** secure.
- Self-custody ensures that third parties cannot confiscate your ***bitcoin*** without your consent.
- Self-custody gives peace of mind in times of uncertainty, knowing your ***bitcoin*** is secure.



It's important to choose the right type of wallet for each individual's needs. Sometimes people find it hard to distinguish whether they are installing a custodial or a self-custodial wallet. This table shows the differences in installation process.

Wallet Type	Step 1: Choose a Wallet	Step 2: Install the Wallet	Step 3: Create a New Wallet	Step 4: Secure Your Seed Phrase	Step 5: Start Using Your Wallet
Self-Custodial Wallets	Choose a self-custodial wallet provider	Follow the wallet provider's instructions	Generate ***recovery phrase*** and at least one **private key**	Store the ***recovery phrase*** in a secure location	Start using the wallet to receive and send ***bitcoin***
Custodial Wallets	Choose a custodial wallet provider	Follow the wallet provider's instructions	Create an account with the wallet provider	N/A (wallet provider holds the **private keys**)	Start using the wallet to receive and send ***bitcoin***



When it comes to storing your ***bitcoin***, it's not just about who has control over it - there are many other risks to consider as well. That's why it's important to find a storage solution that is both secure and convenient.

Wallet Type	Description	Advantages	Disadvantages	Example User
Online Wallet	A wallet that is accessed through a web browser.	Accessible from any device with an internet connection. Easy to use.	Less secure. Can be hacked or compromised.	Someone who needs to access their wallet frequently and doesn't have a lot of funds to store.
Mobile Wallet	A wallet that is installed on a mobile device.	Convenient. Can be accessed from anywhere.	Can be lost if the device is misplaced, stolen, or hacked.	Someone who needs to make transactions on the go and doesn't have a lot of funds to store.
Desktop Wallet	A wallet that is installed on a desktop computer.	More secure than online wallets. Can be used offline.	Can be hacked if the computer is infected with malware.	Someone who wants to store a large amount of ***bitcoin*** and is comfortable with using a desktop computer.
Hardware Wallet	A physical device that stores ***bitcoin*** offline.	Very secure. Can be used offline.	Funds could be unrecoverable if the device is lost or stolen.	Someone who wants to store a large amount of ***bitcoin*** and is willing to pay for the added security of a hardware wallet.
Paper Wallet	A physical record of a bitcoin wallet's private and public keys.	Very secure. Can be used offline.	Can be lost or stolen if the physical record is lost or stolen.	Someone who wants to store a large amount of ***bitcoin*** and is willing to take the added precautions to ensure its security.

Analyze the trade-offs of the wallets and know there is no ideal wallet that satisfies all needs.

- When choosing a ***Bitcoin*** wallet, there are several things you should consider:

- **Security**: Make sure the wallet has strong security measures in place, such as two-factor authentication and secure password policies.
- **Privacy**: Consider whether the wallet allows you to remain anonymous, or if it requires personal information to set up an account.
- **Ease of Use**: Choose a wallet that is easy to use and navigate, especially if you are new to ***bitcoin***.
- **Compatibility**: Make sure the wallet is compatible with your device and operating system.
- **Fees**: Compare the fees charged by different wallets to make sure you are getting the best deal.
- **Reputation**: Research the reputation of the wallet and its team to make sure it is trustworthy.
- **Control**: Some wallets give you more control over your private keys, which can be a security advantage. Consider whether you want a wallet that gives you full control, or one that is more user-friendly but may have less control.

You can always transfer your funds to a different wallet later.

6.1 The Process of Onboarding and Securing Your bitcoin

Onboarding into ***Bitcoin*** refers to the process of acquiring and using ***bitcoin***.

Before moving any further, it's important that we learn the steps for **onboarding** and familiarize ourselves with the process for **buying** and **securing** ***bitcoin*** safely.

1. **Choose a bitcoin exchange, peer-to-peer exchange, or *bitcoin* ATM**: There are different options for buying ***bitcoin***, including traditional exchanges, peer-to-peer exchanges, and ***bitcoin*** ATMs. Choose a platform that meets your needs and is reputable.
2. **Open the app and receive your 12- or 24-word recovery phrase.** Write down the phrase in a safe place. The recovery phrase is used to restore access to your wallet if you lose your device or forget your password. Once you have written down the recovery phrase, you can enter it into the app to access your wallet.
3. **Connect a payment method**: Most platforms will allow you to connect a bank account, credit card, or debit card to fund your account. Follow the platform's instructions to add your payment method.
4. **Place an order**: Once your account is set up and funded, you can place an order to buy ***bitcoin***. The platform will provide you with a price quote and you can specify the amount of ***bitcoin*** you want to buy.
5. **Confirm the transaction**: Review the details of your transaction and **confirm the purchase**. The platform will process the transaction and the ***bitcoin*** will be transferred to your account on the platform.
6. **Withdraw the *bitcoin***: If you want to transfer the ***bitcoin*** to a self-custodial wallet, you will need to ***withdraw the bitcoin from the platform and send it to your wallet***. The platform will provide instructions for how to do this.

Risks Associated with KYC-Exchanges

It's important to note that when buying bitcoin through a KYC-exchange, you are required to provide personal information and verify your identity. This creates a risk of identity theft and puts your personal information at risk. Additionally, KYC-exchanges hold your private keys, which means you don't have full control over your bitcoin.

To minimize these risks, consider using alternative options for buying bitcoin, such as peer-to-peer exchanges or Bitcoin ATMs.

"Not your keys, not your coins"

This is a popular saying among ***bitcoin*** holders. It refers to the idea that if you don't have direct control over the private keys associated with your bitcoin wallet, you don't have true ownership of the coins.

The **private key** is a secret code that allows you to access your ***bitcoin*** and spend it. When you store your ***bitcoin*** with a third-party service, like an exchange or online wallet, you are relying on that service to keep your private key safe. If the service is hacked or goes out of business, you could lose access to your ***bitcoin***.

So, the saying "**Not your keys, not your coins**" is a reminder that it's important to take control of your own **private keys** and store them securely. By doing this, you can ensure that you have full control over your ***bitcoin*** and can access it whenever you want.



6.1.1 Class Exercise: Mastering Self-Custody and Using Your Wallet With Confidence

If students do not have cell phones, the teacher will provide one to each student to borrow. There are two options for this activity:

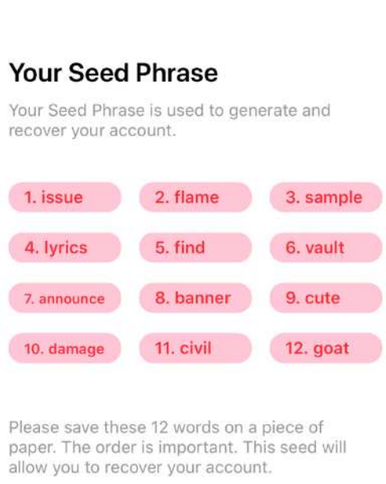
Class Exercise. Option 1. Download a new wallet.

How to create and use a bitcoin wallet.

1. Search for the app in the App Store (iOS) or Google Play Store (Android).

2. Open the app and type in your 12- or 24-word recovery phrase. **Be sure to write it down**. Keep it in a safe place. Remember that if you lose or forget this sequence of words, you will not be able to access your bitcoin if you lose access to your wallet.

3. You must then **confirm** that you have actually saved your recovery or **seed phrase**. To do this, you must **enter**, in the same order, the **words** of your seed phrase.



4. As an additional measure of security, some wallets allow you to **choose** a secure password.
• Your **private key** and first ***bitcoin*** address are automatically created for you by your wallet.

5. Use your "**receive**" address to receive ***bitcoin***. **Transfer *bitcoin* to your wallet.**
• With a self-custodial wallet, you cannot always buy ***bitcoin*** directly with fiat, so you might need to purchase and transfer it from an exchange first.

Class Exercise. Option 2. Restore Wallet (Time Limited).

Download a ***bitcoin*** wallet and add some sats for each student. Give each student a sheet with a seed phrase to retrieve a wallet. Guide students step by step:

1. When you first start your wallet, you will see three methods of wallet creation, tap **[Import an existing wallet]** • You will see an introduction screen, tap **[Restore with recovery phrase]**

2. Enter your 12/18/24-word recovery phrase one by one, in the correct order.

3. Touch [**Restore/Restore**] when finished.

4. You will see an *"Import Successful"* mode when your wallet has been successfully imported.

6.1.2 Class Exercise: How do I Receive bitcoin (in detail)

To receive ***bitcoin***, you will need to provide the sender with your bitcoin wallet address. This is a unique string of letters and numbers that represents your wallet and is used to identify it on the ***Bitcoin Network***. You can find your wallet address by logging into your bitcoin wallet and looking for an option to "Receive" or "Deposit" ***bitcoin***.

You can then share your bitcoin address with the sender in one of several ways:

• **Copy and paste the address**: You can copy the address by highlighting it and pressing "Copy" on your keyboard, then paste it into an email or message to the sender.
• **Share a link to your bitcoin wallet**: Some bitcoin wallets allow you to create a link to your wallet that you can share with the sender. They can then click on the link to access your wallet and send the bitcoin.
• **Share a QR code**: If the sender has a smartphone with a bitcoin wallet app, they can scan the QR code to get your ***bitcoin*** address.

Once the sender has your bitcoin address, they can send you the ***bitcoin*** by entering your address and the amount they want to send you and initiate the transaction. The ***bitcoin*** will then be sent to your wallet and will be visible once the transaction is confirmed on the ***Bitcoin Network***. It usually takes a few minutes.

6.1.3 Class Exercise: How Do I Send bitcoin and Pay for Goods and Services (in detail)

To send ***bitcoin***, you will need a few things: a bitcoin wallet, the recipient's bitcoin address, and the amount of ***bitcoin*** you want to send.

1. Open your bitcoin wallet. • An SMS code will be sent to your phone number, and you will need to enter it in the dialog box. Alternatively, if you have enabled Google 2FA, you will need to enter the six-digit code from the Google Authenticator app.

2. Navigate to the "Send" or "Withdraw" feature and copy the recipient's address.

3. Enter the recipient's ***bitcoin*** address by pasting it in the "To" field.

4. Enter the amount of ***bitcoin*** you want to send in the "Amount" field.

5. Double-check the recipient's address and the amount to be sent.

6. Before clicking **Confirm and Send**, we recommend that you double-check the transaction details one more time to ensure that you are sending the correct amount of ***bitcoin*** to the correct wallet address.

7. Confirm the transaction and wait for the network to confirm the transaction.

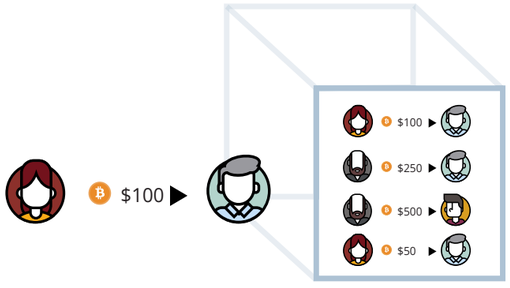
- Let's practice!!! Go to the coffee shop to **buy** snacks with ***bitcoin***.

6.2 On-Chain vs. Off-Chain

It is important to note that not all ***bitcoin*** transactions are recorded on the main ***Bitcoin blockchain***, some networks use different *blockchains* called sidechains to record transactions.

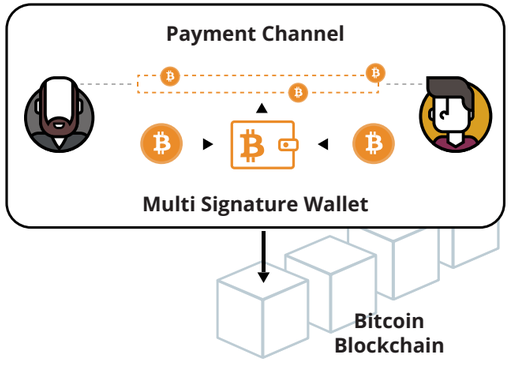
On-chain transactions:

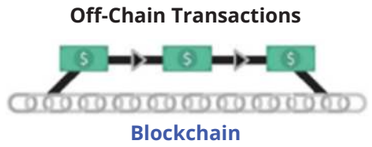
- These are transactions that happen directly on the ***Bitcoin blockchain***.
- They take about 10 minutes to confirm and the fees depend on the size of the transaction in bytes.
- They are secure but can be slower.



Off-chain transactions (Lightning Network):

- These transactions happen on a separate network built on top of the ***Bitcoin blockchain***.
- They are settled faster and with lower fees.
- They are commonly used where regulations and laws support their adoption and where the speed and cost of transactions are more important.
- When compared to transactions on-chain, they are less secure.





If using the lightning network, only **three types of transactions** need to be broadcast to the *blockchain*.

The Lightning Network is a scaling **approach** to ***Bitcoin***.
It's really about moving a lot of ***Bitcoin*** transactions **out of the blockchain and into private channels** between users, but still counting on the blockchain's security.



The transaction that **opens** a channel.



The transaction that **closes** a channel.



Disputes that need to be settled.

Payment Network	Bitcoin Network	Lightning Network
Definition	A decentralized digital network that uses cryptography to secure financial transactions.	A second layer payment protocol that operates on top of the ***Bitcoin blockchain***, enabling faster and cheaper transactions.
Advantages	- Decentralized and secure - No chargebacks or fraud - Can be used anonymously - Global Acceptance	- Faster and cheaper transactions - Increased scalability - Off-chain transactions do not clog the blockchain
Disadvantages	- Slow transaction times - High fees for certain types of transactions- Complex for beginners	- Requires trust in the channel operators - Still experimental and not widely adopted - Requires on-chain transaction to open and close channels

6.3 The Lightning Network

Bitcoin is known for its unalterable public ledger, but it may not be the best choice for everyday transactions like buying coffee. The process of broadcasting these transactions to many nodes and storing them in a shared database can be slow and cumbersome. For personal or private transactions, it's better to use peer-to-peer payment channels.

A better solution is a layered approach to scaling, such as the combination of ***Bitcoin*** and Lightning Networks. This allows users to pick the layer that fits their needs. ***Bitcoin*** is a digital currency that is decentralized, while the Lightning Network provides quick, cheap, and confidential payments.

The Lightning Network is a payment system that allows users to send and receive payments quickly and inexpensively using ***bitcoin***. It works by setting up a shared wallet where both people store their ***bitcoin***, and then making unlimited transactions between each other without touching the main *blockchain*. When they're done, the final balance is recorded on the main *blockchain*.

Lightning operates as a separate network connected to the ***Bitcoin blockchain*** and is designed to work seamlessly with ***Bitcoin***. Taro, which is a recent addition to Lightning, now enables the network to be used for other types of assets, such as stablecoins, allowing users to make nearly instantaneous, low-cost payments in a currency linked to traditional fiat such as the US dollar. Payments can be made directly to the recipient, bypassing intermediaries, and converting the payment into the original currency before it reaches the store.

Using stablecoins in the Lightning Network for international transactions, such as remittances, provides several benefits:

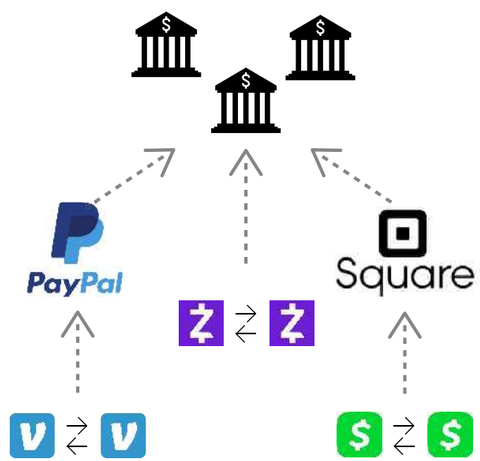
1. Reduced costs: Cross-border transactions can be expensive due to fees charged by banks or other intermediaries. By using stablecoins in the Lightning Network, these fees can be reduced or eliminated, making cross-border payments more affordable.

2. Increased speed: Cross-border transactions can take several days to complete when using traditional methods. By using stablecoins in the Lightning Network, international transactions can be processed quickly, reducing the time required to complete the transaction.

3. Improved access: For individuals or businesses in countries with limited access to traditional banking services, the use of stablecoins in the Lightning Network can provide a means to make international payments, thereby improving access to financial services.

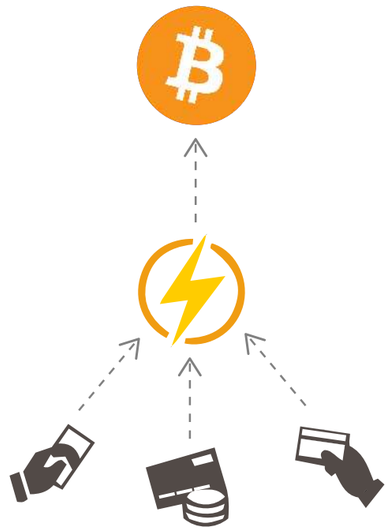
Modern Monetary System = Closed Networks

Banks Maintain Finality



Bitcoin Monetary System = Open Network

Bitcoin Maintains Finality



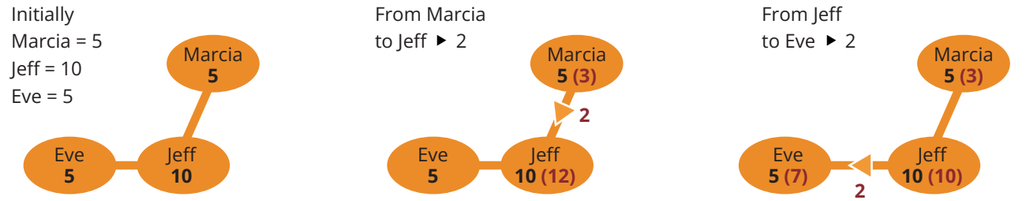
The Lightning Network provides the benefits of digital wallets like Apple Pay without the price volatility associated with ***bitcoin***.

6.3.1 A Lightning Transaction

Example#1

- Below, Marcia has 5 units of some currency and Eve has 5 units as well. Marcia wants to send 2 of her units to Eve, so she sends 2 units to Jeff. Jeff then passes on the 2 units to Eve, who now has 7 units. Marcia now has 3 units. And that's it! The transaction is done.

The key point here is that Marcia and Eve don't have to go through a bank or other intermediary to make the transaction happen.



- Jeff acts as an intermediary or a "**trusted third party**" in this scenario, where Marcia and Eve do not trust each other directly. Jeff receives the 2 units from Marcia and then passes it on to Eve, thus completing the transaction. By using Jeff as an intermediary, Marcia and Eve can complete the transaction without the need for a bank or other centralized institution, which can make the transaction faster, cheaper, and more secure. Jeff is a key element in this peer-to-peer transaction process

As a node operator in a Lightning Network transaction, Jeff benefits in several ways:

1. Transaction fees: Jeff earns a small fee for each transaction that passes through his node, which compensates him for the time and effort he puts into maintaining and running his node.

2. Network participation: By running a Lightning node, Jeff is participating in the network and helping to increase its decentralization, security, and stability. This can increase Jeff's reputation and credibility as a reliable node operator, making him a more attractive intermediary for future transactions.

3. Network growth: As the Lightning Network grows and more people use it, the number of transactions passing through Jeff's node is likely to increase, which can result in increased income from transaction fees.

4. Increased network security: Jeff's role as an intermediary helps to increase the security of the network by adding an additional layer of protection between Marcia and Eve. This can increase the confidence of users in the network, making it more attractive to new users and helping to drive growth.

Overall, being a node operator in the Lightning Network can provide Jeff with a steady source of income, as well as the opportunity to contribute to the growth and development of the network.

In summary, On-chain transactions are slower but more secure while off-chain (Lightning Network) are faster but less secure. You should consider the tradeoff between security and speed depending on your needs.

Example#2

Mina has a serious love for McDonald's. She goes there for breakfast, lunch, and dinner every day! But with so many different payment options available, she's not sure which one is the best choice. Luckily, she's learned a little bit about ***Bitcoin*** and The Lightning Network. After comparing the tables below, Mina has no doubt that using a Lightning Payment method is the way to go.

Benefits	Lightning	Traditional Banking System
Speed	Fast	Slow
Transparency	Transparent	Opaque
Security	Secure	Vulnerable
Transaction Fees	Low	High
Financial Inclusion	High	Limited

Benefits	Lightning	On-Chain
Scalability	High	Low
Privacy	High	Moderate
Interoperability	High	Low
Legal Compliance	Moderate	High
Cost-effectiveness	High	Moderate

Visa, Inc.

On average 1,700 transactions per second.

Capacity of 65,000 transactions per second.

Bitcoin On-chain

Capacity of 7 transactions per second.

Bitcoin Lightning Network

Millions of transactions per second.

Mina is also a fan of fast, secure, and cost-effective transactions, so she decided to use Lightning for her purchases at McDonald's. With Lightning, she can enjoy her meals even more knowing that her payments are processed instantly, securely, and with low fees. Plus, since the Lightning Network provides financial inclusion, Mina can now pay for her meals even if she is in a remote area in El Salvador.

To get started with Lightning, Mina first downloads a Lightning Wallet on her phone. She then funds her Lightning Wallet by sending some bitcoin from her regular bitcoin wallet to her new Lightning Wallet. This process is called "funding the wallet" or "funding a payment channel." Mina can fund her wallet with any amount of bitcoin she is comfortable with, but it's important to note that the amount of bitcoin she locks in her Lightning Wallet cannot be used in her on-chain transactions.

Once her Lightning Wallet is funded, she can use it to make payments to McDonald's. McDonald's has a Lightning Node, so Mina can open a payment channel with them by sending some of her bitcoin from her Lightning Wallet to a specific address provided by McDonald's. This moves her ***bitcoin*** from the Bitcoin blockchain to an off-chain transaction on the Lightning Network.



With the payment channel open, Mina can now make purchases at McDonald's without having to open a new channel or pay high fees each time. The channel stays open as long as both Mina and McDonald's want to use it. For example, if Mina buys a hamburger for 0.0005 ***bitcoin***, the channel tracks that Mina now has 0.9995 ***bitcoin***. And if she buys a milkshake for 0.0003 ***bitcoin*** the next day, the channel tracks that Mina now has 0.9992 ***bitcoin***.

When Mina decides she wants to use her ***bitcoin*** balance for something else, she closes the channel by broadcasting a closing transaction to the ***Bitcoin*** *blockchain*. This is done by initiating a closing transaction in her Lightning Wallet, and the transaction contains the final balance of the channel agreed to by both parties. The transaction is then broadcast to the ***Bitcoin*** *blockchain* and confirmed by a miner. Once the transaction is confirmed, the channel is closed, and the remaining ***bitcoin*** in the channel will be returned back to Mina and McDonald's.

It's important to note that closing a channel can take some time to be confirmed on the *blockchain*. During this waiting period, the funds are still locked in the channel and cannot be used for on-chain transactions. Mina will receive a notification once the closing transaction is confirmed.

6.3.2 Class Exercise: Lightning Wallet Relay Race

1. First, you will need to download a Lightning wallet onto your phone or computer. There are several options to choose from, including Muun, Blue Wallet, Bitcoin Beach Wallet, and Eclair are a few options for mobile phones, and Lightning App and Zap for desktop computers.

2. Follow the instructions for installing the wallet on your device. This may involve downloading the app from the App Store or Google Play, or downloading and installing the software from the wallet's website.

3. Once the wallet is installed, open it and follow the prompts to set it up. This may involve creating a new wallet or restoring an existing one, and securing it with a password or other form of authentication.

4. Make sure that you have a way to receive satoshis. This may involve providing your wallet with a receiving address, or scanning a QR code provided by your teacher or another member of your group.

5. When your wallet is set up and you are ready to receive satoshis, your teacher will give you and your group a starting amount of satoshis by sending them directly to your wallet.

A. Your group's goal is to pass the satoshis from one person's wallet to another, using the Lightning Network, until they reach the last person in the group.

B. To send satoshis to another person, open your wallet and follow the instructions for making a payment. You will need to provide the recipient's lightning invoice or scan a QR code, and enter the amount of satoshis that you want to send.

C. If your group is the first to successfully send the satoshis to the last person, you win! (And get to keep the sats, and some candy.)

6.3.3 Class Exercise: Lightning Online Interactive Demo

Class Exercise. Begin by exploring one of the interactive websites provided by the teacher. Then, follow the instructions in the next page.

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

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



1. Focus on the key concepts discussed in class, including payment channels, routes, and fees.

2. Take note of any questions or difficulties you encounter as you explore the website.

3. Work with your group to share your findings and discuss any questions or difficulties with the class.

4. Be prepared to participate in class discussions about the Lightning Network and its potential as a scaling solution for bitcoin transactions.

Chapter #7

Unlocking the Secrets of Bitcoin's Inner Workings: The Math, Mempool, and UTXOs

7.0 Putting the Double Spend Issue to Rest: Understanding Bitcoin's Solution
7.1 Tracking Your Coin's Journey
7.2 Security and Secrecy
7.3 The "Mempool" or Memory Pool: Understanding the Holding Tank of Bitcoin Transactions
    7.3.1 Class Exercise: On Hold: Examining the Unconfirmed Transactions of the Bitcoin Network
7.4 Behind the Blocks: The Mystery of Bitcoin Scripting
    7.4.1 A Technical Dive into Bitcoin Transactions

00001100111000101000101010101011100100010101001001100110000011101000101000111110011010111100100110110001100101110010011010100111000101001001101101110100011001011010100011011000000101110101000100011110000000001110101101111100001010110011110010101000010100000011

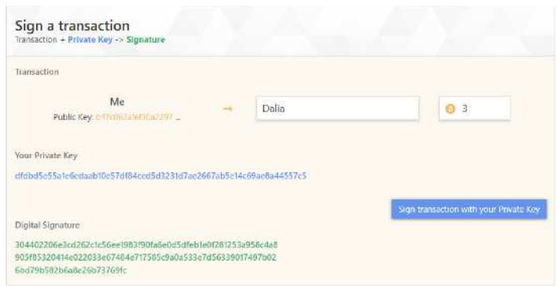
Do you see that long string of ones and zeros up there? It's called a random number, and if we convert it to our regular decimal system, it becomes a number with more than 70 digits, which is even more atoms than there are in our universe! But, we can use a different system to represent this number in a shorter way, and we call it a **private key**.

Something really cool about this particular **private key** is that it's unique, which means it's never been used before and it'll never show up again once you leave this page or generate a new one. It's like flipping 256 coins in a row and getting the exact same outcome twice – impossible!

The security of ***Bitcoin*** depends on this **private key** being private and difficult to guess. If someone else gets their hands on it, or if you lose it, you'll lose all your money forever. So keep it safe!

So far, we've learned about the history of money and the revolutionary idea of *blockchain* technology, and we've explored the basics of ***Bitcoin*** - the world's first decentralized digital currency. But how does ***Bitcoin*** prevent fraud and ensure that people can't **spend the same money twice**?

The truth is, when you send some ***bitcoin*** to someone else, you gotta say "yes, I approve this" with your **private key**. Then the network is like "cool, let me just double-check that this is legit" and it looks at the signature to make sure everything's good before sending the ***bitcoin*** over.



Digital signatures are an essential component of secure transactions on the Bitcoin network. A digital signature is a mathematical algorithm that is used to verify the authenticity of a transaction.

When a transaction is made, the sender uses their private key to generate a digital signature, which is then added to the transaction data. When the transaction is broadcast to the network, each node can use the sender's public key to verify the digital signature and ensure that the transaction was indeed sent by the owner of the private key.

Without digital signatures, anyone could attempt to send a transaction on someone else's behalf and steal their Bitcoin. Digital signatures ensure that only the owner of the private key can authorize a transaction and that the transaction cannot be altered in transit.

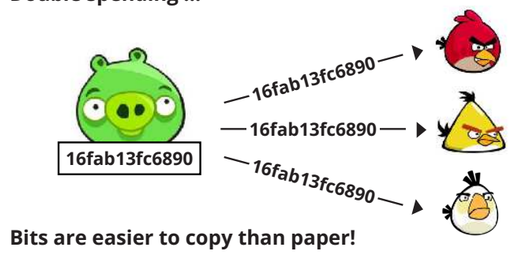
That's where the magic of **UTXOs**, **public key cryptography**, **hashing**, **scripting**, and the **mempool** come into play. Just like a fingerprint ensures that nobody else can use your identity, **hashes** in ***Bitcoin*** ensure that transactions can't be altered. **Scripts** are like the rules for a game, making sure transactions follow specific conditions. **UTXOs** are like the building blocks of a puzzle, keeping track of all the money in your virtual wallet. And the **mempool** acts like a holding area, making sure all transactions are verified before being added to the *blockchain*. So, let's dive in and discover how ***Bitcoin*** solves the **double-spending problem** and ensures the integrity of every transaction on its network.

7.0 Putting the Double-Spend Issue to Rest: Understanding Bitcoin's Solution

Remind me, what is the "double spending problem"?

Private, **public keys** and ***bitcoin*** transactions, as we've experienced, are represented by a series of random numbers and letters that can be viewed on any device with internet access.

Additionally, much of the information related to these transactions is typically communicated using a numerical notation system known as **hexadecimal numbers**.



This means that it is common to see strings of 64-character hexadecimal numbers consisting of letters (A-F) and numbers (0-9), such as

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

So how do we actually prevent someone from copying and pasting their bitcoin and spending it multiple times, like they would with an email or photo?

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16.
f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16.

How do we reach consensus on who owns what money without a central authority?

Hashing and code. Let's explain.

Imagine you have 1 ***bitcoin*** and you want to send it to your friend as a birthday gift. You send the ***bitcoin*** to your friend's address, but then you realize that you owe your ex-partner money and should have sent the ***bitcoin*** to them instead. In a moment of panic, you decide to be sneaky and create a new transaction to send the same 1 ***bitcoin*** to your ex-partner. This is what we call a "double spend."

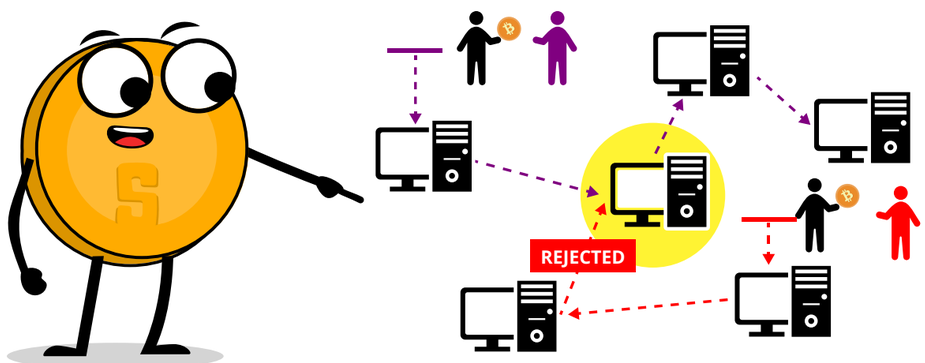
But wait, how does the network prevent this from happening? It's simple. The nodes on the network detect conflicting transactions and only allow one to go through based on a set of rules known as the "**consensus rules**." In this case, it's likely that the transaction to your ex-partner would be rejected since it was sent after the original transaction to your friend. However, it's just a matter of luck which transaction is picked up first by a miner.

Thanks to the *blockchain*, **everyone on the network is able to agree on the current state of the ledger**. This helps to prevent **double-spending** and fraud, making it a secure and trustworthy system, just like a digital version of the "honor system." So, next time you send ***bitcoin***, you can relax knowing that the network ensures no one cheats the system.

So how does ***Bitcoin*** actually solve this? Well, let's find out.

- ***Bitcoin*** prevents double-spending by implementing a confirmation mechanism and maintaining a universal ledger (*blockchain*).
- Transactions are added to the *blockchain* in a chronologically-ordered, time-stamped manner.
- To prevent double spending, only the first transaction to receive enough confirmations (usually 6) is included in the *blockchain*, while the others are discarded.
- Transactions on the *blockchain* are irreversible and impossible to tamper with.

Bitcoin Mining Node Rejects Transaction from the Mempool



When any transaction is initiated, any **node** can verify it on the network in a few simple steps:

1. First, the node will **check that the transaction is properly signed by the sender's private key**, which ensures that the transaction is legitimate and not tampered with.

2. Next, the node will **check that the sender has enough *funds*** to complete the transaction. This is done by examining the sender's balance on the *blockchain* ledger.

3. Finally, the node will also validate the transaction **inputs** and **outputs**, making sure that the inputs being spent in the transaction are not already spent in another transaction and that the outputs are not exceeding the total supply.

As we'll see, the combination of **public key cryptography** and the **UTXO** (Unspent Transaction Output) system is used in **Bitcoin** to verify the authenticity of transactions and prevent fraud without a central authority. **Public key cryptography** ensures secure communication and transfers of funds, while UTXO maintains a record of all the funds on the network and prevents double-spending.

UTXO, which stands for "Unspent Transaction Output," is simply a record of all the available funds in the network that have not yet been spent.

7.1 Tracking Your Coin's Journey

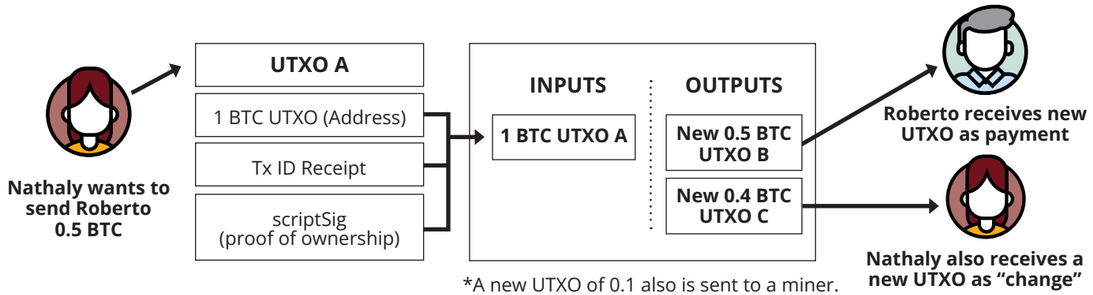
In ***Bitcoin***, transactions work like breaking a big bill into smaller bills and giving them to different people. The change you receive from a transaction is called an unspent output and can be used as an input for a new transaction. Outputs in ***Bitcoin*** transactions can either be **spent** or **unspent**, and unspent outputs are considered valuable because they can be used in new transactions.

- Think of it like using multiple gift cards to pay for a purchase. The gift cards from previous transactions act as inputs, and the change you receive is represented by a new gift card with the remaining amount. This is similar to how ***Bitcoin*** transactions work with UTXOs.

What are UTXOs?

The balance of a wallet is the sum of all a user's UTXOs. UTXOs are used to track the ownership of ***bitcoin*** in the network. When a transaction is made, it creates new UTXOs, and when a transaction is spent, it uses up existing UTXOs.

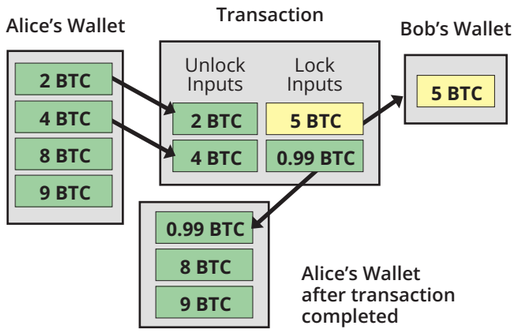
- UTXOs are like digital coins in the world of ***Bitcoin***. It is the change that you get back after you spend some ***bitcoin***.



How UTXOs Work in Bitcoin Transactions

When a transaction is made, the amount of ***bitcoin*** that is sent is divided into multiple outputs, each of which is associated with a specific address.

- When sending ***bitcoin*** to someone, you will use one or more Unspent Transaction Outputs (UTXOs) as the source of the funds. These UTXOs will be combined, if necessary, to create a new output that belongs to the recipient of the transaction. This new output, or UTXO, will then become the recipient's property and can be used as the source of funds in a future transaction. This chain of UTXOs creates a transparent and traceable history of all ***bitcoin*** transactions on the *blockchain*, starting from the very first block.



- For example, if someone wants to send 2 ***bitcoin*** but has a UTXO worth 5 ***bitcoin***, the difference of 3 ***bitcoin*** is sent back to the sender as "change." This change is a new UTXO for the sender and can be spent in a future transaction.

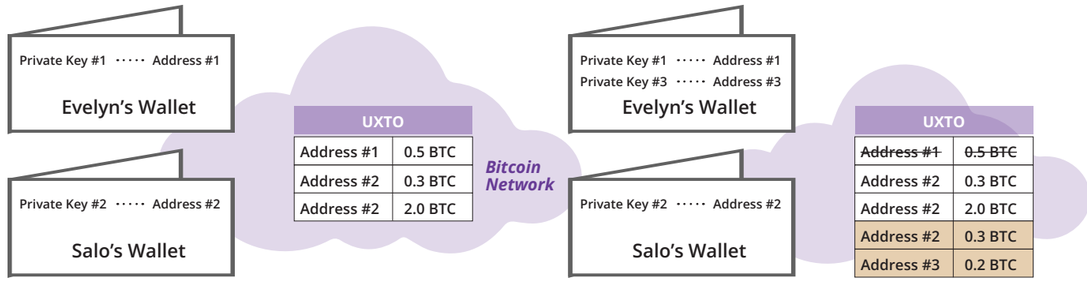
- In the example, Alice sends Bob 5 BTC while retaining some for herself. She combines 6 ***bitcoin*** from her four UTXOs, which totals 23 ***bitcoin***, and sends 5 to Bob and .99 back to herself, with a .01 fee for processing. The transaction is then added to the *blockchain*, updating all nodes with a copy of the updated UTXO ledger. If Alice then tries to send 23 BTC to Ximena in a separate transaction, the nodes will reject it as some of the output has already been spent.

If someone were to attempt to use a spent output in their transaction, it would likely be rejected by the network nodes. This is because these nodes maintain a copy of the same database set and can easily reach a consensus by checking the balance of each address before validating any new transaction. This ensures the integrity and validity of the transactions on the network.

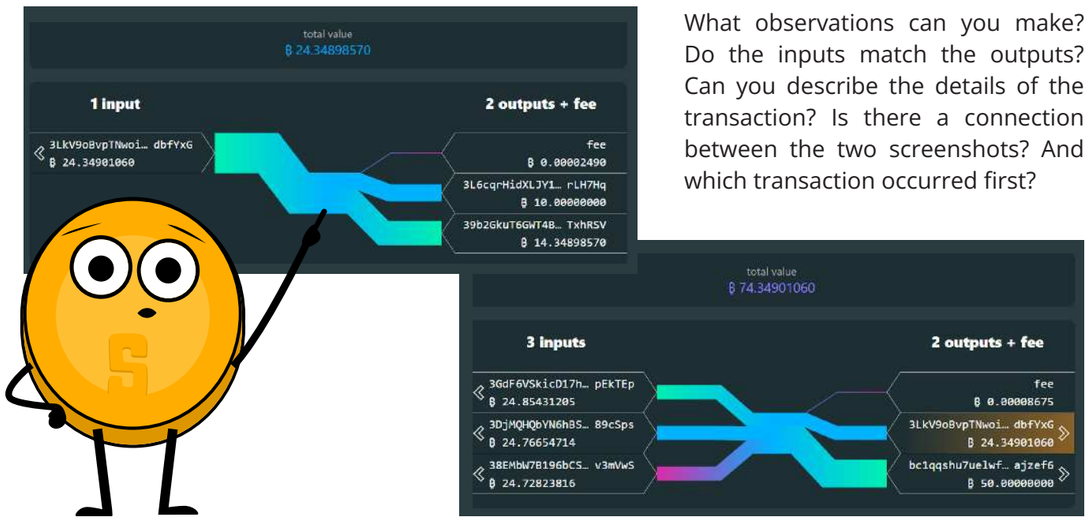
Let's look at another example:

Only the person who has the **private key** for an address can access the UTXOs stored in that address. For example, if Evelyn has a **private key** for address #1, she will see 0.5 ***bitcoin*** in her wallet. If Salo has a **private key** for address #2, he will see 2.3 ***bitcoin*** in his wallet.

When Evelyn sends 0.3 ***bitcoin*** to Salo, her wallet generates a new **private key** and address (#3). The original UTXO on address #1 gets spent and two new UTXOs are created: one for Salo's address with 0.3 ***bitcoin*** and one for Evelyn's new address with 0.2 ***bitcoin***. After this transaction is recorded in the ledger, Salo's wallet shows 2.6 ***bitcoin*** and Evelyn's wallet shows 0.2 ***bitcoin***.



Below is an actual screenshot of a real transaction where there is only one input. However, in a more general case, the starting balance could be the sum of multiple UTXOs that a person has accumulated from previous transactions.



What observations can you make? Do the inputs match the outputs? Can you describe the details of the transaction? Is there a connection between the two screenshots? And which transaction occurred first?



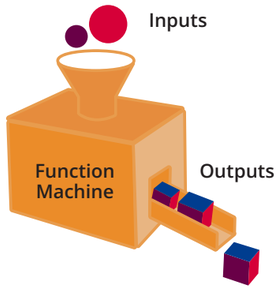
Generally, **spent outputs** are displayed in red and **unspent outputs** in green. This color coding provides a visual way to quickly identify spent and unspent outputs, which can be useful for tracking transactions and understanding the flow of funds in a blockchain.

7.2 Security and Secrecy

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

What is a function, but more specifically, what is a one-way function?

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



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





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

In ***Bitcoin***, **functions** are utilized to **execute transactions**. We already know that transactions in ***Bitcoin*** are essentially transfers of value from one address to another. To perform a transaction, a number of cryptographic functions are used to validate the transaction and update the state of the ***Bitcoin*** blockchain, which is a decentralized ledger that keeps track of all transactions.

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

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



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



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

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

What is a hash function?

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

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

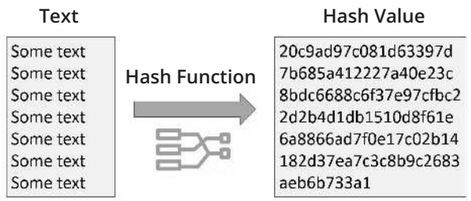
How Hashing is Used in Bitcoin Transactions

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

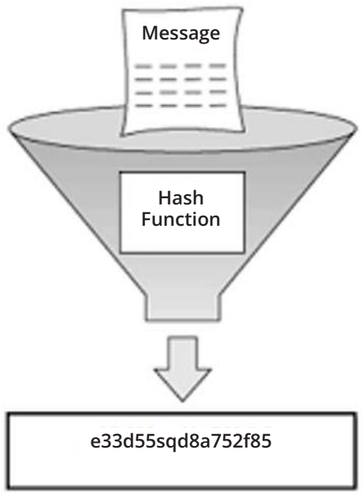
The Role of Hashing in Providing Security

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

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



Data of Arbitrary Lenth



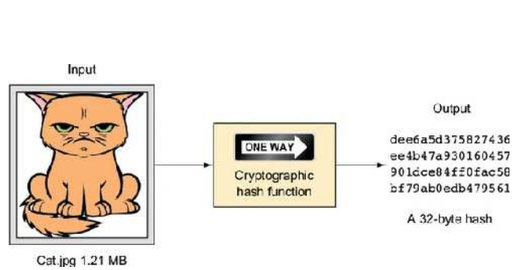
Fixed Length Hash (Digest)

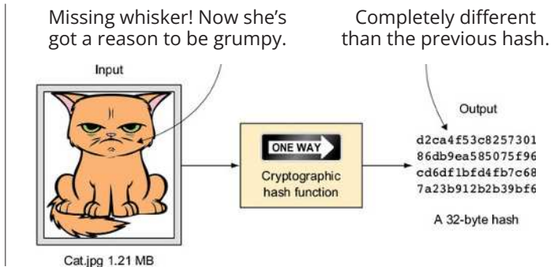
A **hash function** is like a secret code machine. It takes in a **message** and turns it into a code.

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



Instantly generate a SHA256 hash of any string or input value. Hash functions are used as one-way methods.





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

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

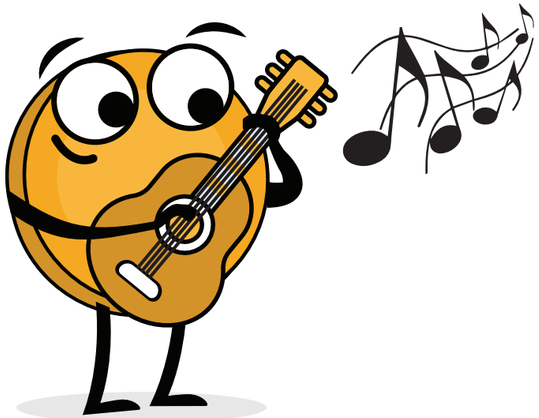
- Notice that a period in the second input changes the output completely when compared to the first one.
- The third input is a huge file yet the output is still the same fixed length as the other two.

SHA256 hash of the string ***hello world***
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

SHA256 hash of the string **hello world.**
7ddb227315f423250fc67f3be69c544628dffe41752af91c50ae0a9c49faeb87

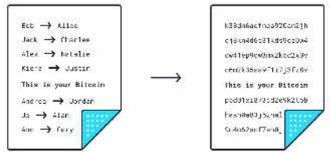
SHA256 hash of the downloadable iso file **Ubuntu 18.10**
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

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



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

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

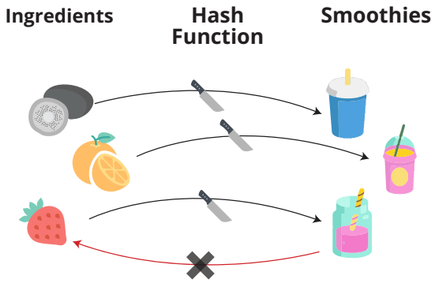




In this link you'll find another hash generator where you can try it out yourself.

Hashing

A hash function takes any input, and produces a fixed-length output (hash).



- ***Deterministic.*** The same ingredients always yield the same smoothie.

- ***Pre-Image Resistance.*** You can't glue together a strawberry when given a smoothie.

- ***Correlation Resistance.*** Changing the ingredients a little results in a completely different smoothie.

- ***Collision Resistance.*** It's hard to find different ingredients for a smoothie that result in the exact same one.

- ***Speed & Verifiablility.*** Throw fruit into the mixer. It's fast and what comes out for sure is a smoothie.

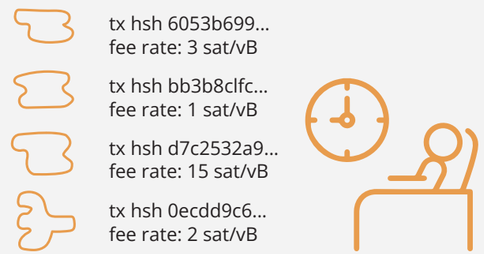
7.3 The "Mempool" or Memory Pool: Understanding the Holding Tank of Bitcoin Transactions

What is the Mempool?

The mempool is like a waiting room for transactions in the ***Bitcoin Network***. When a transaction is made, it is first added to a node's mempool before it is verified and added to the *blockchain*.

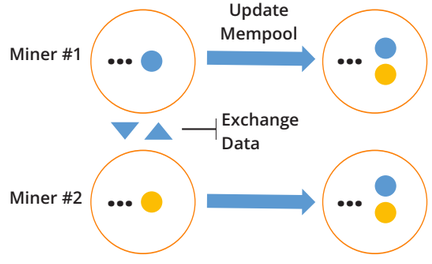
Imagine you are waiting in line at a restaurant. Your name is added to a list of people waiting for a table. When a table becomes available, the host calls your name and seats you. Similarly, a ***Bitcoin*** transaction is added to the mempool when it is made, and is confirmed and added to the *blockchain*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

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



When a node fist receives a transaction from a peer, it has to verify the transaction is legit. Nobody wants faulty or deceptive transactions.

Mempool synchronization allows nodes to share their transactions with other nodes by sending a message containing a list of **verified** transactions in the mempool.



The main purpose of a **mempool** is to:

1. Relay unconfirmed transactions.



2. Provide miners transactions to mine.



Accept To Memory Pool (ATMP) involves checking things like:

- Do I already have this transaction?
- Is there a conflict with a different transaction in the mempool?
- Does the ***bitcoin*** in cover the ***bitcoin*** out?
- Do the signatures prove the previous outputs can be spent?
- Are there enough fees?

How Transactions are Verified and Added to the Mempool

A **full node** checks all transactions to make sure they are valid and have not been used before. If a transaction is good, the node will verify it and add it to it's memory pool. Then it will share it with other nodes to double-check. Finally, if the majority agree, it will be taken out of everyone's mempool to become permanent part of the *blockchain*.

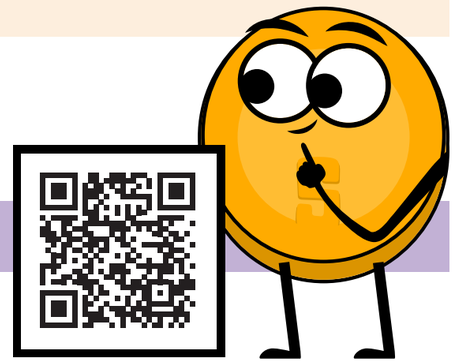
Transactions in the ***Bitcoin Network*** are taken out of the mempool and confirmed when they are included in a block, which is then added to the *blockchain*. However, there are several reasons why a transaction might not be confirmed after 72 hours:

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

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

A **DDoS** (Distributed Denial of Service) attack is an attempt to make the network unavailable to users by overwhelming it with too much traffic from multiple sources. This attack aims to disrupt normal traffic of a website or service by overwhelming it with fake traffic, making it difficult or impossible for real users to access it.

7.3.1 Class Exercise: On Hold: Examining the Unconfirmed Transactions of the Bitcoin Network



Class Exercise. Follow the following instructions:

1. Visit the website *https://bits.monospace.live/*

2. Locate an unconfirmed transaction and click on it.
- What information can you find?
- Can you follow the history of where bitcoin came from?
- How many addresses do you see? What does input and output mean?
- Can you follow the UTXO? Do you recognize which BTC has been spent?
- Does the input match the output?
- Does every transaction have a fee?
- Who does the fee goes to? Is it fair?
- Who pays the fee?
- Can you locate how much bitcoin was transferred from one address to another?

3. Write down the TxID, fee rate, fee, and total value of the transaction in a notebook.

4. Analyze other transactions if desired, and compare them to the first one in terms of amount, fee paid, and likelihood of being included in the next block.

5. Consider what it means for a block to be "mined" and for a transaction to be "unconfirmed."

6. Be prepared to discuss these observations and questions in the next class.

7.4 Behind the Blocks: The Mystery of Bitcoin Scripting

Script is a **programming language** used in ***Bitcoin*** to create **smart contracts** and **automate** transactions. To understand script, it's helpful to think of it as a set of instructions that tell the ***Bitcoin Network*** what to do with a specific transaction.

A **smart contract** is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained within it exist on a blockchain network and are enforced automatically.

- Think of it like a vending machine. You put in money, make a selection, and the machine dispenses your item automatically. In the same way, a smart contract automatically executes the terms of the agreement between two parties, without the need for intermediaries such as lawyers or banks.

For example, a smart contract could be used to represent a financial agreement, such as a loan or a bond. The terms of the agreement, such as the interest rate and repayment schedule, are encoded into the contract. When the agreed-upon conditions are met, the contract automatically executes the terms and transfers the funds.

The key benefits of smart contracts are that they are transparent, secure, and self-executing, which can help to reduce the costs and risks associated with traditional contract processes. Additionally, because they exist on a decentralized network, they are resistant to tampering or interference, making them a more secure and trustworthy way of conducting transactions.

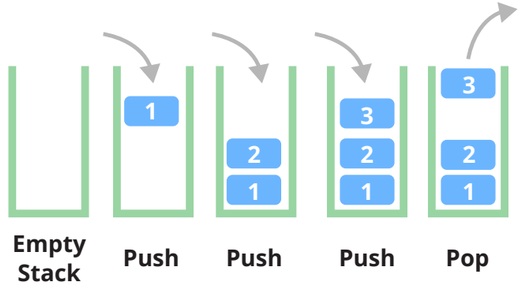
In a similar way, ***Bitcoin*** uses script to make sure that specific conditions are met before a transaction is processed.

While other *blockchain* networks, such as Ethereum, also support smart contracts and programmable transactions, they use different programming languages and approaches to enforce the rules and conditions of transactions. Only Bitcoin uses script.

Script is a very basic programming language, but it's powerful enough to handle a wide range of transactions. For example, it can be used to create **multi-signature** transactions, where multiple people must sign off on a transaction before it can be processed, or to create a smart contract, where a transaction is automatically executed when certain conditions are met.

While script may seem complex, the basic idea behind it is actually quite simple. By using script, the Bitcoin network can automatically enforce the rules and conditions of transactions, making it a secure and efficient way to transfer value.

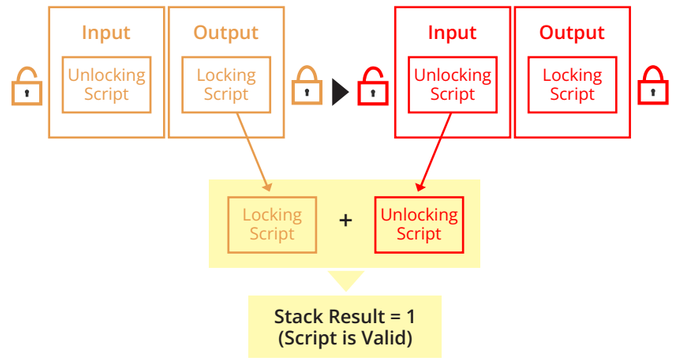
How Scripting is Used in Bitcoin Transactions



- Imagine you have a row of coins and you want to sort them into different slots, like putting coins into different piggy banks. The order in which you put the coins into the slots is important. This is similar to how satoshis are transferred in a transaction. The inputs are like a row of coins and the outputs are the slots waiting to receive a coin. To assign the coins to the slots, you go through each coin in the row in order, and put each one into the first available slot. This is called "first-in-first-out" or FIFO, which means that the first coin in the row goes into the first available slot, and so on.

- Scripts operate on a **stack-based system**, where instructions are processed in the order they appear, from top to bottom.The concept is similar to a stack of plates, where you can only access the plate that is on top of the stack.

A basic ***bitcoin*** transaction uses at least one "**locking script**" and one "**unlocking script**" to determine who can access the funds in a particular wallet address. The locking script can be thought of as a **list of instructions that describes how the recipient of the funds can access them**, while the unlocking script **unlocks the funds**.



- Think of Script as a recipe for baking a cake. Just as you need to follow the steps in the recipe to make the cake, the computer needs to follow the instructions in Script in a specific order to transfer ownership of ***bitcoin***.

By using locking and unlocking scripts, along with private and public keys, the ownership and transfer of UTXOs can be securely tracked and verified.

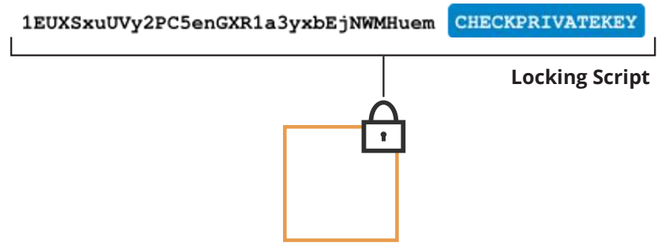
7.4.1 A Technical Dive into Bitcoin Transactions

The locking script holds the **recipient's address** and verifies that the correct **private key** was used. This ensures that **private keys** remain confidential and can be securely protected.

To unlock the funds, the sender must demonstrate ownership by generating a digital signature with their **private key**, thereby confirming possession of the address.

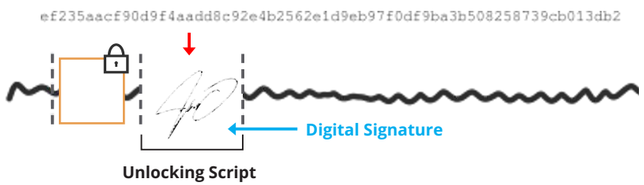






The output (***bitcoin UTXO***) has been locked to this address (1EUX...) and only the correct **private key** will unlock it.

For example, let's say that you want to send some ***bitcoin*** to your friend, but you want to make sure that your friend can only spend them after a certain date. You can use ***Bitcoin*** script to define this condition, which is known as a "**time-lock**". When you create the transaction, you include a script that specifies the time-lock condition. When your friend receives the ***bitcoin***, they can only spend them after the specified date has passed.



Bitcoin script can also be used to create more complex conditions for spending ***bitcoin***, such as multi-signature transactions, which require multiple parties to authenticate a transaction before it can be spent. This can be useful in situations where multiple parties need to approve a transaction.



CHECKPRIVATEKEY is a function that checks whether the address matches the correct **private key**.



CHECKSIG verifies that THE transaction was approved by the owner of the **private key** that matches the **public key** used to sign the **transaction**.

In simple terms, script helps ensure the security and reliability of ***Bitcoin*** transactions by using private and public keys to verify ownership and transfer of funds. Different methods of transactions have varying levels of security. Some reveal the recipient's **public key** during the transaction, making it vulnerable to theft if the **private key** is ever hacked. Others keep the **public key** hidden, providing a higher level of security.

In the next chapter, we will delve deeper into the process of mining and the role of miners in the ***Bitcoin Network***. We will explore how they validate transactions, create new blocks, and receive rewards for their efforts.

Stay tuned for a comprehensive understanding of how the ***Bitcoin Network*** operates!

Chapter #8

Building the Chain of Security: Understanding the Process of Bitcoin Mining and its Role in the Blockchain

8.0 Uncovering the Gems of the Blockchain: Meet the Miners and the Mining Process
8.1 The Dynamic Rewards System of Bitcoin Mining: Block Rewards, Transaction Fees, and Halvings
8.2 The Vital Task of Bitcoin Mining: Securing the Blockchain
8.3 Dissecting the Block
8.4 Rehashing the Hashes-No Pun Intended
8.5 The Step-by-Step Process of Mining a Block
- **8.5.1** Class Exercise: Mining Interactive Exercise
- **8.5.2** Summary of the Transaction from Start to Finish
- **8.5.3** Don't Trust, Verify

8.6 Class Exercise: Transaction with UTXO's

8.0 Uncovering the Gems of the Blockchain: Meet the Miners and the Mining Process

Think of miners as digital bookkeepers.

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

Miners collect unconfirmed transactions, form a block, and set off on a quest to find a valuable key that will **secure the block's spot in the blockchain.**

The sought-after prize is a "**valid block hash**," cleverly hidden among billions of others, and only a specific key assigned by the network can unlock it.

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

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

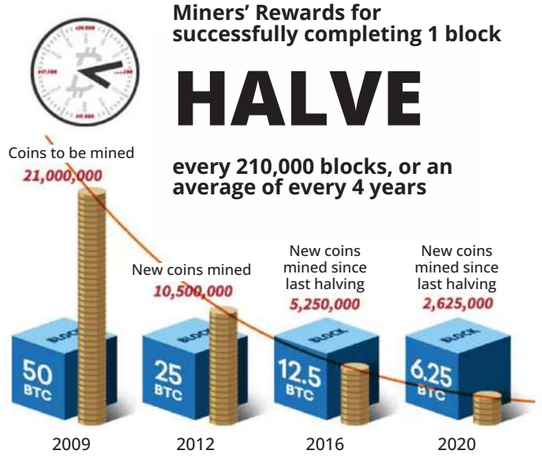
Miners earn rewards for their efforts in two ways: block rewards and transaction fees. **Block rewards** are new bitcoin released into circulation with each block added to the blockchain. **Transaction fees** are small ***bitcoin*** payments users make to have their transactions processed faster and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

8.1 The Dynamic Rewards System of Bitcoin Mining: Block Rewards, Transaction Fees, and Halvings

Bitcoin halving is an essential part of the ***Bitcoin*** universe that helps maintain its scarcity and value over time. Satoshi Nakamoto cleverly designed a block reward system to distribute new ***bitcoins*** without a central authority. In ***Bitcoin's*** early days, miners got a sweet 50 bitcoin reward for each block they mined, motivating them to invest in powerful equipment and electricity for their mining operations.

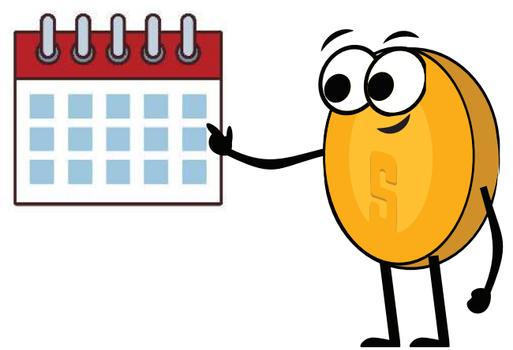
To keep the network stable and manage new bitcoin supply, the block reward is halved about every 210,000 blocks. This event, called "**halving**," decreases the number of new ***bitcoin*** entering **circulation** and continues to motivate miners to protect the network and uphold its decentralization.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

- Let's say you have a jar that can only hold 1000 pieces of candy. Every day, you get to add 10 pieces of candy to the jar. However, after every four years, the amount of candy you can add to the jar is cut in half. This is how new ***bitcoin*** are created and added to the supply through the process of mining.



Circulating Supply refers to the amount of ***bitcoin*** that is currently in circulation and available for trading. This measurement represents the total number of coins that have been mined and are in circulation at any given time, excluding any coins that may be locked up or lost forever.

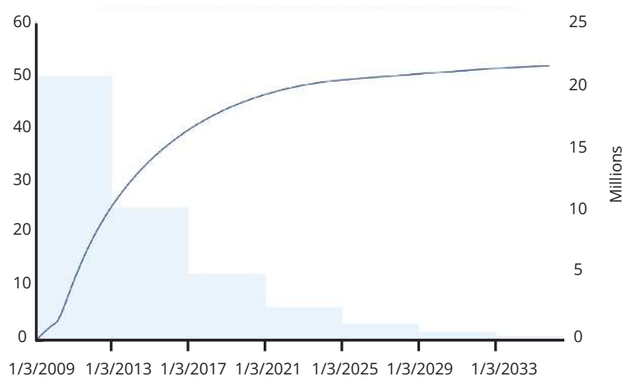
During each halving event, miners receive fewer ***bitcoin*** rewards, which lowers the **issuance rate** of new coins. As a result, ***Bitcoin's*** **mining difficulty** increases to maintain a block time of approximately 10 minutes, ensuring new blocks are added to the blockchain at a steady pace.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



Halving events are pre-programmed into the ***Bitcoin*** protocol, making the **supply schedule** of ***bitcoin*** predictable and transparent.

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

Bitcoin Supply Schedule



The following table provided outlines the details of upcoming halving events for ***Bitcoin***, including the percentage of the total supply that will be mined by that date, the expected date of the next halving event, and the block number at which the halving event is expected to happen.

Event	Expected Date	Block	Block Reward	Percentage Mined
Fourth Halving	2024	840,000	3.125	96.875 %
Fifth Halving	2028	1,050,000	1.5625	98.4375 %
Sixth Halving	2032	1,260,000	0.78125	99.21875 %

As more ***bitcoin*** is mined, the circulating supply and the **percent of the total supply** that has been mined will keep increasing until the **total supply of 21 million** is reached. The reduced supply, combined with rising demand, can boost ***bitcoin's*** price. This benefits early adopters and also motivates miners to continue securing the network and contributing their computing power and resources.

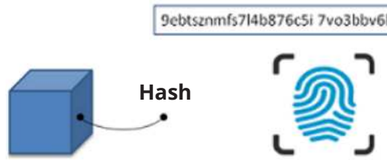
Bitcoin: Percent of 21M Supply Mined

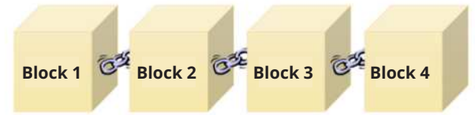


8.2 The Vital Task of Bitcoin Mining: Securing the Blockchain

What is a Valid Block Hash in Blockchain?

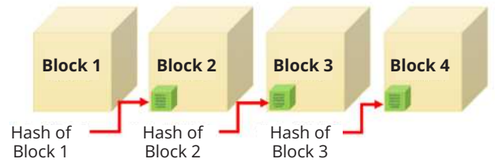
A **block hash** serves as a **unique identifier** for each block in the *blockchain* and helps detect any attempts to alter past transactions. The **blocks in the blockchain store transactions and form a chain of blocks**, starting from the **genesis block** to the most recent one, creating a public and transparent record of all transactions. The block hash links each block to the previous one, allowing anyone to view the history of any transaction and ensuring the accuracy and security of the data stored on the network. Just like a **fingerprint** identifies an individual, the block hash identifies each unique block in the *blockchain*.





The blocks are "linked" together by enforcing a specific relationship between blocks. That is, a block must contain a "fingerprint", which is a hash value of the data of the previous block. A hash function can condense arbitrary message (the block information) to a fixed size (e.g., 160 bits) and produces a finger print of the message.

The first ever block of ***bitcoin***, containing total of 50 ***bitcoin*** was mined by the creator of ***bitcoin***, Satoshi Nakamoto.

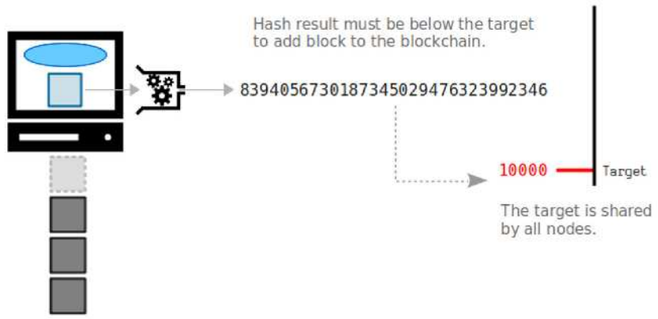


While a block hash **can be used to verify the integrity** of the data in the block, it **does not reveal all of the information** within the block. The information within the block can only be accessed by using the cryptographic keys required to decode it. The block hash simply provides a means of verifying that the data in the block has not been altered.

The Race to Mine a Block

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

- Mining can be compared to a race where the goal is to reach the finish line as quickly as possible. The **difficulty target** in the race is adjusted periodically, making it harder to mine a block as more miners join the race.



- Let's say the target set by the network in a *blockchain* is 1000. The miners would have to use their computers to search for a special number, called the block hash, that is lower than 1000. The first miner to find a block hash that is lower than 1000 gets to add a group of transactions to the blockchain and is rewarded with some ***bitcoin***.

The **difficulty level** is a measure of how difficult it is to find a valid block hash that meets the target set by the network. It is adjusted periodically to ensure that blocks are added to the blockchain at a consistent rate. The difficulty level is expressed as a number, and the higher the difficulty level, the more difficult it is to find a block hash that meets the target.

- For example, consider two different hashes:
  - Hash 1: **0000A1mINgF0RbL0cK5wItHth3hAy5tAcK**
    Difficulty level: 1
  - Hash 2: **00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK**
    Difficulty level: 2

In this example, Hash 2 has a higher difficulty level than Hash 1 because it requires more zeros at the beginning. This means that it is harder to find a block hash that meets the target set by the network when the difficulty level is higher.

Finding a valid block hash involves **a lot of computer work.**

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

PoW keeps the *blockchain* safe by making it difficult for anyone with malicious intentions to take control. The target is adjusted to aim for one block to be mined every 10 minutes, making the network even safer as the target becomes harder to reach.

As an example, the target set by the network for mining a specific block could be:

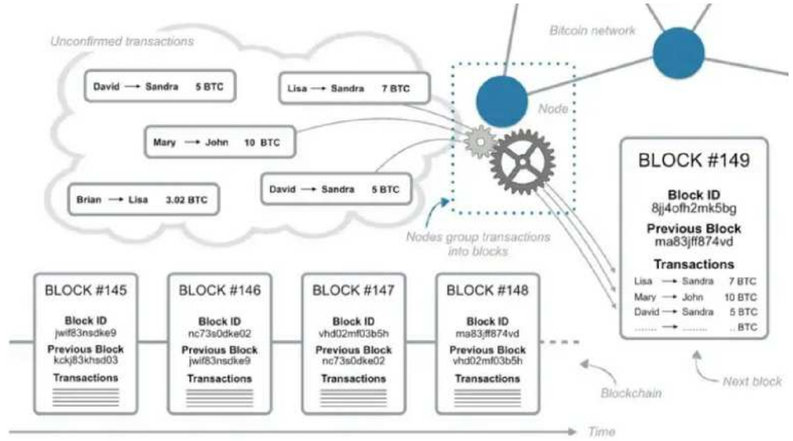
00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK

Which means that first miner to find a hash with eight leading zeros will achieve this target thus be allowed to add the block to the blockchain and will receive compensation in bitcoin.

The Role of Miners

Miners actually have two tasks in a *blockchain* network: 1) **verifying transactions** and 2) **adding new blocks**.

They collect unconfirmed transactions into their **mempool**, select a subset of these to include in their **candidate block**, and then search for the block hash.

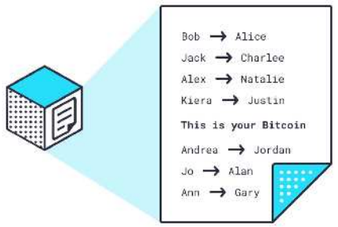


Multiple miners can be working on creating new blocks simultaneously. The first miner to discover a block hash that meets the target set by the network announces it to the network, and the other miners then **check** the transactions in that miner's candidate block to make sure they are valid. If the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

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

8.3 Dissecting the Block

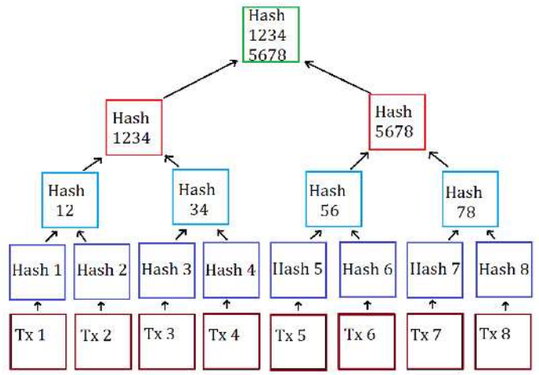
A *blockchain* is made up of blocks, similar to pages in a ledger, that store new **transactions**. Each block has a **header** with a summary of the data, a link to the previous block, and a unique number called a **nonce**, or a **number used once** and a few other details. Miners' task is to correctly complete the header information when creating candidate blocks.



The Organization of Transactions

Miners must arrange the transactions in their candidate blocks in a specific format, where only some of the information is included in the header.

Transactions form the backbone of the ***Bitcoin Network*** and are efficiently and securely organized through the use of **Merkle Trees**. These trees condense large amounts of data into a compact representation, improving the overall security and efficiency of the network.



The **Merkle Root Hash**, which is the data included in the header, is a **single hash value** that acts as a digital fingerprint for all the transactions in a block. This allows for efficient verification of transactions without having to examine each one individually, making it an important component of the security and scalability of the Bitcoin network.

If a transaction is included in a block, its hash will be included in the **Merkle Root Hash**. If any part of the data changes, the final code will be different, making it easy to detect any malicious changes to the data. This helps to maintain privacy and protect sensitive information contained within each transaction on the network.

If a hacker tries to alter a single character in a transaction, the subsequent block verifications will fail as each block depends on the information from the previous block. The Merkle Root acts as a secure chain that links all the transactions in a block, ensuring the accuracy and integrity of the data on the network.

A Coinbase transaction in ***Bitcoin*** is a special type of transaction included in every block of the blockchain. It serves two purposes: first, it rewards the miner who successfully mined the block and second, it provides an address to receive transaction fees as a commission.

This transaction is also included in the Merkle Tree. Unlike other transactions, the Coinbase transaction does not have an input as it generates new coins through the software algorithm. Instead, it creates a new unspent transaction output (UTXO), which can be used as input for future transactions.

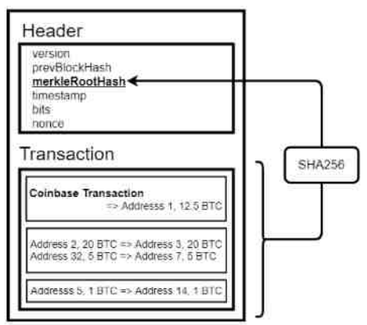
The Building Blocks of a Block: Understanding the Block Header in Blockchain

A **block header** is like the cover of a book; it provides a summary of its content and important details of a block.

- **The Block Hash**: The block's valid unique code by which it is identified. A **block hash** can be used to verify the consistency of information in a block each time it, or the information in it is checked.
- **Version**: This is like a label that tells you what version of the software the person who created the block used.
- **Previous block Hash**: This is the valid block hash for the block that came before the one you're looking at. It makes sure that the blocks are in the right order and that no one can change the previous blocks without it affecting the current and all the blocks that come after it.

Block Header

Version	1
Previous block	000000000000002efa96db4fd543284c4b8bdc21daaac75c9f311af6312da87d
Merkle root	ba3ffef2b2b29e6ae2fd4f7188c5c2ad13cfe618aa2cde86adacb6229e75b762
Timestamp	2012-08-31 11:32:28
Bits	436658110
Nonce	538012418

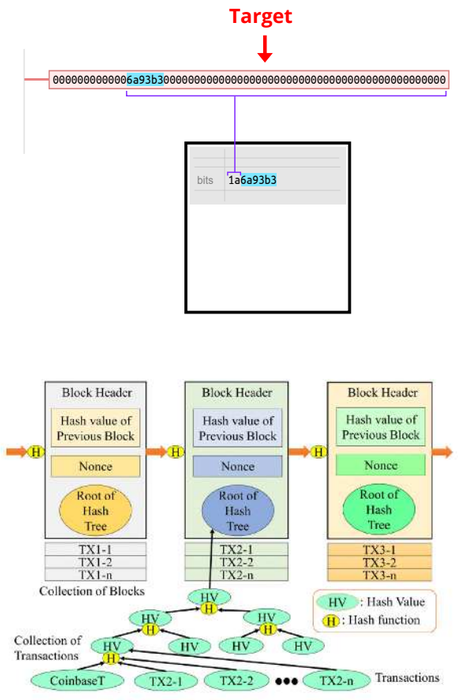


• **Merkle root hash**: **SHA256 (Hash(H(1,2),H(3,4,)), Hash(H(5,6),H(7,8).....))**. This updates specific UTXOs on the chain.

• **Time**: This is the time when the person who created the block started working on it.

• **Bits**: This is like a code that tells you how hard it was to make this block. It is also called the "**target value**".

• **Nonce**: A nonce is a unique number used by miners to create a new block in a blockchain. Miners try different nonces until they find one that gives them the correct hash value for the block, which proves that they did the necessary work to validate the block and add it to the *blockchain*.

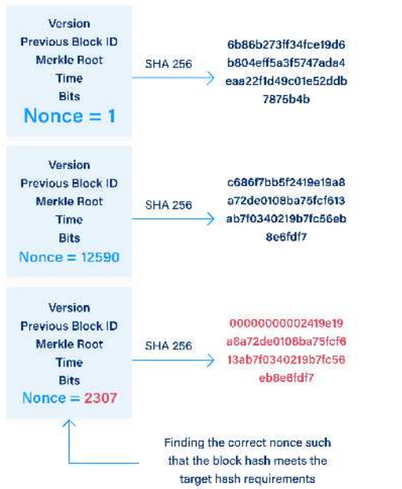


The Nonce Quest: Finding the Magic Number in the Blockchain Race

In the world of *blockchain*, each block has unique information and security measures in place to prevent tampering. One of these measures is the **nonce**, a number used once to create a **unique candidate block hash**.

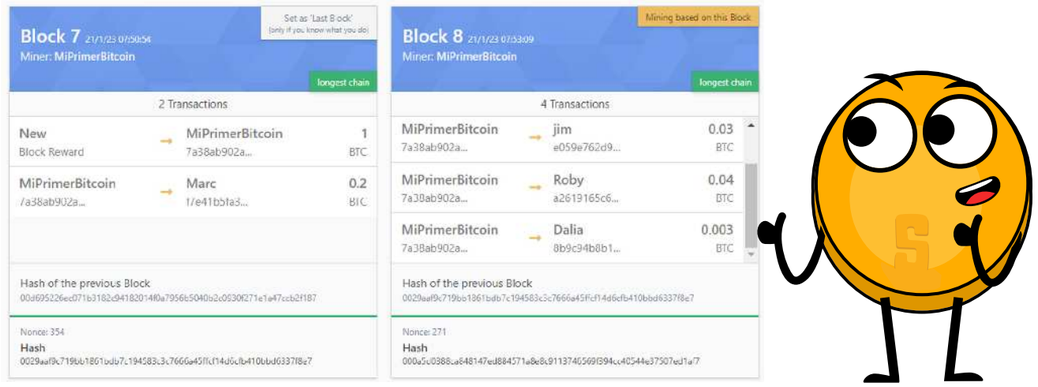
When a miner is trying to add a new block to the *blockchain*, they need to **find the right nonce** that will **produce a hash value that meets the target set by the network**. This is done by trying different nonce values and running them through the hash function until the correct one is found.

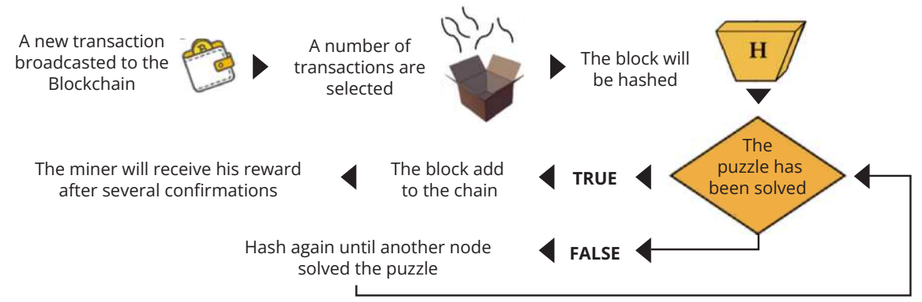
Remember that hash functions are highly sensitive to any changes in the input, which means even a small change in the **input** will result in a completely different **output**. So, by using a different nonce value, miners can ensure that each block they mine has a **unique hash value**.



The nonce is just one of the components in the block header, along with other important information such as the timestamp and the previous block hash. Once all of the information in the block header has been hashed together, it creates the **candidate block hash**. The miner who finds the hash value that meets the target set by the network is the one who wins the race and gets to add the block to the blockchain.

As we see below, for Block #7, **Mi Primer Bitcoin** was rewarded 1BTC for calculating the correct block hash required by the network at the time (21/1/23). In addition, MPB collected fees from the transactions included in the block. The **nonce** that finally produced the **winning hash** was 354.

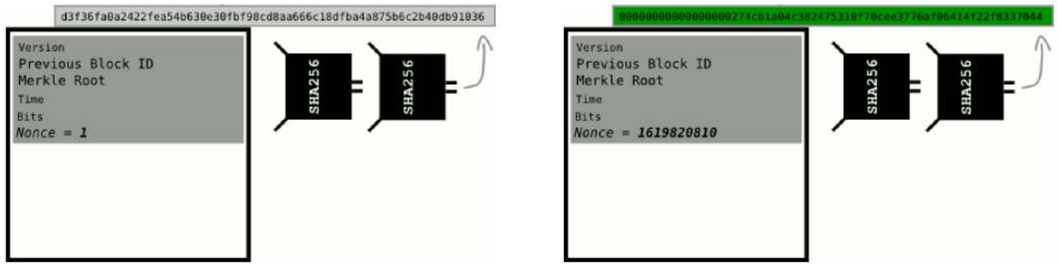




8.4 Rehashing the Hashes *- No Pun Intended*

How long does it take miners to discover a valid hash? And how quickly can they modify the nonce values during their calculation process?

In the example below, it took a miner 1619820810 iterations to find a hash value with the required number of zeros. The miner who succeeded in finding the right nonce value added the block to the blockchain, forming a secure and unalterable part of the chain.



The **hash rate** is a measure of the computational power of the network and the **speed at which miners can make nonce calculations**, which are used to find the correct block hash.

The more computational power a miner has, the faster they can make these calculations, which can give them an advantage in the mining process. However, as the network's hash rate increases, the difficulty of mining new ***bitcoin*** also increases, making it more challenging for all miners to find the correct **block hash**.

- Just like athletes upgrade their equipment to run faster, Bitcoin miners invest in specialized computer hardware to increase their **hash rate** and mine blocks more efficiently. The more resources they invest in, the better their chances of reaching the finish line first.
- Hash rate can be compared to the speed of the runner. The more powerful the miner's machine, the higher the hash rate, and the faster they can mine. However, just like in a race, having a high speed does not guarantee a win if the difficulty target has been adjusted to a higher level. Miners must constantly upgrade their equipment and improve their hash rate to stay ahead of the competition and have a chance of mining a block and winning the race.

The process of finding the correct **hash value** by changing the **nonce**, is what is called **mining**!

When we talk about individual miners and the entire network size, we use different SI-Prefixes which can be confusing.

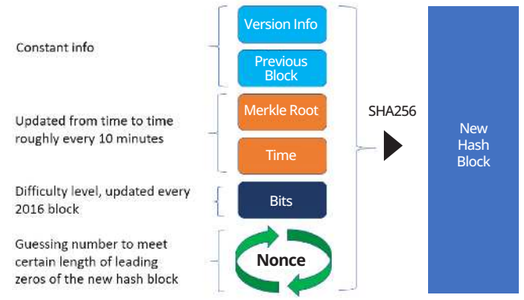
The main hash denotations are as follows:

- ***Bitcoin*** **mining machines** hash in Terahash per second (**TH/s**).
- The network's **total hash rate** is described in Exahash per second (**EH/s**)

Bitcoin Hash Rate:
1.1 Exahash / second

One hash / second
One **Kilo**hash = 1,000 hashes
One **Mega**hash = 1,000,000 hashes
One **Giga**hash = 1,000,000,000 hashes
One **Tera**hash = 1,000,000,000,000 hashes
One **Peta**hash = 1,000,000,000,000,000 hashes
One **Exa**hash = 1,000,000,000,000,000,000 hashes

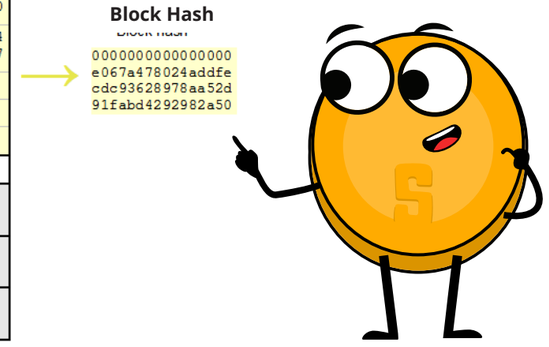
Bitcoin Block Hashing



The Block Hash can be referred to as the Proof of Work

In summary, every ten minutes or so, miners enter into a race to find a valid block hash. They begin taking all the data from their candidate blocks (which is summarized neatly in the block headers), double hashing it into a single hash, and comparing the output to a target hash value set by the network. If the block hash produced is too high, the miner adjusts the nonce and tries again, repeating this process trillions of times per second until one lucky miner finally finds a hash that meets the network's target.

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	



No matter how little, or how much mining hash power is applied, the average block is mined every 10 minutes.

- When the total **hash rate** decreases, the **difficulty level** decreases to make it easier for miners to mine new bitcoin.
  - This helps to keep steady the rate at which new ***bitcoin*** are mined.

- The difficulty adjustment is done using a formula that takes into account the average time it took to mine the previous 2016 blocks.
  - If the average time to mine 2016 blocks takes less than 14 days, the difficulty level is increased.
  - If the average time to complete 2016 blocks takes more than 14 days, the difficulty level is decreased.

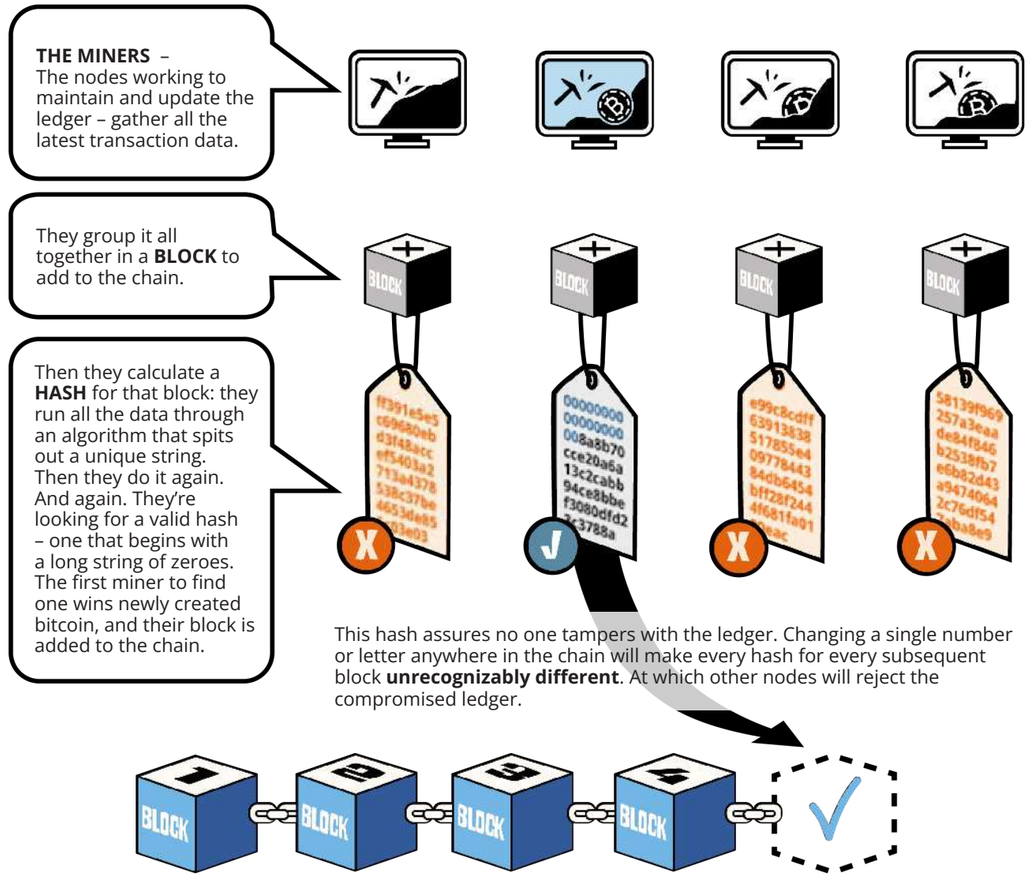
The Issuance Rate refers to the rate at which new coins are being added to the circulating supply, often through mining. This rate can be impacted by various factors, including changes in network hash rate, the number of blocks mined, and halving events, which reduce the number of coins that can be mined per block.

8.5 The Step-by-Step Process of Mining a Block

Mining a block in the ***Bitcoin Network*** involves several steps:

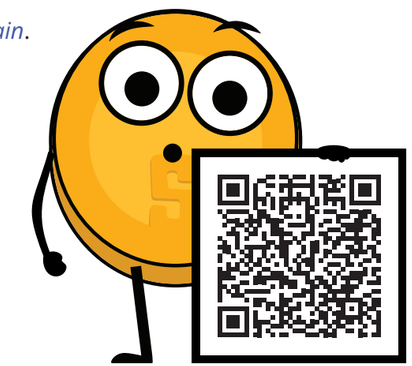
1. New transactions are broadcast to the network, picked up, and verified by the nodes.
2. Transactions are collected from the unconfirmed transactions in the **Mempool**. Transactions with higher fees are prioritized.
3. These transactions are then organized in a **Merkle Tree** and included in a **candidate block**, along with the **previous Block's Hash**, a **timestamp**, and a **nonce**.
4. Miners compete to solve a mathematical puzzle based on the information in the block, including the transactions and a random number.
5. The puzzle involves finding a specific number (the "hash") that, when combined with the block data, results in a value that is less than a target number.

In other words, miners use **proof-of-work** to adjust the **nonce** value until a hash is obtained that meets the **specified difficulty** requirements.



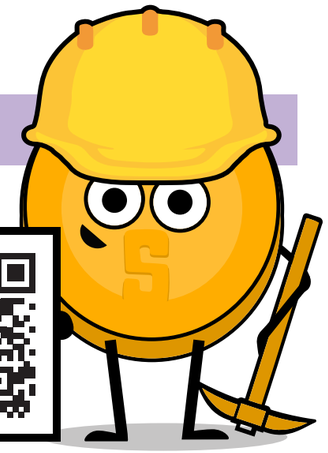
6. The miner who first finds the correct hash broadcasts it to the network, and the other miners check the solution to verify that it is indeed correct.
7. If the solution is verified, the block is added to the *blockchain*.

The **mined block** is broadcasted to the network for **verification** and once it is verified by other miners and consensus is reached among the network, the block is added to the ***blockchain*** as the last block in the chain.



8. The miner who successfully mined the block is **rewarded with newly minted *bitcoin* from the coinbase transaction** and the transaction fees from the included transactions.
9. The new block becomes part of the immutable and transparent record of all transactions on the *blockchain*. The block hash and the information in it is used to update the *blockchain* and the process starts again with the next block.

8.5.1 Class Exercise: Mining Interactive Exercise



Class Exercise. Follow the following instructions:

1. Visit the following websites:

https://chainflyer.bitflyer.jp/

https://mempool.space/

You can scan the following QR Codes:

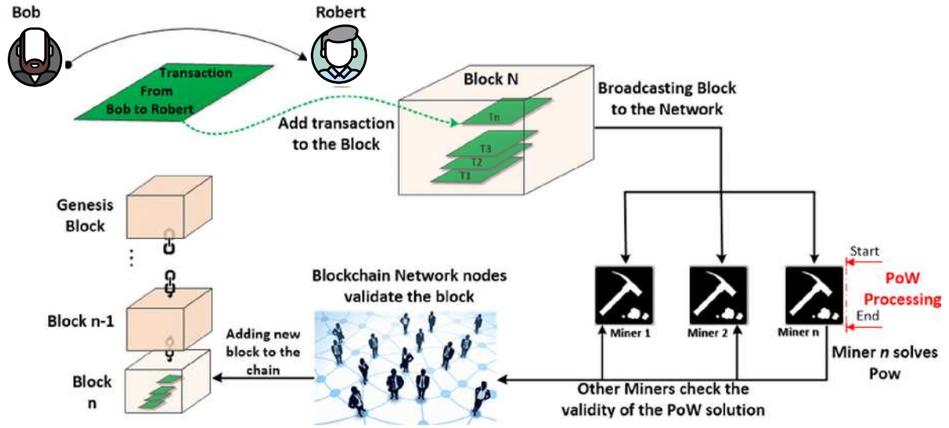
2. Review the various elements displayed on the page, including the latest blocks, confirmed transactions, the number of transactions, memory usage, and approximate value of the entire block.
a. Answer the questions:

i. What was the last mined block?

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

8.5.2 Summary of the Transaction from Start to Finish

1. A user wants to send some ***bitcoin*** to another user. They create a transaction with the details of the send, including the amount of ***bitcoin*** being sent, the sender's address, and the receiver's address.
2. The user then uses their **private key** to encrypt the transaction. This private key is like a secret code that only the user knows and it is used to prove that the user is who they say they are.
3. The encrypted transaction is broadcasted to the network of ***Bitcoin*** nodes.



4. The nodes verify the transaction using the sender's **public key**, which is available on the *blockchain*. They check that the signature is valid and that the sender has enough ***bitcoin*** to complete the transaction.
5. The nodes then group the verified transactions into a block.
6. The block is then broadcasted to the network of ***Bitcoin*** miners.
7. Miners use a complex mathematical algorithm to solve a puzzle, which is called "mining." Once the puzzle is solved, it is added to the *blockchain* and the block is added to the chain.
8. Once the block is added to the *blockchain*, the transaction is considered complete and the receiver can access the ***bitcoin*** using their own **private key**.

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

8.5.3 Don't Trust, Verify

In the world of ***Bitcoin***, the phrase '**Don't trust, verify**' emphasizes the importance of independently verifying transactions rather than relying on a centralized authority or intermediary. This is a fundamental aspect of the ***Bitcoin network***, which is designed to be decentralized and secure through the use of a distributed network of nodes. By verifying transactions on their own, users can help maintain the integrity of the network and ensure that no single entity has control over it.

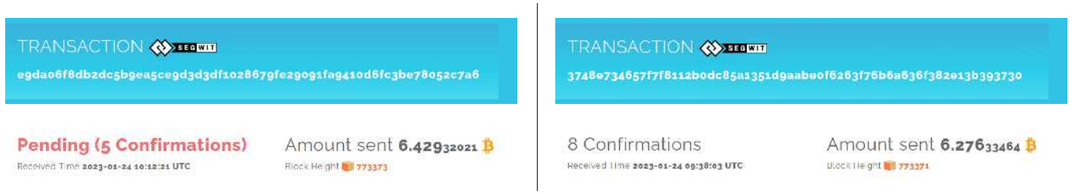
However, there are scenarios that can cause transactions to be **reversed**, such as **double-spending**, **orphaned blocks**, and **reorganization**. To increase the security of transactions, it is recommended to wait for 6 confirmations, or 6 blocks containing the specific transaction, before considering it final. The more confirmations a transaction has, the more secure it becomes as the likelihood of it being reversed decreases. The number of confirmations needed may vary depending on the use case and desired level of security.

- **Double-spending**: In a double-spend attack, a malicious actor attempts to spend the same bitcoin twice by manipulating the network to accept their second spending of the same ***bitcoin*** as valid. If a miner or group of miners controlling more than 50% of the network's **hashing power** (known as 51% attack) confirm a double-spend transaction, it could be added to a block and considered valid, effectively reversing the original transaction.

- **Orphaned blocks**: When two miners find a new block at the same time, the network may temporarily accept both. When one of the blocks is later extended by additional blocks, the network will recognize this chain as the main chain and the other block will become an orphan, no longer part of the main *blockchain*. The transactions included in the orphaned block are not lost and will be included in a later block if they remain valid.

An orphaned block in ***Bitcoin*** is a valid block that is not included in the longest chain, which is considered the main chain.

- **Reorganization**: This could theoretically happen if a new block were added to the blockchain and it causes the existing chain to be replaced by a different one. If a transaction was included in a block that is no longer on the main chain, it would be considered invalid and the transaction would be reversed.



8.6 Class Exercise: Transaction with UTXO's

Class Exercise. Follow the following instructions:

1. Understand your role: You have been assigned one of the following roles: sender, receiver, node, or miner.
- As a **sender**, you will be responsible for creating and broadcasting transactions.
- As a **receiver**, you will be responsible for receiving and verifying transactions.
- As a **node**, you will be responsible for validating the transactions and following the rules.
- As a **miner**, you will be responsible for verifying, adding the transactions to the *blockchain* and collecting rewards for your hard work.

2. If you are the **sender**, create a transaction: To create a transaction, follow these steps:
- Take a transaction form and fill in the following fields:
  - Input UTXO: 20BTC
  - Output UTXO: 10BTC to the receiver's address
  - Output UTXO:1 BTC to the miner's address
  - Change UTXO: 9 BTC to your address
  - Signature: Your signature simulating a private key.

- Pass the transaction form and the corresponding number of coins to the receiver.

3. If you are the **receiver**, Verify transactions: Follow these steps:
- Check the transaction form to ensure that the correct number of coins and the receiver's name or initials are written.
- Count the coins you received and compare them to the number of coins written on the transaction form.
- If the coins match, check the approval box on the UTXO chart that is shared and accessible to everyone in the class.
- If the coins do not match or you have doubts, reject the transaction and write the reason on the UTXO chart.

4. If you are a **node**, validate transactions: As a node, you are responsible for validating the transactions by checking that the transaction is valid by checking it against the rules of the protocol and the consensus mechanism.
- Verify that the sender's address is valid and that the receiver's address is valid.
- Check that the sender has enough funds to complete the transaction by verifying that the UTXO used as input in the transaction actually exist and have not been spent before by looking at the UTXO chart.
- Check that the transaction does not double-spend any coins by looking at the UTXO chart.

5. If you are a **miner**, add transactions to the *blockchain*: As a miner, you are responsible for adding the transactions to the *blockchain*. Follow these steps:

- Check the transactions that have been approved by the receivers and validated by the nodes.
- Roll the dice and compare the numbers with the other miner. The miner with the smaller roll number (under 25) will add the transaction to the *blockchain*.
- For your time, energy, and effort, you will receive a reward ...1BTC.
- Once a transaction is added to the blockchain, it cannot be changed or reversed.

6. Keep track of your coin balance: Throughout the activity, keep track of your coin balance by counting the coins in your digital wallet.

7. Discuss with your classmates and teacher the key concepts learned.

Chapter #9

Why Bitcoin's Intrinsic Value Is Anything but Hollow

9.0 Why Bitcoin?
9.1 The Future of Bitcoin
    9.1.1 The Lindy Effect
9.2 Using Bitcoin for More Than Just Digital Money
9.3 The Challenges
    9.3.1 The Regulatory Environment for Bitcoin
    9.3.2 Understanding the Energy Usage of Bitcoin Mining
9.4 The Risks
9.5 Trading and Investing in bitcoin

9.0 Why Bitcoin?

Bitcoin is not just a technology, it's a powerful movement for positive change that has the potential to transform the lives of people all over the world. It represents a peaceful revolution towards collective freedom and equity, opening up new opportunities for humanity. As a decentralized global network, ***Bitcoin*** enables greater financial freedom, shifting power from the few to the many. It provides a secure, censorship-resistant platform for storing and transferring value, empowering individuals to take control of their wealth and protect their purchasing power. This is especially important in today's uncertain economic climate, where the traditional financial system is facing unprecedented challenges. Integrating ***Bitcoin*** into one's life means greater autonomy and the ability to achieve one's full potential.

The possibilities for positive change are immense, which is why we invite you to watch this video to learn more.



9.1 The Future of Bitcoin

"**Hyperbitcoinization**" is a theoretical future where ***Bitcoin*** becomes the dominant global currency. This would mean that bitcoin would be used by everyone, everywhere, and for everything - from buying coffee to paying bills and even to buy a house.

The growing interest in ***Bitcoin*** by billionaires, countries, and governments highlights the potential impact of its widespread adoption on the economy and society. Here are some of the benefits of a hyper-bitcoinized world:

1. A Revolution in the Remittance Market: The remittance market involves the transfer of funds from one party to another, often across international borders. Despite declining costs, remittances remain relatively expensive compared to domestic bank transfers, especially for smaller amounts. ***Bitcoin*** has the potential to revolutionize the remittance market by reducing costs to near-zero through its Lightning Network layer 2 protocol. The Lightning Network offers fast and low-cost transactions, making it well-suited for the remittance market and addressing the high costs and other challenges associated with remittances, such as slow settlement times and restrictions on business hours.

2. A Self-Sovereign Future: A self-sovereign future is one where individuals have full control over their own digital identity and assets. It could lead to greater financial inclusion, privacy, and security, and increase the value placed on privacy in transactions.

3. Changes in Monetary Policy: If ***Bitcoin*** were to become widely adopted, it could challenge the ability of governments to control the money supply through traditional monetary policy tools, leading to changes in monetary policy management and implementation. It could also increase financial inclusion, equality, and opportunities, as well as reduce the ability of governments and financial institutions to manipulate the economy.

4. A Reliable Store of Value: ***Bitcoin***'s digital scarcity makes it a reliable store of value, which could encourage more people to use it as a means of saving for the future.

5. Enhanced Transparency and Traceability: The tamper-proof and immutable record of all transactions on the blockchain could increase transparency and accountability in various industries and sectors.

6. Improved Cybersecurity: The decentralized structure of Bitcoin makes it less vulnerable to hacking and data breaches, improving overall security.

7. Reducing Carbon Footprint and Promoting Renewable Energy: By making the process of mining for bitcoin more sustainable and environmentally friendly, miners can help to reduce its carbon footprint and promote the use of renewable energy sources. This aligns with important environmental, social, and governance (ESG) considerations.

9.1.1 The Lindy Effect

The Lindy Effect is a simple theory that says the longer something has been around, the more likely it will continue to be around in the future. This theory can be applied to many things, including ***Bitcoin***.

Bitcoin, a decentralized digital currency that has been around since 2009, is a prime example of the Lindy Effect in action. Despite facing numerous challenges over the years, including technological changes, security breaches, and government regulations, Bitcoin has continued to grow in popularity and has been adopted by an increasing number of businesses as a means of payment.

Acing the Test of Time



One of the key reasons for ***Bitcoin***'s longevity and continued use is its decentralized nature. This means that it operates as a secure and transparent financial system without the need for intermediaries, making it appealing to individuals who value financial privacy and control. In addition, ***Bitcoin***'s ability to operate as a secure store of value has also contributed to its growing popularity and acceptance.

Another factor that contributes to ***Bitcoin***'s longevity is its resistance to change and competition. Changes to the network consensus rules require the majority of users to agree to the update, making it difficult to achieve consensus and leading to only updates that the overwhelming majority of network participants agree upon being implemented. Additionally, despite the existence of many competing cryptocurrencies, none have yet been able to match ***Bitcoin***'s longevity or achieve the same level of network effects.

Bitcoin's hash rate has been increasing exponentially over the years and the distribution of mining is also becoming more widespread. The number of users joining the ***Bitcoin Network*** has also increased at an exponential rate, with an estimated 140-190 million users now a part of it. These factors, combined with its continued popularity and usefulness, suggest that ***Bitcoin*** is likely to continue being used and trusted into the future.

9.2 Using Bitcoin for More Than Just Digital Money

Bitcoin has gained popularity for various reasons beyond just being a means of making money. Some users are driven by the idea of creating a financial system that is free from central control, while others simply want to benefit financially.

Bitcoin also allows for the creation of unique **digital artifacts** known as **Satoshi inscriptions**. These inscriptions, which can include text, images, videos, audio, and software, are stored on the ***Bitcoin*** *blockchain*, making them immutable, secure, and decentralized. The unique identification of each Satoshi is made possible through **Ordinals**. Unlike traditional NFTs, these inscriptions don't require a separate infrastructure or token, which further enhances their security and decentralization.

The combination of ***Bitcoin*** and AI can be utilized for various applications such as cryptocurrency trading, security, and market analysis.

Bitcoin's lightning network has made faster and more secure financial payments possible. For example, atomic swaps enable people to exchange one cryptocurrency for another without the need for an intermediary. RSK, a platform built on top of the ***Bitcoin*** *blockchain*, also allows for the creation of smart contracts and decentralized apps, which opens up new possibilities for what can be built on top of ***Bitcoin***.

As these technologies continue to be developed and improved, exciting things are expected to come in the future.

9.3 The Challenges

Bitcoin Core is a powerful and widely-used implementation of the ***Bitcoin*** protocol. However, there are a few areas in which it could be improved:

1. Scalability: As the number of users and transactions on the network grows, the amount of data that needs to be stored and processed by nodes can become quite large. This can slow down the validation of transactions and make it more difficult for new users to join the network.

2. Privacy: While ***bitcoin*** transactions are pseudonymous, the *blockchain* is publicly accessible, which means that it is possible for third parties to track the flow of funds and identify users. There are some proposed solutions to this problem, such as the use of **coin mixing** and stealth addresses, but they are not yet widely adopted.

3. Usability: For the average user, the process of setting up and using a full node can be quite technical and daunting. Simplifying the user experience and making it more accessible to a wider range of people could help to increase adoption.

4. Decentralization: ***Bitcoin***'s current consensus algorithm is **Proof-of-Work**, which can be mined by specialized and large mining farms. This can lead to a concentration of mining power and threat to the decentralization and security of the system.

5. Security: While ***Bitcoin Core*** is open-source, which means that its code can be audited by anyone, it's still possible for bugs or vulnerabilities to be introduced into the code. Continuously auditing and improving the security of the software can help to protect users from potential attacks. For example, if an attacker were to generate a private key that corresponds to a large number of ***bitcoin***, they could steal those ***bitcoins***.

Overall, while ***Bitcoin Core*** is a solid piece of software, ongoing development and research is essential to address these areas of improvement and ensure that the network remains secure, decentralized and widely adopted.

9.3.1 The Regulatory Environment for Bitcoin

The cryptocurrency market has faced numerous challenges in recent years, including the collapse of FTX in 2022 and the fall of stablecoins TerraUSD and LUNA earlier in the same year, leading to significant losses and a decline in investor confidence. The risks associated with investing in cryptocurrencies include volatility, difficulty in evaluating assets, custodial risks, unregistered assets and providers operating outside of regulatory frameworks, and unpredictable regulations.

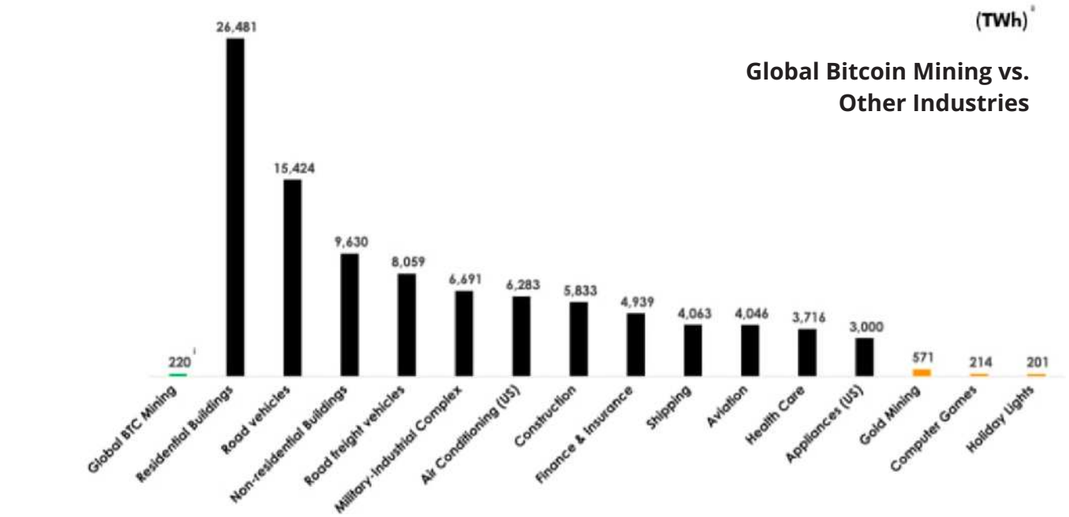
The regulation of cryptocurrencies, including ***Bitcoin***, has been a topic of debate among governments and financial regulators worldwide. While some have banned cryptocurrencies, others have sought to regulate them in a way that balances innovation and consumer protection. The U.S. SEC Chairman

Gary Gensler recently stated that the regulation of the cryptocurrency market is getting closer and that ***Bitcoin*** will be considered a commodity. According to the SEC, many tokens in the market have the key attributes of securities and will fall under the jurisdiction of the SEC, while ***Bitcoin*** falls under the oversight of the Commodity Futures Trading Commission (CFTC) as a commodity. The SEC has work to do to introduce comprehensive laws that protect investors, and this decision by the SEC chair is seen as positive by some investors, leading to the expectation of gradually rising prices. Despite the current market volatility, some investors view this as a buying opportunity and believe in the future of digital currencies as a borderless, decentralized, tamper-proof, and unconfiscatable form of money.

9.3.2 Understanding the Energy Usage of Bitcoin Mining

Bitcoin mining uses a lot of energy, around 79 terawatts-hours per year. However, this does not necessarily mean that it is a waste of energy or harmful to the environment. ***Bitcoin*** mining can help to utilize unused capacity of energy, especially in remote or inaccessible places. Additionally, most ***Bitcoin*** mining is done with renewable energy such as hydroelectric, solar, wind, and geothermal. This helps to make the production and research of these energy sources more profitable. Furthermore, ***Bitcoin*** mining provides security for the ***Bitcoin network***, enabling people to have access to secure and accessible money.

However, it's important to note that the energy usage is determined by the competition among miners, not the number of transactions. The digital signature validation process, which is a small part of mining, uses minimal energy. The energy usage of ***Bitcoin*** mining is high, but it is not as high as other industries like the traditional financial system or gold mining and recycling. Miners are also increasingly using clean and renewable energy sources like geothermal and hydroelectric power to power their mining operations.



The key to reducing the environmental impact is to drive the demand for green energy, and as the industry grows, it's leading to innovation in clean energy production and decreased pollution. It's also important to note that the source of energy used by miners greatly impacts the ecological impact. As the technology and industry evolve, more miners are using renewable energy sources such as hydroelectric, solar, and wind power, which greatly reduces the environmental impact.

9.4 The Risks

Bitcoin can offer great freedom, but it's important to remember that with great power comes great responsibility. There are risks involved in using ***bitcoin***, so it's essential to understand these risks and take proactive steps to protect your funds.

1. Volatility: It is commonly believed that ***bitcoin*** is inherently volatile. However, it is important to note that the volatility of ***bitcoin*** depends on the currency in which its value is measured. For example, if ***bitcoin*** value is measured in a currency that is itself volatile, such as the Venezuelan bolivar or the Zimbabwean dollar, then the volatility of ***bitcoin*** may appear even more extreme. ***Bitcoin*** is not primarily a way to invest but to save for the future; as with any investment, it is important to have a long-term perspective and to be aware of the risks involved.

2. The **risk of custodial wallets** is significant and should not be overlooked. Funds held by third-party custodians are always connected to the internet, making them vulnerable to loss, hacking, and breaches. Furthermore, custodians control and decide whether people can withdraw their funds or not, posing a substantial risk that cannot be ignored.

3. Decentralized systems like ***Bitcoin*** are vulnerable to risks posed by malicious nodes that could harm the network. However, it's important to note that ***Bitcoin*** has become very strong nowadays and is basically unstoppable. If a large number of malicious nodes try to cause trouble or change the rules, all of the current ***Bitcoin*** core nodes will simply ignore and continue maintaining the original Bitcoin code/software.

That being said, there are still potential security threats to the ***Bitcoin network***. One such threat is a 51% attack, which occurs when a single miner or group of miners control more than 50% of the total computational power or hashrate of the network. This would allow them to take control of the network and potentially manipulate the blockchain by either preventing new transactions from being added or modifying transactions in their favor.

If an attacker were to successfully perform a **51% attack**, they could double-spend ***bitcoin***, which means they could spend the same bitcoin more than once. This would allow them to effectively steal ***bitcoin*** or commit fraud on the network. However, executing a 51% attack is incredibly difficult and costly, as it would require controlling a significant amount of computational power, and the costs involved in obtaining such power could outweigh any potential gains from the attack.

It's important to note that the ***Bitcoin network*** has never been successfully attacked in this way, but the possibility of a 51% attack is always present, and it highlights the importance of ensuring that the network remains decentralized and secure.

4. Lack of regulation: ***Bitcoin*** is not regulated by governments or financial institutions, which means there is little oversight to protect consumers.

5. Security risks: ***Bitcoin*** exchanges and wallets can be subject to hacking and theft, which can result in the loss of funds for users.

6. Scams: There are many scams related to ***Bitcoin*** that can lead to the loss of funds for investors.

7. Illicit activities: ***Bitcoin*** has been used for illegal activities like money laundering and buying illegal goods on the dark web.

8. Lack of understanding: ***Bitcoin*** is complex and can be difficult to understand for the average person, which can lead to poor decision making and potential losses.

9. Lack of acceptance: ***Bitcoin*** is not widely accepted as a means of payment, which limits its usefulness in everyday life.

10. Technical risks: ***Bitcoin*** is subject to technical risks like bugs and errors, which could lead to problems and potentially a loss of value.

11. Quantum computing: Quantum computing could potentially compromise the security of ***Bitcoin*** by breaking the encryption used to secure transactions and wallets.

Quantum computing is a way of doing computer calculations that's different from the way most computers work today. Instead of using just "on" and "off" states like traditional computers, quantum computers use "**qubits**" that can be in many states at the same time. This makes quantum computers potentially much faster at certain types of calculations than regular computers.

12. Digital Threats: Hackers can exploit your internet connection to access your **private keys** and sensitive data, which includes hacking software wallets, clicking malicious links, and falling for spyware scams.

13. Social Engineering Scams: Scammers can manipulate you into confirming transactions by posing as customer service agents or creating a false sense of trust, so it's important to be cautious and not share your recovery phrase.

14. Blind Signing: Lack of transparency can lead to blind signing, where you agree to transactions without fully understanding the details, so it's important to educate yourself on the latest scams and choose a wallet that displays full transaction details.

To protect your ***Bitcoin*** security, use an offline wallet, read full transaction details, and continuously educate yourself on the latest threats. Don't let ignorance and a false sense of trust compromise your hard-earned assets.

While the risk of quantum computing to ***Bitcoin***'s security is real, it's important to remember that it's still a speculative threat and it's uncertain when or if it will become a reality. A 51% attack on ***Bitcoin*** is a concern, but it would be costly and not very beneficial for the attacker. More efficient and cost-effective methods of attack, such as DDoS, would be more likely for a rational actor seeking to commit fraud.

9.5 Trading and Investing in bitcoin

We will explore the topic of trading and investing in ***Bitcoin***, but it's important to note that the primary goal of using ***Bitcoin*** is not to make short-term profits through speculative trading. Instead, the main goal is to protect oneself from inflation and the potential destruction of traditional fiat currency systems. While it is possible to use ***Bitcoin*** as an investment tool, it's crucial to approach it with a long-term mindset and a focus on its fundamental principles of decentralization and financial sovereignty. This section will provide insights into the risks and benefits of investing in ***Bitcoin***, as well as practical tips for buying, holding, and using ***Bitcoin*** for its intended purpose as a decentralized and secure store of value.

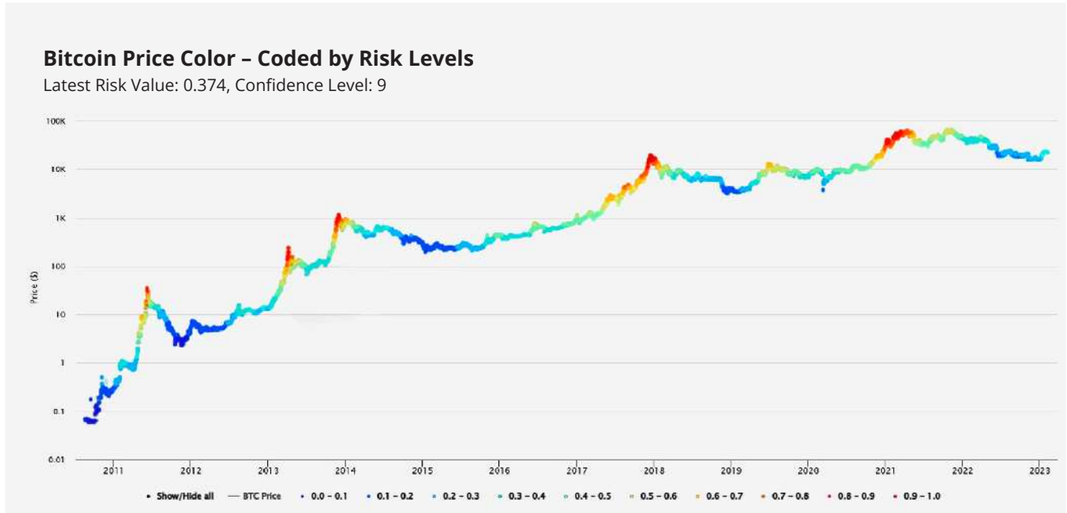
Market trends refer to the general direction that the market is moving in. A bullish trend is when the market is on an upward trajectory, while a bearish trend is when the market is on a downward trajectory. This is usually associated with investor optimism and an expectation that prices will continue to rise. In contrast, a bearish trend is when the market is on a downward trajectory, characterized by lower highs and lower lows. This is usually associated with investor pessimism and an expectation that prices will continue to fall.

Technical analysis is not a perfect science, and past performance is not always indicative of future results. It should be used in conjunction with other forms of analysis, such as fundamental analysis and market sentiment, to make informed trading and investment decisions.

The Risk Metric chart, created by Benjamin Cohen, is a quick and intuitive way to understand market sentiment and asses potential buying or selling opportunities for bitcoin. This chart displays the price of the assets and assigns a color-coded value to represent the risk associated with that price. The risk values range from 0 to 1, with darker red colors indicating higher risk and darker blue colors indicating lower risk.

The purpose of the **Risk Metric** is not to predict market tops or bottoms, but rather to identify areas that may be attractive for buying or selling in the long term. A low risk score suggests that bitcoin may be undervalued and may present an opportunity to buy, while a high risk score suggests that it

may be overvalued and may present an opportunity to sell.

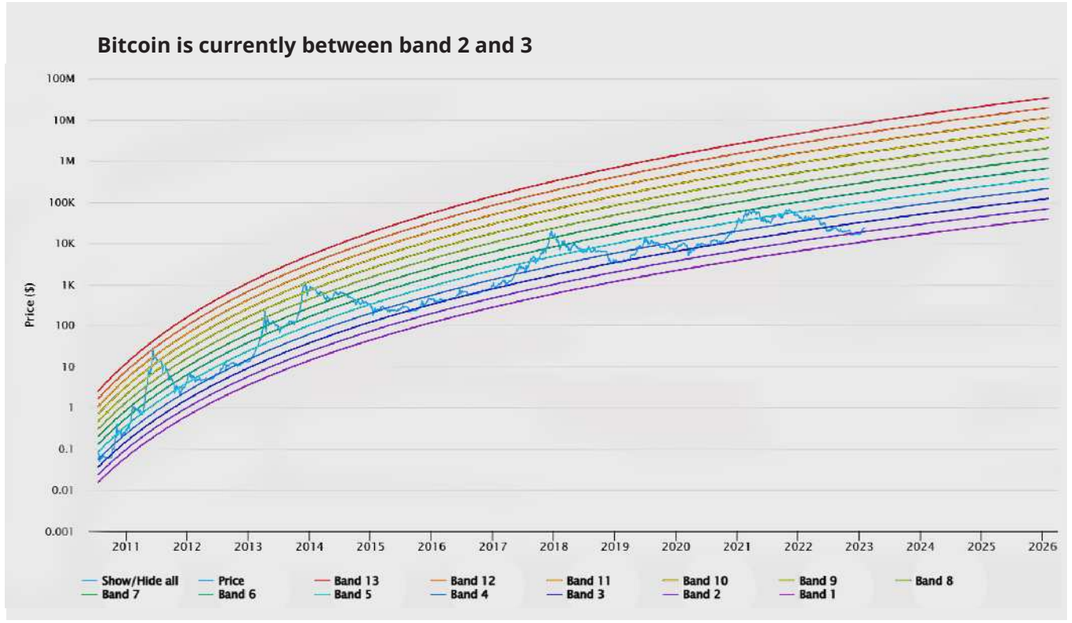


The logarithmic market price is a method of visualizing the price movements of an asset, such as bitcoin, over time. This approach uses a logarithmic scale on the y-axis to better reflect the exponential growth that is often seen in asset prices.

The logarithmic market price is being used to track the price movements of bitcoin over time and to identify potential peaks and accumulation zones. The market cycles referred to in the example are periods of price increase and decrease, and the rainbow bands are used to illustrate the relative magnitude of these price movements.

The logarithmic market price can be useful for identifying potential accumulation zones, or periods where the price may be relatively low and provide a good opportunity for buying. In the example, the zones between band 3 and 4 are identified as good accumulation periods for market cycles 3 and 4.

Market cycles in ***Bitcoin*** refer to the recurring pattern of growth and contraction in its price and market activity. It is characterized by periods of speculation and hype, followed by correction and consolidation. Some analysts argue that the cycles are strongly correlated to the halving events.



It is important to note that while the logarithmic market price can provide valuable insights, it is only one of many tools that can be used to analyze market trends and price movements, and should be used in conjunction with other analysis methods to form a more complete understanding of the market. Additionally, market conditions are constantly changing, and past performance is not a guarantee of future results.

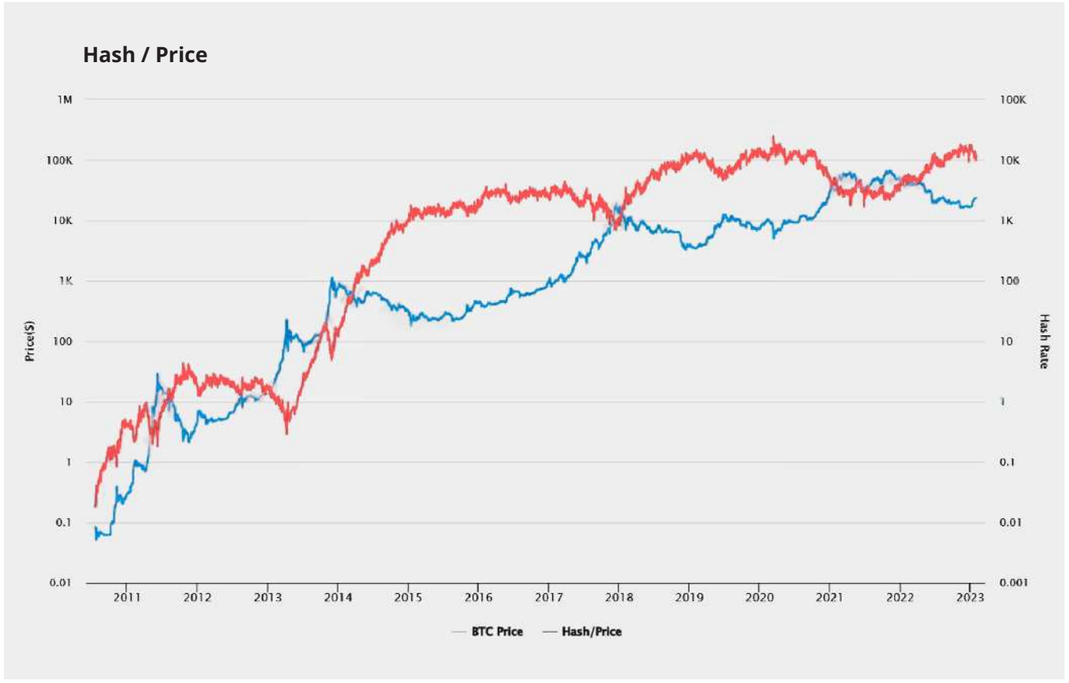
The Hash/Price ratio and Price/Hash ratio are metrics used to compare the growth of the ***Bitcoin*** price and the growth of the ***Bitcoin Network***'s computational power, or hash rate. These metrics are used to help understand the relationship between the two, and how changes in one may affect the other.

When the price of ***bitcoin*** increases at a faster rate than the hash rate, the Hash/Price ratio decreases and the Price/Hash ratio increases. This means that the price of ***bitcoin*** is growing faster than the computational power of the network, which could indicate increased demand for ***bitcoin***.

However, near local peaks, when the price of ***bitcoin*** is increasing quickly, you may see sudden drops in the Hash/Price ratio. This is because the growth in price outpaces the growth in computational power, leading to a decrease in the Hash/Price ratio.

On the other hand, if both the hash rate and price of ***bitcoin*** decrease or increase at the same relative rates, the ratios will stay constant. This means that the computational power of the network

and the price of ***Bitcoin*** are growing at the same rate.

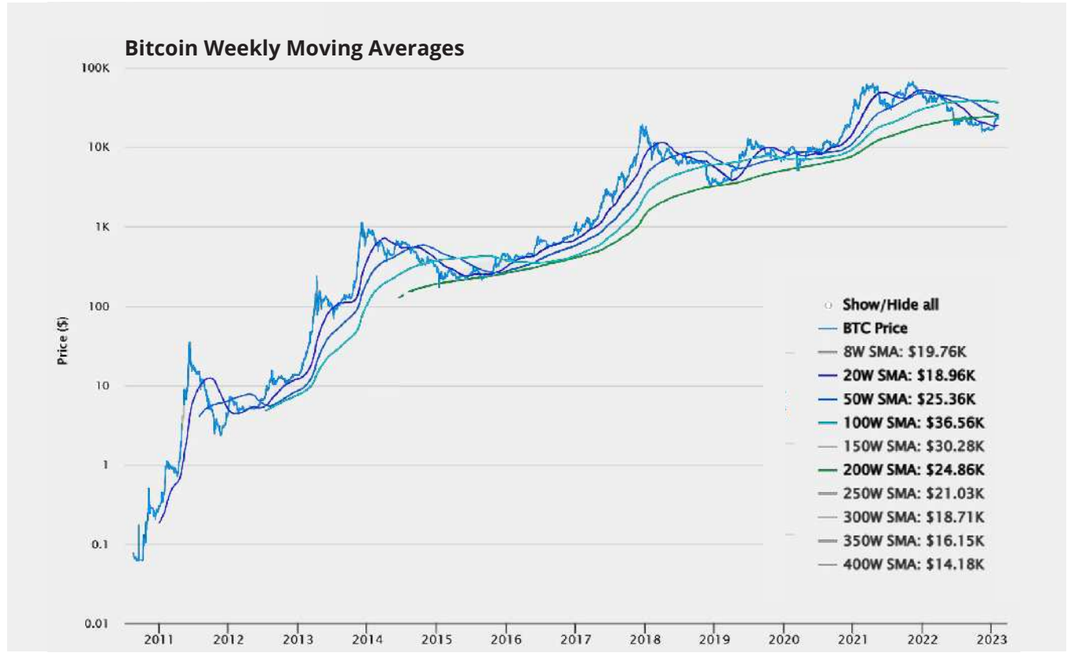


If the hash rate of the ***Bitcoin Network*** is increasing at a faster rate than the price of ***bitcoin***, the Hash/Price ratio will increase and the Price/Hash ratio will decrease. This could indicate that the network is becoming more secure and more capable of processing transactions, which could have a positive impact on the price of ***bitcoin*** in the future.

Trend lines are used to identify a current trend in the market. They are formed by connecting two or more price points and are used to indicate a level of support or resistance. A trend line that is angled up is considered bullish, while a trend line that is angled down is considered bearish.

Moving averages are used to smooth out the volatility of a security's price over a specific period of time. They are calculated by adding up the closing prices of a security over a specific number of periods and then dividing by the number of periods. A moving average can be used to identify the direction of a trend and can also be used to generate buy and sell signals. **Dollar-cost averaging** (DCAing) below shorter term moving averages like the 100-week and 50-week SMA can provide more entry points, but it may leave you at a loss in the short term.

Dollar-cost averaging (DCA) is a strategy of investing a fixed amount of money into a particular asset at regular intervals, regardless of the price.



The goal of DCA is to reduce the impact of market volatility on an investment portfolio by spreading out the purchases over time, instead of buying all at once.

• For example, an investor may decide to invest $100 into ***bitcoin*** every month. If the price of the asset is high, the investor will purchase fewer units, and if the price is low, the investor will purchase more units. Over time, this approach can lead to a lower average cost per unit of the asset, and thus reduce the impact of short-term price fluctuations.

DCA can be used in a variety of investments, including stocks, bonds, and commodities, and is often recommended for individuals who are just starting to invest and want to minimize the risk of market volatility.

It's important to note that DCA does not guarantee a profit or protect against loss in a declining market, and should be combined with thorough research and market analysis. Additionally, investors

should consider their own financial goals and risk tolerance when deciding on the best investment strategy.

Indicators such as the **RSI** and the **MACD** are used to identify overbought and oversold conditions and potential trend changes. The RSI compares the magnitude of recent gains to recent losses to determine overbought and oversold conditions. The MACD is calculated by subtracting the 26-period exponential moving average (EMA) from the 12-period EMA, and then plotting a 9-day EMA of the result. It is used to identify changes in momentum and trend.

It is important to note that these metrics are only one of many tools that can be used to analyze market trends and price movements, and should be used in conjunction with other analysis methods to form a more complete understanding of the market. Additionally, market conditions are constantly changing, and past performance is not a guarantee of future results.

Chapter #10

From Bits to Bitcoin: Piecing Together the Puzzle

10.0 Just Some Facts, a Few Jokes... and the Lingo.
10.1 My First Bitcoin Final Project Submission and Evaluation Guidelines

10.0 Just Some Facts, a Few Jokes… and the Lingo



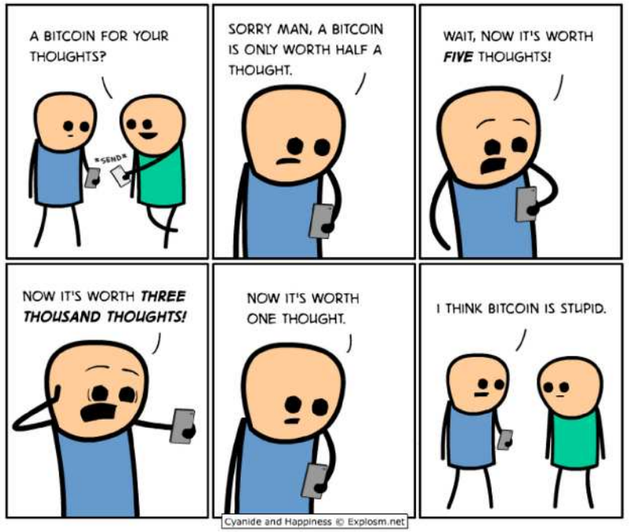


The Bitcoin Network *is more powerful than* 500 supercomputers put together.

Refunds are **not possible** on ***bitcoin*** transactions.



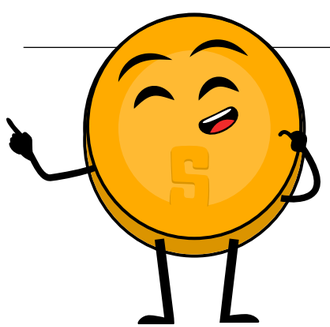




How many miners does it take to change a light bulb?

- A million.

One miner to change it, and 999,999 miners to run in circles to determine who gets to do it.



10.1 My First Bitcoin Final Project Submission and Evaluation Guidelines

Introduction:

The final project of **My First Bitcoin** course is a 1-2 page essay titled *"Why Bitcoin?"* where you will be asked to explain what ***Bitcoin*** is, how it works and what are the ways it changes the world today.

Requirements:

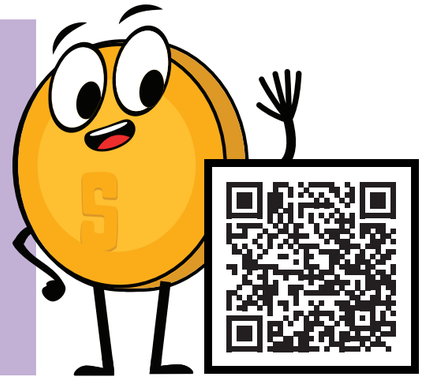
- The essay should be a minimum of 1 page and maximum of 2 pages, double spaced, 12-point font.
- The essay should be written in proper English and free of grammar and spelling errors.
- The essay should include an introduction, body, and conclusion.

Topics to Cover:

- Explain what ***Bitcoin*** is and its history.
- Explain how ***Bitcoin*** works, including its key features such as decentralization, transactions, and mining.
- Discuss at least two ways ***Bitcoin*** changes the way the world operates today. Provide examples and evidence to support your answer.

Alternative Project:

For those who prefer a hands-on experience, you can participate in the Final Activity (Bitcoin Simulator) using the *Bitcoin Blockchain Simulator Tool*: **https://www.bitcoinsimulator.tk/**.
Here you will create a new wallet and receive a private key, which will allow you to mine a block, sign transactions, create a private blockchain, and perform a 51% attack.



Evaluation Criteria:

The following criteria will be used to evaluate your final project:

- Clarity of explanation of what ***Bitcoin*** is and how it works.
- Use of examples and evidence to support your answer.
- Coherence and organization of the essay.
- Proper use of grammar and spelling.
- Relevance and depth of discussion on the topic.

Submission:

The final project should be submitted in a Word or PDF format via email to the course instructor by the deadline specified in the course syllabus. Late submissions will not be accepted.

Conclusion:

The final project is an opportunity for you to showcase your understanding of ***Bitcoin*** and its impact on the world. The essay should demonstrate your ability to analyze and synthesize information and present it in a clear and concise manner. Good luck with your final project!

Additional Resources

Additional Resources

Why use bitcoin?

• **Hard Money Film** (30 minutes):
This film explores the history of money and how bitcoin fits into the current financial system. It delves into the issues with traditional fiat currencies and how bitcoin offers a solution.

• **"Why Bitcoin" by Wiz**:
This article provides an overview of the benefits of using bitcoin as a currency and store of value. It highlights the decentralized nature of bitcoin and how it allows for greater financial freedom and security.

• **"The Bullish Case for Bitcoin" by Vijay Boyapati**:
This article makes the case for why bitcoin is a valuable asset and why it has the potential to become a dominant global currency. The author covers the technical and economic aspects of bitcoin that make it a strong investment opportunity.

• **"Why Bitcoin Matters" by Aleks Svetski** (1 hour): This video covers the importance of bitcoin as a decentralized digital asset and how it can impact the current financial system. The speaker explores the potential for bitcoin to bring financial freedom to people around the world.

What is Bitcoin?

• **"What Is Bitcoin" by Greg Walker**:
This article provides a comprehensive explanation of what bitcoin is, including its history, technology, and how it differs from traditional currencies.

• **"Bitcoin - The Genesis" by RT** (30 minutes):
This video covers the creation and early days of bitcoin. It explores the motivations of the mysterious creator, Satoshi Nakamoto, and how the concept of bitcoin evolved.

• **"Understanding Bitcoin" by BJ Dweck** (1 hour 30 minutes):
This video provides a detailed explanation of the technical aspects of bitcoin and how it works. The speaker covers topics such as the blockchain, mining, and the decentralized nature of bitcoin.

Further Learning

• **The Bitcoin Standard** (1 hour 40 minutes):
This audiobook explores the economic and historical context that led to the creation of bitcoin. It covers the benefits of a decentralized currency and the potential for bitcoin to become a global standard.

• **"Intro to Bitcoin Austrian Thought"** (1 hour):
This audio lecture covers the Austrian School of economics and how it relates to the concept of bitcoin. It provides an in-depth look at the economic principles behind bitcoin and how it aligns with Austrian thought.

Important Authors

Alex Gladstein	Check Your Financial Privilege
Alex Swan	Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications
Amanda Cavaleri	Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide
Anita Posch	Learn Bitcoin: Become Financially Sovereign
Eric Yakes	The 7th Property: Bitcoin and the Monetary Revolution
Jeff Booth	The Price of Tomorrow: Why Deflation is the Key to an Abundant Future
Jimmy Song	The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future
Nik Bhatia	Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies
Robert Breedlove	Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money

Other Resources

1. Bitcoin.org: This is the official website of the Bitcoin project and provides a wealth of information about Bitcoin, including how it works, how to get started, and how to use it.

2. Bitcoin Wiki: This is a community-driven resource that provides a comprehensive guide to everything related to Bitcoin. It covers everything from the technical aspects of Bitcoin to its history and use cases.

3. Bitcoin Magazine: This is an online publication that covers news and insights related to Bitcoin and other cryptocurrencies. It provides a great way to stay up-to-date with the latest developments in the Bitcoin ecosystem.

4. Coindesk: Coindesk is a popular news and information site that covers the latest developments in the cryptocurrency industry, including Bitcoin.

5. Bitcointalk: Bitcointalk is a forum where users can discuss Bitcoin-related topics, ask questions, and share information. It's a great place to learn from other Bitcoin enthusiasts and experts.

6. Blockchain.info: This is a popular blockchain explorer that allows users to view and explore the Bitcoin blockchain in real-time. It provides a wealth of information about individual transactions, blocks, and addresses.

7. Bitcoin Core: This is the original Bitcoin software and is still widely used by many users and developers. It provides a powerful set of tools for interacting with the Bitcoin network and building Bitcoin applications.

8. Electrum: Electrum is a popular Bitcoin wallet that provides a simple and secure way to store and manage Bitcoin. It's also highly customizable and provides a wide range of features for advanced users.

Dalia Platt **- Curriculum & Content Creator**
dplatt@miprimerbitcoin.io
@dalia_platt

Glossary

Glossary

51% Attack: A type of attack on a blockchain network in which a single entity or group controls a majority of the network's computing power, allowing them to manipulate transactions and potentially disrupt the network.

Address Reuse: The practice of using the same Bitcoin address for multiple transactions.

Altcoin Season: A period of time when alternative cryptocurrencies experience significant price increases, often due to increased investor interest and adoption.

Altcoins: Digital currencies excluding Bitcoin.

Atomic Swap: A peer-to-peer exchange of one cryptocurrency for another without the need for a centralized exchange or intermediary.

Auction: A process by which goods or assets are sold to the highest bidder.

Bartering: The exchange of goods and services without the use of money.

Basket of Goods: A collection of goods or services used to measure changes in the cost of living.

Bitcoin: A digital currency/system that allows people to send money to each other without using a bank.

Block Explorer: A tool used to view and explore the blockchain, allowing users to view individual blocks, transactions, and wallet addresses.

Block Reward: The amount of new bitcoins that are awarded to miners for adding a new block to the blockchain.

Blockchain: A public record of all Bitcoin transactions that have taken place.

BTC: The unit used for bitcoin. A digital currency that can be used to make purchases or be traded.

Capital Controls: Restrictions on the movement of money across borders.

Central Bank (Fed): A government-owned institution that manages a country's monetary policy.

Centralization: The concentration of power or control in a single entity.

Centralized System: A system in which power or control is concentrated in a single entity.

Cold storage: A method of storing bitcoins offline, away from the risk of hackers or other online threats.

Commodity money: Objects that have value in and of themselves and are used as a medium of exchange, such as gold or silver.

Confirmation: The process of a transaction being processed by the network and highly unlikely to be reversed. The method "miners" verify the authenticity of transactions with their computer hardware and software. It is recommended to wait for at least 6 confirmations to prevent double spending.

Consensus mechanism: A method used in blockchain technology to validate transactions and ensure the integrity of the blockchain.

Cryptocurrency Exchange: A platform where users can buy, sell, and trade cryptocurrencies for other assets such as fiat currency or other cryptocurrencies.

Cryptocurrency wallet: A software program that stores private keys and allows users to send, receive, and manage their cryptocurrency.

Cryptography: A branch of mathematics that helps create secure systems.

Debasement: The reduction in the value of a currency, often by reducing the amount of precious metal in a coin.

Debt: Money that is owed to someone else.

Decentralization: The distribution of power and control across a network, rather than having a central authority.

Decentralized Autonomous Organization (DAO): An organization or network governed by smart contracts and run on a blockchain, without a central authority or management structure.

Decentralized Finance (DeFi): A movement within the cryptocurrency industry to create decentralized financial products and services that operate on a blockchain.

Decentralized System: A system in which power or control is distributed among multiple entities.

Glossary

Digital Asset: A digital representation of value that can be traded or used as a store of value, such as Bitcoin.

Distributed Ledger: A database that is spread across a network of computers, rather than being stored in a central location.

Double coincidence of wants: The phenomenon where two parties in a barter economy both have what the other party wants and wants what the other party has.

Double Spend: When a person tries to spend their bitcoin to two different recipients at the same time.

Dust Transaction: A transaction that sends a very small amount of Bitcoin that is too small to be economically viable.

Exchange Rate: The value of one currency in relation to another.

FOMO: Fear of missing out, a term used to describe the feeling of anxiety or regret that one may miss out on a profitable opportunity in the cryptocurrency market.

FUD: Fear, uncertainty, and doubt, a term used to describe negative rumors or information that can cause market panic or decline.

GDP: Gross domestic product, the total value of goods and services produced in a country in a given period of time.

Hard Fork: A change to the Bitcoin protocol that creates a new version of the blockchain, which is not compatible with the previous version. (ie. Bitcoin Cash)

Hardware Wallet: A physical device used for storing private keys and managing cryptocurrency, providing enhanced security over software wallets.

Hash Function: A mathematical function that takes input data of any size and outputs a fixed-size string of characters, commonly used in cryptography and blockchain technology.

Hash Rate: A way to measure the processing power of the Bitcoin network.

HODL: A term used in the cryptocurrency community to describe holding onto cryptocurrency long-term, rather than selling or trading it.

Hot Wallet: A Bitcoin wallet that is connected to the internet, allowing for easy access to bitcoins.

Imports: Goods and services produced in another country and sold in the domestic market.

Inflation: An increase in the general price level of goods and services in an economy.

Initial Coin Offering (ICO): A fundraising method in which a new cryptocurrency is sold to investors in exchange for a more established cryptocurrency, such as Bitcoin.

Layer-1 Protocol: The underlying layer of a blockchain network that handles the fundamental aspects of consensus, transaction validation, and data storage.

Layer-2 Protocol: A secondary layer built on top of a layer-1 blockchain network, often used to enhance scalability, speed, and functionality.

Ledger: A record of financial transactions.

Lightning Network: A layer-2 payment protocol that enables faster and cheaper Bitcoin transactions by using off-chain channels for smaller transactions.

Lightweight Node: A Bitcoin client that only stores a limited amount of data from the blockchain, rather than the full chain.

Mediums of exchange: Objects or systems that are widely accepted in exchange for goods and services.

Merkle Tree: A tree-like data structure used in the Bitcoin blockchain to efficiently verify the integrity of large sets of data.

Mining Pool: A group of miners who work together to increase their chances of finding new blocks and earning bitcoin.

Mining: The process of using computer hardware to do mathematical calculations for the Bitcoin network to confirm transactions and increase security.

Monetary and Fiscal Policy: The policies of a central bank and government, respectively, that influence the money supply and interest rates in an economy.

Money supply: The total amount of money in circulation in an economy.

Multi-Signature (Multisig) Wallet: A wallet that requires multiple signatures or approvals before a transaction can be executed, providing additional security and control.

Multi-Signature: A security feature that requires more than one private key to authorize a Bitcoin transaction.

Network: A group of interconnected entities.

Node Network: A network of connected computers or devices that support and maintain the Bitcoin network.

Node: A computer or device that is connected to the Bitcoin network and participates in the verification and transmission of transactions.

Non-Fungible Token (NFT): A type of digital asset that represents a unique or one-of-a-kind item, often used to represent art, collectibles, or other unique objects.

Nonce: A random number that is added to a block header to create a hash that meets the difficulty target.

Orphan Block: A block that is not included in the main chain of the blockchain due to being invalidated by a longer competing chain.

Paper Wallet: A printed copy of a user's private and public keys used for storing and managing cryptocurrency offline.

Peer-to-Peer (P2P): A decentralized network in which participants interact directly with each other, rather than through a central authority.

Peg: A fixed exchange rate between two currencies, where one is pegged to the value of another.

Private Blockchain: A blockchain that is controlled by a single organization, rather than being decentralized.

Private Key: A secret piece of data that proves a person's right to spend bitcoin from a specific wallet through a cryptographic signature.

Proof of Stake (PoS): A consensus mechanism used in some blockchain networks that requires users to hold a certain amount of cryptocurrency to participate in the validation of transactions.

Proof of Work: A consensus mechanism that requires users to perform a certain amount of computational work in order to participate in the network.

Public Blockchain: A blockchain that is open to anyone to participate in and verify transactions, making it decentralized.

Public Key: A unique identifier used for receiving bitcoin, derived from a user's private key through a mathematical process.

Public Key / Bitcoin Address: A public password/number used to receive bitcoins.

Public Ledger: A decentralized database that keeps a public record of all transactions on the Bitcoin network.
Purchasing Power: The ability of money to buy goods and services.

Recovery Phrase / Seed Keyword: a series of 12, 18, or 24 words that can be used to generate multiple pairs of private and public keys. These can be used to restore a Bitcoin wallet.

Reserve Ratio: The proportion of deposits that a bank must hold as reserves.

Restrictive banking: Restrictions or limitations on banking services or access to banking services.

Satoshi Nakamoto: The pseudonym used by the anonymous creator(s) of Bitcoin.

Satoshi: the smallest unit of Bitcoin, equal to 1/100,000,000 of a bitcoin. It is named after the creator of Bitcoin, Satoshi Nakamoto.

Satoshis per byte (sat/b): A unit used to measure the amount of bitcoin transaction fee paid per byte of transaction data.

SegWit (Segregated Witness): A Bitcoin protocol upgrade that changes the way data is stored on the blockchain, allowing for increased capacity and lower transaction fees.

Sidechain: A blockchain that is connected to another blockchain, allowing for the transfer of assets or information between the two chains.

Signature: A mathematical mechanism that allows someone to prove ownership

Smart Contract: A self-executing contract with the terms of the agreement written into code.

Glossary

Soft Fork: A change to the Bitcoin protocol that is backward-compatible with older versions of the software.

Stablecoin: A type of cryptocurrency designed to maintain a stable value, often by being pegged to a fiat currency or other asset.

Supply and Demand: The economic principle that the price of a good or service is determined by the interaction of the quantity of the good or service that is supplied and the quantity that is demanded.

Time Value of Money: The principle that money is worth more in the present than in the future.

Token: A unit of value created on a blockchain, often used to represent a specific asset or utility within a particular ecosystem.

Tokenization: The process of creating a digital representation of an asset or asset class on a blockchain, allowing for fractional ownership and transferability.

Trading Pair: A set of two currencies or assets that can be traded against each other on a cryptocurrency exchange.

Transaction Fee: A small amount of bitcoin paid by the sender of a transaction to incentivize miners to include the transaction in a block and add it to the blockchain.

Transaction ID: a string of numbers and letters that shows the details of a bitcoin transfer (such as the amount sent, the addresses of the sender and recipient, and the date of the transfer) on the Bitcoin blockchain.

Transaction: The transfer of bitcoin from one address to another on the Bitcoin network.

Trustless: A system or transaction that does not require trust in any third party or intermediary, instead relying on the security and transparency of the underlying technology.

Two-Factor Authentication (2FA): A security measure that requires two methods of authentication, typically a password and a separate code or device, to access an account or complete a transaction.

Unbanked: Individuals or communities without access to traditional banking services.

Unit of Account: A standard unit of measurement used to express the value of goods and services.

Volatility: The degree of variation in the price of an asset over time.

Wallet Address: A unique identifier used to send and receive bitcoin on the Bitcoin network, typically represented as a string of letters and numbers.

Wallet Backup: A copy of the private keys and recovery phrase/seed keywords of a Bitcoin wallet, which can be used to restore access to the wallet in case the original is lost or stolen.

Wallet: A virtual container for bitcoin similar to a physical wallet, that contains private key(s) that allow you to spend the bitcoin allocated to it in the blockchain.

Whale: An individual or organization that holds a significant amount of cryptocurrency, capable of influencing market prices through large trades.

White Hat Hacker: An ethical hacker who uses their skills to identify and fix vulnerabilities in computer systems and networks.

Whitepaper: a report that explains the problem and solution that a blockchain project or cryptocurrency is trying to address.

XBT and BTC: abbreviations for bitcoin.

Why is it important to learn about Bitcoin?

*1. What is **Bitcoin** and how does it work?*

Bitcoin is a decentralized digital currency that operates independently of a central bank. It allows for peer-to-peer transactions without the need for intermediaries, making it a revolutionary technology in the financial industry. Understanding how it works is crucial to comprehend its potential implications and usage.

*2. What makes **bitcoin** unique and valuable?*

Bitcoin is unique because it operates on a decentralized network, making it resistant to government interference and manipulation. It also has a finite supply, capped at 21 million, making it scarce and valuable, much like gold. Learning about these qualities helps to understand its potential as a store of value and investment.

*3. What impact can **Bitcoin** have on the financial industry?*

The widespread adoption of ***Bitcoin*** has the potential to disrupt traditional financial systems and challenge the monopoly of central banks. It also provides new opportunities for investment and financial inclusion, particularly for individuals in countries with unstable currencies. Understanding the potential impact of Bitcoin on the financial industry is crucial for anyone interested in finance and technology.

Mi Primer Bitcoin
EL SALVADOR