Primul Meu Bitcoin

Diploma Bitcoin

Educație financiară pentru era Bitcoin

Caietul elevului

Limba Română | 2025

My First Bitcoin a creat această lucrare și a făcut-o disponibilă gratuit sub Creative Commons.

Această lucrare este licențiată sub

Creative Commons

Attribution-ShareAlike

4.0 International (CC BY-SA 4.0)

Diploma Bitcoin

Educație financiară pentru era Bitcoin

Caietul elevului

Română | 2025

My First Bitcoin
EL SALVADOR

DONATE NOW

bc1q5es60qpa7gpkp0k32xl4zefkj43kd9zjkzd54sgmv3yzr34dw8dqm9pzsd

Povestea Diplomei Bitcoin

Nu există ceva mai puternic decât o idee al cărei timp a sosit.

Povestea Diplomei Bitcoin a început în El Salvador, cu primul program pilot de 38 de elevi din școli publice care au absolvit în iunie 2022.

E greu de crezut că a trecut doar un an și jumătate.

Creșterea din 2023 a fost fenomenală, cu mii de elevi din toată țara care au absolvit Diploma Bitcoin. În septembrie, la doar 15 luni după acea primă absolvire, a început un program pilot mult mai mare. Ministerul Educației din El Salvador a creat propria Diplomă Bitcoin folosind caietul nostru ca material principal. Împreună cu Bitcoin Beach, profesorii noștri au predat Diploma Bitcoin la 150 de profesori din școli publice. Acești profesori s-au întors la școlile lor și au predat elevilor proprii. Anul acesta, planificăm să începem prin a ajuta la formarea a încă 700 de profesori din școli publice din toată țara, iar speranța este să aducem educație bitcoin de calitate în fiecare școală din El Salvador în doi ani.

Unul dintre obiectivele noastre inițiale a fost să educăm o națiune și să demonstrăm educația Bitcoin ca un instrument benefic la scară largă. Acest vis este acum pe cale să devină realitate.

El Salvador este focusul; misiunea este lumea.

Am facut open-source caietul, precum și o varietate de alte materiale educaționale, și am fost impresionați de interesul internațional. 2022 a fost prima dată când o Diplomă Bitcoin a fost predată vreodată într-un sistem de școli publice oriunde în lume. În 2023, acest lucru a explodat. Tradusă în 12 limbi, a fost predată deja în Guatemala, Honduras, SUA, Canada, Cuba, Republica Dominicană, Coreea de Sud, Costa Rica, Brazilia, Uruguay, Argentina, India, Italia, Mexic, Africa de Sud, Zambia, Kenya, Portugalia, Marea Britanie și Hong Kong. Și, așa cum creșterea din 2023 a depășit cu mult anul precedent, ne așteptăm ca 2024 să fie la fel.

Aceasta este o mișcare globală, descentralizată.

Educația bitcoin independentă, imparțială, condusă de comunitate va schimba lumea. Deja a făcut-o.

Pentru o lume mai bună,

Echipa My First Bitcoin - 2025

Table of Contents

Chapter #1: Why Do We Need Money?

1.0 Introducere 01

1.1 Întâlnește-l pe Satoshi 02

Activitate: Cinci întrebări despre bani 03

1.2 Discuție în clasă: De ce avem nevoie de bani? 04

Chapter #2: What is Money?

2.0 Introducere 07

Activitate: Discuție în clasă - „Ce sunt banii?” 07

2.1 Definiția banilor 07

2.2 Funcția banilor 07

2.3 Proprietățile banilor 10

2.4 Tipuri de bani 13

2.5 Psihologia banilor: raritate, preferință de timp și compromisuri 14

Activitate: Preferință de timp 16

Chapter #3: The History of Money

3.0 Introduction 21

Activity: Barter Game 21

3.1 Evolution from Barter to Moder 23

3.1.1 Problems with Early Forms of Money 23

3.1.2 Development of Coinage and Paper Money 24

3.1.3 Transition from Sound to Unsound Money 25

3.1.4 Paper to Plastic 27

3.2 Digital Currency 31

Chapter #4: What is Fiat Money and Who Controls it?

4.0 Introduction 31

4.1 Brief History of Fiat Money 31

4.2 The Fiat System 34

4.2.1 A Monetary System by Decree 34

4.2.2 Fractional Reserve Banking: A System Fueled by Debt 35
Activity: Fractional Reserve Banking 38
4.2.3 Who Controls the Fiat System and How Do They Benefit? 39
4.3 Central Bank Digital Currencies: The Future of Fiat Money 41

Chapter #5: How Problems Lead to Solutions

5.0 Introduction to the Problem 45
5.1 Decreasing Purchasing Power 45
5.1.1 Monetary Inflation and Its Effect on Purchasing Power 45
Activity: The Effects of Inflation: An Auction Activity 46
5.2 The Global Debt Burden and Social Inequality 47
5.2.1 Impact on the individual - Loss of Purchasing Power 47
5.2.2 Impact on Society - Increasing Wealth Inequality 52
Activity: Consequences of the Fiat System 53
5.2.3 The Global Debt Burden 55
5.3 The Cypherpunks and the Quest for a Decentralized Currency 55
5.3.1 The Cypherpunks 56
5.3.2 Centralized vs Decentralized Systems 57
5.3.3 Brief History of Digital Currencies 59

Chapter #6: An Introduction to Bitcoin

6.0 Satoshi Nakamoto and the Creation of Bitcoin 63
6.1 How Does Bitcoin Work? 65
6.1.1 The Nakamoto Consensus Mechanism 65
6.1.2 The Players of the Game 67
Activity: Consensus Building in a Peer-to-Peer Network 69
6.2 Bitcoin as Sound Digital Money 71
6.2.1 Introduction 71
6.2.2 Bitcoin’s Features 72
Activity: Class discussion - Is Bitcoin Sound Money? 76
6.2.3 Embracing Personal Responsibility 76

Chapter #7: How to Use Bitcoin

7.0 Introduction 81

7.1 Acquiring and Exchanging Bitcoin 81

7.1.1 P2P: Physical 81

7.1.2 P2P: Online 82

7.1.3 Centralized Exchanges 82

7.2 An Introduction to Bitcoin Wallets 83

7.2.1 Self-Custodial vs Custodial Wallets 83

7.2.2 Different Types of Bitcoin Wallets 85

7.3.3 Open Source vs Closed Source 86

Activity: Class Evaluation of Bitcoin Wallets 87

7.3 Setting Up a Mobile Bitcoin Wallet 87

Activity: Setting Up/Recovering a Bitcoin Wallet 87

7.4 Receiving and Sending Transactions 89

Activity: Bitcoin Transactions in Action 91

7.5 Saving in Bitcoin 93

7.6 DYOR - Don’t Trust, Verify 94

Chapter #8: Lightning Network: Using bitcoin in your daily life

8.0 Introduction 97

Activity: Watch “Bitcoin Lightning Network Explaine 98

8.1 The Lightning Network 98

8.2 Different Types of Lightning Wallets 100

8.2.1 Self-Custodial vs Custodial Wallets 100

8.2.2 Open Source vs Closed Source 100

8.3 Setting Up a Bitcoin Lightning Wallet 100

8.4 Sending and Receiving Lightning Transaction 102

Activity: Lightning Wallet Relay Race 106

8.5 Buying Coffee and Groceries with Bitcoin 107

8.5.1 Online: Payment Plugins - Ecommerce 108

8.5.2 In Person: Find a Merchant In Your Area 109

8.5.3 Transitional Tools: Gift Cards and Payment Cards 110

8.5.4 Circular Economies and Bitcoin as a Medium of Exchange 110

Chapter #9: An Introduction to the Technical Side of Bitcoin

9.0 Introduction 115

Activity: Watch “How Bitcoin Works Under the Hood” 115

9.1 Public and Private Keys: Security through Cryptography 116

9.1.1 Cryptography Public/Private Keys 116

9.1.2 Hashing Explanation 119

Activity: Generate SHA 256 Hash 121

9.2 The UTXO Model 122

9.3 A Closer Look at Bitcoin Nodes and Miners 125

9.3.1 What is a Bitcoin Node and How Do I Set One Up? 125

Activity: Watch Video on Bitcoin Nodes 126

9.3.2 What is a Bitcoin Miner and How Does Mining Work? 126

9.4 What is the Mempool? 132

Activity: Mempool 134

9.5 How Bitcoin Transactions Work from Start to Finish 135

Chapter #10: Why Bitcoin?

10.0 Introduction 139

Activity: What Could a Bitcoin Future Look Like? 139

10.1 What are Central Bank Digital Currencies (CBDCs) and Who Controls Them? 140

10.2 The Philosophy of Bitcoin 141

Activity: Class Discussion: Do You Have the Right to Control Your Own Money? 141

10.3 The Benefits of Bitcoin 142

10.4 An Empowered Future 143

Activity: Class Discussion: How Did Your Perspective Change? 143

Additional Resources 147

Chapter Key Concepts 149

Glossary 153

Diploma Bitcoin

O călătorie de zece săptămâni
prin educație independentă,
imparțială,
de calitate și gratuită

It is essential to have a firm grasp of the basics of money, its history, and the current financial system before studying Bitcoin. Understanding these concepts provides a strong foundation for comprehending Bitcoin's unique and disruptive nature. 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 Bitcoin's significance and potential impact. 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.

Capitolul #1

De ce avem nevoie de bani?s

1.0 Introducere

1.1 Întâlnește-l pe Satoshi

Activitate: Cinci întrebări despre bani

1.2 Discuție în clasă: De ce avem nevoie de bani?

Caietul elevului

Limba Română | 2025

De ce avem nevoie de bani?

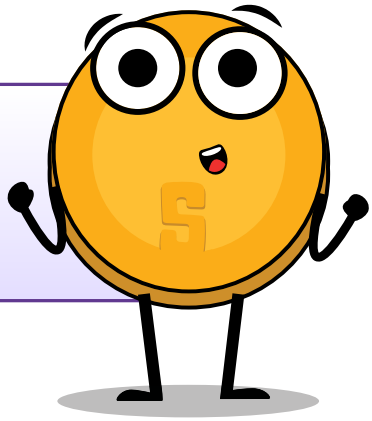
1.0 Introducere

> Banii sunt unul dintre cele mai mari instrumente ale libertății inventate vreodată de om.
>
> Friedrich Hayek

Bine ai venit la Diploma Bitcoin. În acest capitol, vom explora întrebarea fundamentală de ce banii sunt esențiali în viețile noastre. Vom analiza natura banilor și diferitele lor forme, cu scopul de a înțelege mai profund semnificația lor. Banii sunt ceva ce folosim aproape în fiecare zi, dar înțelegem cu adevărat de ce avem nevoie de ei și ce sunt? De ce părinții și membrii familiei noastre dau la schimb timpul lor pe bani? De ce unii oameni au mai mulți bani decât alții? De ce banii sunt diferiți în alte țări? De ce nu putem pur și simplu să creăm mai mulți bani când avem nevoie?

1.1 Întâlnește-l pe Satoshi

> ***Salut! Sunt Satoshi, un asistent interactiv care te va ajuta pe parcursul Diplomei Bitcoin. Îți voi oferi resurse și recomandări utile, astfel încât să poți aprofunda conceptele cheie.***



Activitate: Să începem capitolul răspunzând la cele cinci întrebări de mai jos:

Ia în considerare utilizări practice precum obținerea celor necesare, cum ar fi mâncarea și alte lucrurile dorite. Încearcă să fii specific în exemplele tale, echilibrând creativitatea cu realismul.

De ce avem nevoie de bani?

Ce sunt banii?

De ce avem nevoie de bani?

Cine controlează banii?

Ce oferă banilor „valoare”?

Ce întrebare ai despre bani? Scrie întrebarea ta aici pentru a o împărtăși cu clasa.

Extinde discuția la întreaga clasă, împărtășind și comparând listele pentru a determina cele mai esențiale cinci motive pentru care avem nevoie de bani. Identifică ideile comune din clasă. Reflectează asupra ideilor tale unice care nu au fost incluse pe listă, dar merită luate în considerare. Notează aceste perspective suplimentare.

1.2 Discuție în clasă: De ce avem nevoie de bani?

Clasa se va împărți în grupuri și:

- Își va împărtăși și discuta răspunsurile la primele patru întrebări. Notează răspunsurile preferate.
- Își va împărtăși răspunsurile la ultima întrebare și va vota o întrebare preferată a unui elev. Notează rezultatul.
- Clasa va reveni la răspunsurile și întrebările lor la finalul Diplomei Bitcoin

Acum că ai o înțelegere mai clară a motivului pentru care banii sunt necesari, capitolele următoare vor explora ce sunt banii, cum au evoluat de-a lungul timpului, cine îi influențează și cea mai nouă formă a lor. Continuă să consulți listele tale din prima zi de curs pentru a face legătura între ideile tale și evoluția creării, definirii și utilizării banilor de-a lungul timpului.

Capitolul #2

Ce sunt banii?

2.0 Introducere

Activitate: Discuție în clasă - „Ce sunt banii?”

2.1 Definiția banilor

2.2 Funcția banilor

2.3 Proprietățile banilor

2.4 Tipuri de bani

2.5 Psihologia banilor: raritate, preferință de timp și compromisuri

Activitate: Preferință de timp

Caietul elevului

Limba Română | 2025

Ce sunt banii?

2.0 Introducere

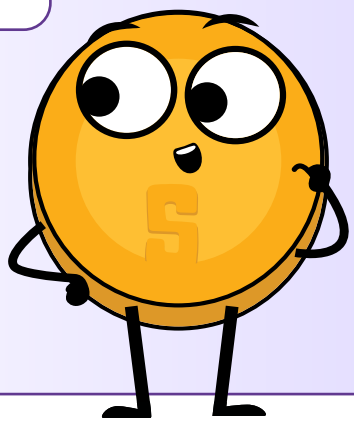
> Banii sunt o garanție că putem avea ce ne dorim în viitor. Chiar dacă nu avem nevoie de nimic acum, ei asigură posibilitatea de a satisface o nouă dorință când apare.
>
> **Aristotel**

Pornind de la explorarea necesității banilor, acest capitol abordează întrebarea esențială: Ce sunt banii? Vom începe cu o discuție și o activitate de grup.

Activitate: Discuție în clasă - „Ce sunt banii?”

- Vă rugăm să nu mâncați bomboana pusă pe biroul vostru încă.
- Cine ar fi dispus să schimbe bomboana pentru o bancnotă de 1 USD?
- Acum, țineți mâna sus dacă ați fi dispuși să schimbați bomboana pentru o bancnotă de 1 dolar Monopoly în loc de bomboana voastră.
- De ce sau de ce nu?
- Ce face ca o bancnotă să fie atât de dorită și alta să fie considerată fără valoare?
- Ce oferă banilor „valoare”?
- De unde vin banii și cine decide cât să se tipărească?
- De ce nu tipărim mai mulți bani și nu îi distribuim tuturor în mod egal?

Singura diferență dintre aceste două bancnote este convingerea ta că una are mai multă valoare decât cealaltă.



2.1 Definiția banilor

Te-ai oprit vreodată să te gândești ce sunt cu adevărat banii? Te-ai întrebat vreodată ce face ca banii să fie... bani? Majoritatea știm cum să-l folosim, dar puțini înțelegem de unde vine sau cum funcționează. Banii sunt, în esență, o modalitate de a schimba bunuri și servicii. Ei reprezintă valoarea acestor lucruri într-o formă ce poate fi ușor tranzacționată. Poate lua multe forme: bancnote, monede metalice, plăți electronice. Guvernele sau alte autorități emit și controlează de obicei banii, dar banii sunt mult mai mult decât un simplu mijloc fizic sau digital de schimb; este ca un limbaj universal care ne permite să facem schimburi cu oameni din toată lumea, chiar dacă nu vorbim aceeași limbă sau nu avem aceeași cultură. De exemplu, poți fi la capătul celălalt al lumii și tot „vorbești bani” punând un produs pe tejghea și schimbându-l pe moneda locală sau folosind un card de credit.

Capitolul #2

Primul Meu Bitcoin

Banii sunt ca un contract social care ne permite să facem schimburi fără să ne bazăm pe troc sau să găsim pe cineva care vrea exact ce avem noi de oferit. Dacă un grup de oameni ar începe să accepte ciocolata ca plată pentru majoritatea bunurilor și serviciilor, ciocolata ar deveni bani (deși, pentru că s-ar topi în unele părți ale lumii, am considera-o bani proști).

Așa cum a subliniat economistul francez Jean-Baptiste Say, „Banii îndeplinesc doar o funcție temporară într-un schimb; iar când tranzacția se încheie, se va constata întotdeauna că un tip de marfă a fost schimbat pentru altul."

Cu alte cuvinte, banii în sine nu au puterea de a satisface dorințele umane; este doar un instrument care ne permite să schimbăm o marfă pentru alta.

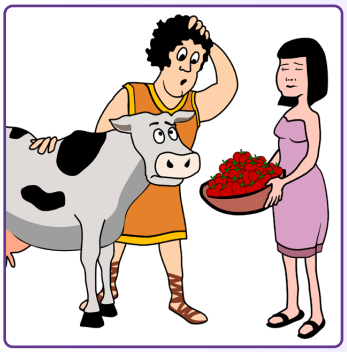
Tranzacția este un schimb sau transfer de bunuri și servicii. Este o modalitate de a schimba valoare între două sau mai multe părți.

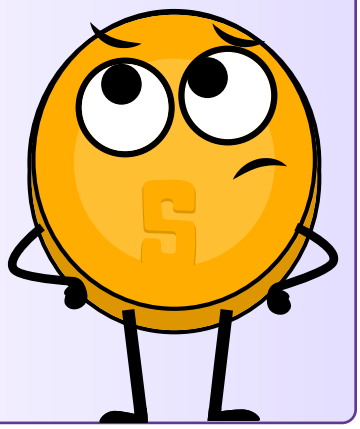
Există multe tipuri de tranzacții, de la schimburi simple (cum ar fi cumpărarea unui sandviș la o cafenea) la tranzacții financiare complexe (cum ar fi cumpărarea unei case sau investiția în acțiuni sau obligațiuni). Tranzacțiile pot fi realizate față în față, la telefon, online sau prin alte mijloace și pot implica o gamă largă de părți: persoane fizice, companii, instituții financiare.

Fără bani, cât de ușor sau fezabil ar fi acest schimb?

Ați schimba o vacă pentru 1.000.000 de căpșuni?

Sau 600.000 de căpșuni? Dar 50.000?





Uită-te la acest videoclip scurt!

Banii SUNT valoarea PRIN care bunurile sunt schimbate.
Banii NU SUNT valoarea PENTRU care bunurile sunt schimb

Pe scurt, banii:

Facilitează schimbul pentru că toată lumea îi acceptă ca plată finală. Ne permite să măsurăm valoarea și să facem comparații între diferite bunuri și servicii. În continuare, vom analiza funcția banilor.

Ce sunt banii?

2.2 Funcția banilor

Când vine vorba de cumpărarea și vânzarea bunurilor și serviciilor, banii sunt jucătorul principal. Banii îndeplinesc mai multe funcții importante în lume, precum:

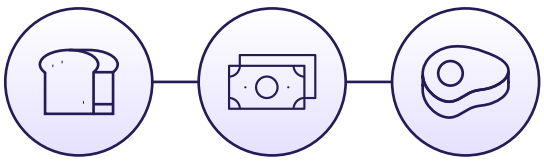
1 Depozit de valoare

Banii ar trebui să-și mențină valoarea în timp, fiind utili ca metodă de economisire și investire a valorii muncii umane. Acest lucru le permite oamenilor să folosească banii pentru a planifica viitorul și pentru a împrumuta sau a da cu împrumut bani. Deci, data viitoare când economisești pentru ceva special, amintește-ți că banii sunt mai mult decât o modalitate de a plăti – sunt un instrument care te ajută să planifici și să investești în viitorul tău.

Ce preferi ca depozit de valoare?		BTC (USD)	Gold (USD)	USD (EUR)
	14 Martie, 2019	$3,846	$1,293	€0.8817
	14 Martue, 2020	$5,258	$1,529	€0.90056
	Câștig / Pierdere	+36.71%	+18.25%	+2.14%

2 Mijloc de schimb

Cu bani, nu trebuie să găsești pe cineva care vrea exact ce ai tu de oferit. Poți folosi bani pentru a cumpăra și vinde orice dorești. Acest lucru face comerțul mult mai convenabil și eficient.



3 Unitate de cont

Banii oferă un standard universal de valoare care permite oamenilor să exprime și să compare prețul diferitelor bunuri și servicii. Acest lucru permite o piață mai eficientă și transparentă, unde oamenii pot lua decizii informate despre ce să cumpere sau să vândă.

Unitate de cont

Consumatorii recunosc valoarea unui bun atunci când i se atribuie un preț (valoare monetară).

Gândește-te așa: dacă vrei să cumperi o mașină nouă, poți compara prețurile de la diferiți dealeri și să iei o decizie informată pe baza prețului în lei/dolari/euro. Fără o unitate de cont, ar trebui să compari valoarea unei mașini cu alta folosind altceva, cum ar fi numărul de vaci sau timpul necesar pentru a construi mașina.

Aceste trei funcții permit economiilor să devină complexe și dinamice. Fără bani, ar fi mult mai greu să cumperi și să vinzi bunuri și servicii, iar economia ar fi mult mai puțin dezvoltată.

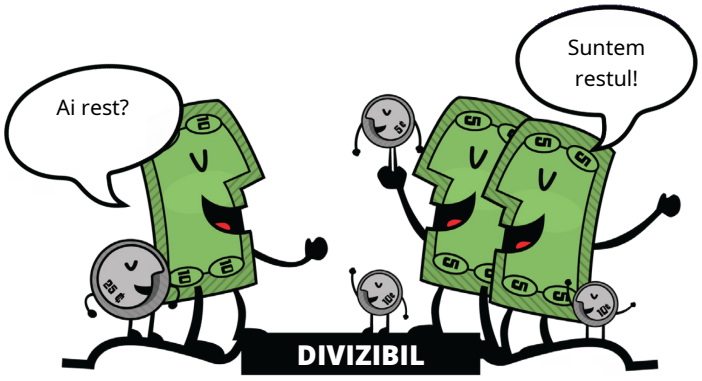
Exercițiu în clasă: Ce funcție a banilor este exemplificată aici?

- Ionuț a decis să economisească o parte din salariul săptămânal pentru a cumpăra un cățel.
- Adam cumpără două felii de pizza pentru 8,30$ la Ray's Pizza.
- Marc nu se poate decide dacă să cumpere bilete la concert pentru 75$ sau un abonament de schi pentru 95$.

2.3 Proprietățile banilor

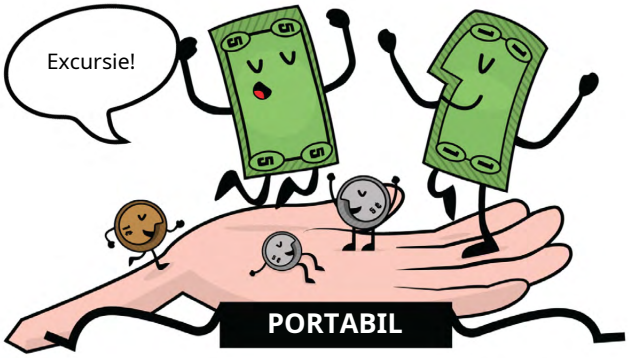
De-a lungul timpului, oamenii au realizat că banii trebuie să aibă anumite calități pentru a fi eficienți ca mijloc de schimb. Aceste caracteristici includ durabilitate, divizibilitate, portabilitate, acceptabilitate, raritate și fungibilitate.

- Durabilitate se referă la capacitatea banilor de a rezista deteriorării fizice și de a dura în timp. Astfel, banii pot circula în economie într-o stare acceptabilă și recognoscibilă. Aurul este un material durabil care rezistă uzurii, fiind o bună reprezentare a caracteristicii de durabilitate a banilor.
- Divizibilitate se referă la capacitatea banilor de a fi împărțit în unități mai mici, astfel încât oamenii să poată face achiziții de valori diferite. Bancnotele pot fi ușor împărțite în denominații mai mici, fiind o bună reprezentare a caracteristicii de divizibilitate a banilor.

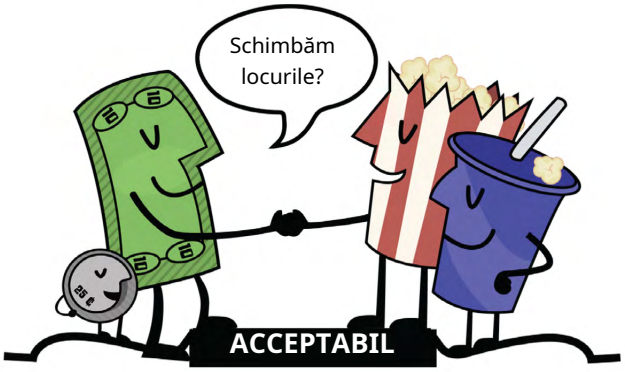


Ce sunt banii?

Portabilitate se referă la ușurința cu care banii poate fi transportați și purtați. Acest lucru permite oamenilor să folosească banii pentru a cumpăra și vinde bunuri și servicii fără dificultate. Cardurile de credit sunt portabile, deoarece pot fi ușor purtate în portofel sau geantă, fiind o bună reprezentare a portabilității banilor.

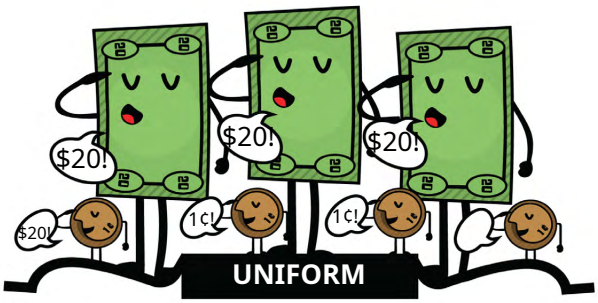


Acceptabilitate se referă la acceptarea pe scară largă a banilor ca formă de plată, astfel încât oamenii să-l poată folosi cu încredere pentru a cumpăra și vinde bunuri și servicii. Dolarul american este larg acceptat ca formă de plată, fiind o bună reprezentare a acceptabilității banilor.



Raritate se referă la oferta limitată de bani, ceea ce ajută la menținerea valorii și previne necesitatea de a cheltui mai mulți bani pentru a cumpăra aceeași cantitate de bunuri. Timbrele de colecție, mai ales cele rare și valoroase, pot fi o formă bună de bani pentru că sunt rare și pot crește în valoare în timp. Colecționarii de timbre folosesc adesea timbrele ca modalitate de a-și investi averea și de a-și diversifica portofoliul.

Fungibilitate se referă la interschimbabilitatea banilor, astfel încât o unitate de bani să fie echivalentă cu alta de aceeași valoare. Banii ar trebui să fie uniformi. Monedele de cupru sunt uniforme ca dimensiune și greutate, fiind o bună reprezentare a uniformității banilor. Un cent este întotdeauna un cent.



În ansamblu, aceste caracteristici fac banii un instrument util și eficient pentru facilitarea comerțului și sunt esențiale pentru dezvoltarea și stabilitatea economiilor.

Exercițiu în clasă

Diferite bunuri au proprietăți diferite și îndeplinesc funcțiile banilor în grade variate. Societatea decide în final ce activ este folosit ca bani pe baza unor factori precum stabilitatea, raritatea, divizibilitatea, transferabilitatea și acceptarea ca mijloc de schimb.

Pentru a determina cât de bine îndeplinesc diferite obiecte caracteristicile banilor, poți nota fiecare obiect pe o scară de la 1 la 5 pentru fiecare caracteristică. Adunând punctajele pentru fiecare obiect, poți determina care este cel mai potrivit să fie o formă de bani.

[0 = Teribil; 3 = Acceptabil; 5 = Excelent]

*** Vă rugăm să nu completați coloana pentru Bitcoin; vom reveni la ea mai târziu în curs.**

- Durabilitate: Pot banii să reziste uzurii în timp?
- Portabilitate: Pot banii fi ușor transportați și folosiți în diferite locuri?
- Fungibilitate: Sunt banii interschimbabili cu alte forme de bani?
- Acceptabilitate: Sunt banii larg acceptați ca formă de plată?
- Raritate: Sunt banii rari și nu prea abundenți?
- Divizibilitate: Pot banii fi împărțit în unități mai mici pentru tranzacții?

Caracteristică a banilor buni	Vaci	Țigări	Diamante	Euro	Bitcoin
Durabil					
Portabil					
Uniform					
Acceptabil					
Rar					
Divizibil					
Total					

Ce sunt banii?

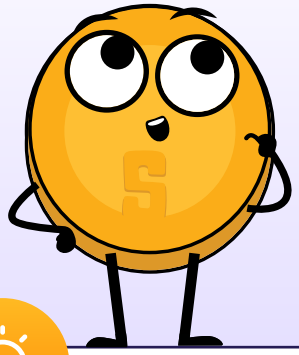
2.4 Tipuri de bani

Banii pot fi împărțiți în două categorii principale: fizic și digital.

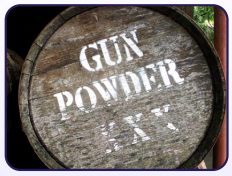
Banii fizici includ:

- Banii fiat, adică bancnotele și monedele emise de guverne și acceptate ca mijloc de schimb.
- Banii reprezentativi, care reprezintă o revendicare asupra unei mărfi fizice.
- Banii marfă, care sunt un obiect fizic cu valoare intrinsecă și este larg acceptat ca mijloc de schimb. De exemplu, aurul și argintul.

Nu toți banii sunt la fel!



Banii marfă



Obiecte precum pulberea de pușcă au fost folosite în trecut ca monedă de tip marfă.

Banii reprezentativi

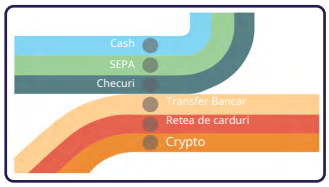
Moneda reprezentativă, precum acest certificat de argint, putea fi răscumpărată în argint.

Banii fiat

Astăzi, bancnotele Rezervei Federale sunt bani fiat desemnați de guvernul federal ca mijloc acceptat de plată a datoriilor.

Monedeledigitale, pe de altă parte, pot fi folosite pentru tranzacții online și includ monede electronice, stablecoins și criptomonede.

Monedele electronice sunt versiuni digitale ale banilor obișnuiți, ca dolarii sau euro, și pot fi folosite pentru a cumpăra și vinde online prin infrastructura de plăți digitală



Infrastructura de plăți este sistemul care permite mișcarea monedelor electronice și a altor active digitale dintr-un loc în altul. Totuși, în sistemul financiar tradițional, există mereu un intermediar, cum ar fi o bancă sau o instituție financiară, care percepe o taxă și are autoritatea de a accepta, anula, inversa sau întârzia tranzacțiile.

În sistemul financiar intermediat, principalele tipuri de infrastructură de plăți digitale includ rețelele de carduri – care facilitează transferul de fonduri între instituții financiare și comercianți când un client face o achiziție cu un card de debit sau credit – și portofelele digitale, care sunt conturi online ce permit utilizatorilor să stocheze și să gestioneze monedele electronice și să facă plăți transferând fonduri din contul lor în contul destinatarului.

Monedele digitale ale băncilor centrale (CBDC):

Sunt versiuni digitale ale monedei fiat a unei țări, emise și garantate de banca centrală și intermediată de guvern.

Stablecoins

Sunt monede digitale concepute să mențină o valoare stabilă față de un activ, cum ar fi dolarul american.

Criptomonedele

Sunt un tip de monedă digitală. Unele criptomonede sunt descentralizate și guvernate de reguli, altele sunt centralizate și controlate de un grup restrâns de persoane.

În final, o monedă care funcționează fără intermediari este mai eficientă și benefică pentru societate, deoarece împiedică câțiva indivizi să controleze oferta de bani și să concentreze puterea. Totuși, crearea unei astfel de monede care să faciliteze tranzacții sigure fără a se baza pe încredere între părți a fost o provocare de-a lungul istoriei. Pentru a realiza acest lucru, trebuie creată o monedă care să funcționeze ca internetul, unde controlul este distribuit între toți și nimeni în același timp. Acest lucru necesită acordul tuturor părților, inclusiv al celor care dețin puterea, de a renunța la control pentru binele comun.

2.5 Psihologia banilor: raritate, preferință de timp și compromisuri

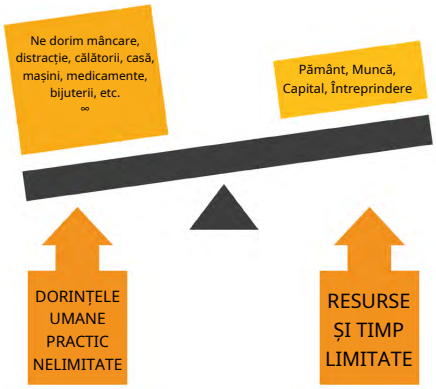
Imaginează-ți că ești blocat în deșert și ai doar o sticlă de apă rămasă. Ești însetat și disperat după o gură de apă, dar știi că vei avea nevoie de apă ca să supraviețuiești până găsești mai multă. Acesta este un exemplu clasic de raritate – ai doar o cantitate limitată dintr-o resursă (apă) și trebuie să alegi cum să o folosești. În această situație, ai putea decide să o raționalizezi și să iei înghițituri mici pe o perioadă mai lungă pentru a o face să dureze cât mai mult.

Ce sunt banii?

Raritatea ne obligă să cântărim avantajele și dezavantajele modului în care folosim resursele și să facem compromisuri.

Alternativ, ai putea decide să bei cât poți dintr-o dată, sperând că valul de hidratare îți va da energia necesară să găsești mai multă apă. Indiferent de alegere, te confrunți cu o decizie dificilă. În acest caz, alegerea este între a-ți potoli setea imediată și a conserva apa pentru mai târziu. Acest concept de raritate se aplică tuturor tipurilor de resurse, nu doar apei. Fie că e vorba de bani, timp sau chiar dragoste și atenție, suntem mereu puși în fața alegerii modului în care să alocăm resursele limitate.

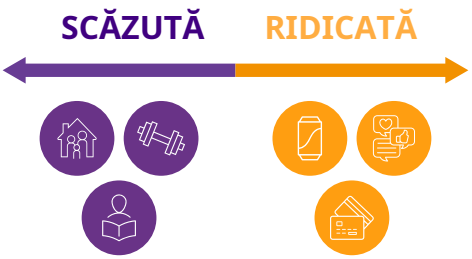
Există două tipuri de raritate: creată de om și naturală.



- Raritatea creată de om, cunoscută și ca raritate centralizată, include lucruri precum genți de designer ediție limitată, carduri sportive rare și opere de artă rare. Acestea pot fi ușor replicate sau contrafăcute.
- Raritatea naturală, cunoscută și ca raritate descentralizată, include lucruri precum sarea, scoicile și metalele prețioase ca aurul. Acestea sunt mai greu de replicat sau contrafăcut. Diferența principală este controlul.

Raritatea centralizată este controlată de o singură entitate, ca o companie sau guvern, în timp ce raritatea descentralizată nu este controlată de nimeni. Un exemplu de raritate centralizată care afectează disproporționat persoanele sărace este controlul resurselor esențiale precum apa potabilă. În unele regiuni, accesul la apă potabilă este gestionat de companii private sau entități guvernamentale care pot limita distribuția, ducând la raritatea acestei resurse vitale. Acest control centralizat poate duce la creșterea prețurilor sau acces inegal la apă, iar comunitățile sărace suportă adesea consecințele. Accesul limitat la apă nu afectează doar sănătatea și bunăstarea lor, ci perpetuează sărăcia, deoarece pot fi nevoiți să plătească prețuri mai mari sau să călătorească distanțe mari pentru a obține apă.
Raritatea ne influențează alegerile. Înțelegerea ei ne poate îmbunătăți procesul decizional. Adesea trebuie să alegem între câștiguri imediate și beneficii pe termen lung, iar aceste compromisuri ne modelează drumul spre atingerea scopurilor.

Preferința de timp se referă la ideea că oamenii preferă să aibă ceva ACUM decât mai târziu.



Un exemplu de preferință de timp:

Să zicem că ai opțiunea să primești 100$ azi sau 110$ peste un an. Dacă ai o preferință de timp ridicată, ai putea alege să primești 100$ azi pentru că apreciezi mai mult beneficiul imediat decât cel de a aștepta un an pentru încă 10$. Pe de altă parte, dacă ai o preferință de timp scăzută, vei prefera să aștepți recompensa mai mare pentru că ești mai orientat spre planificare pe termen lung și mai puțin preocupat de satisfacția imediată.

Activitate: Preferință de timp

Preferință de timp ridicată vs preferință de timp scăzută

1. Ascultă explicația profesorului despre alegerea bomboanei.
2. Decide dacă vrei să primești o bomboană mică sau o bezea acum sau să aștepți până la finalul orei pentru a primi două bomboane sau o bomboană mai mare.
3. Angajează-te în decizie și anunță profesorul. Primește bomboana fie imediat, fie la finalul orei, în funcție de alegerea ta.
4. Participă la discuția de clasă despre activitate, reflectând asupra procesului decizional și conceptului de preferință de timp.

Concluzie și discuție:

- Ce factori ți-au influențat decizia de a lua bomboana acum sau de a aștepta o recompensă mai mare mai târziu?
- Cum te simți acum că activitatea s-a încheiat?
- Poți da exemple reale unde preferința de timp ridicată poate fi dăunătoare și unde preferința de timp scăzută poate fi benefică?
- Care sunt posibilele consecințe ale alegerii preferinței de timp ridicate în locul celei scăzute?

În contextul exemplului din deșert, asta înseamnă că ai putea fi mai tentat să bei toată apa imediat, chiar dacă asta înseamnă că nu vei mai avea pentru mai târziu. Asta pentru că setea pe care o simți acum este mai presantă decât cea pe care ai putea să o simți în viitor.

Pe de altă parte, dacă alegi să raționalizezi apa și să o bei încet în timp, demonstrezi o preferință de timp mai scăzută. Asta înseamnă că ești dispus să aștepți pentru a-ți satisface setea și să-ți îmbunătățești șansele de supraviețuire. Conceptul de cost de oportunitate este strâns legat de ideea de raritate și preferință de timp.

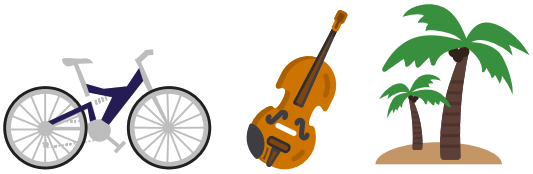
Ce sunt banii?

Costul de oportunitate se referă la valoarea celei mai bune alternative la care renunți când iei o decizie. Fiecare decizie implică compromisuri.

Alegeri Azi | ACUM | MAI TÂRZIU

Cumpăra un smoothie de 7$

Cheltie $7 în alt fel



Beneficii din a economisi regulat $7

În exemplul din deșert, costul de oportunitate al consumului întregii ape imediat este beneficiul de supraviețuire pe care l-ai fi obținut raționalizând apa și folosind-o pe o perioadă mai lungă.

Să zicem că alegi să raționalizezi apa și să iei înghițituri mici pe o perioadă mai lungă. Astfel, ai energia și hidratarea necesară să cauți mai multă apă. Totuși, în timp ce cauți, dai peste un cactus care are puțină apă în interior. Nu e mult, dar e suficient să-ți potolești setea pentru moment. Dacă ai fi ales să bei toată apa dintr-o dată, poate nu ai fi avut energia să cauți mai multă apă și să găsești cactusul.

În acest caz, costul de oportunitate al consumului întregii ape dintr-o dată ar fi fost șansa de a găsi cactusul și de a obține mai multă hidratare.

Acest exemplu arată cum costul de oportunitate implică nu doar compromisul imediat între două opțiuni, ci și oportunitățile viitoare ce pot fi câștigate sau pierdute ca rezultat al alegerilor noastre.

Disponibilitatea de a renunța la o recompensă mai mare în viitor în schimbul uneia mai mici acum este influențată de preferința de timp, adică cât de mult apreciem satisfacția imediată versus planificarea pe termen lung.

În acest capitol, am explorat conceptul fundamental de bani, acoperind definiția, funcțiile, proprietățile și tipurile sale. Un aspect esențial al discuției a fost înțelegerea psihologiei banilor, concentrându-ne pe concepte precum raritatea, preferința de timp și compromisurile. Această explorare a pus bazele pentru înțelegerea naturii complexe a banilor și a rolului său în viața noastră. În capitolul următor, vom vorbi despre istoria banilor și cum a evoluat de-a lungul timpului.

Capitolul #3

Istoria Banilor

3.0 Introducere

Activitate: Jocul Trocului

3.1 Evoluția de la troc la moneda modernă

3.1.1 Problemele formelor timpurii de bani

3.1.2 Dezvoltarea monedelor și a banilor de hârtie

3.1.3 Tranziția de la monedă sănătoasă la monedă fără aco

3.1.4 De la hârtie la plastic

3.2 Moneda digitală

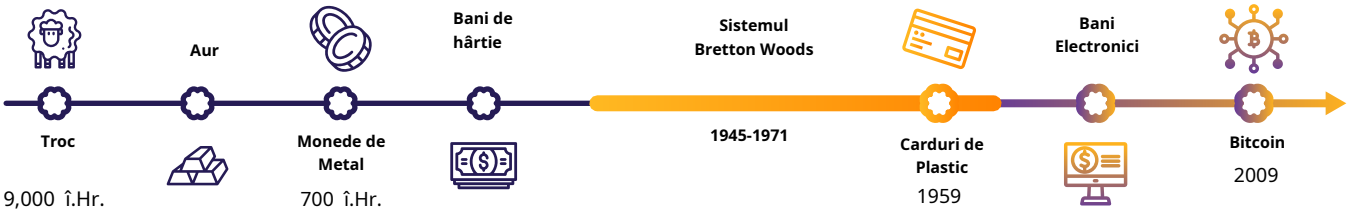
Caietul elevului

Limba Română | 2025

Istoria Banilor

3.0 Introducere

> Banii nu au evoluat prin design, ci au apărut din procesul pieței. Nu au fost creați de guverne. Au apărut în timp ca o ordine spontană.
>
> **Murray Rothbard**



Imaginează-ți o perioadă când oamenii nu aveau monedele sau bancnotele pe care le folosim astăzi. Atunci, ei aveau alte modalități de a face schimb – folosind obiecte precum scoici sau metale prețioase ca aurul, ca un fel de monedă specială. Poate sună ciudat, dar era versiunea lor de bani, ceva ce toată lumea accepta ca având valoare. În acest capitol, vom porni într-o călătorie prin timp, experimentând evoluția banilor. Vom urmări originile banilor și vom observa cum s-au schimbat și adaptat de-a lungul istoriei.

Activitate: Exercițiu în clasă - Jocul Trocului

Profesorul ți-a dat o bucată mică de hârtie. Scopul tău este să schimbi ceea ce „ai" cu ceea ce „vrei" într-un joc al comerțului de-a lungul istoriei. Scrie-ți numele în partea de sus a hârtiei, cu litere mici și lizibile.

Runda #1: Troc

Este anul 6000 î.Hr. Evident, banii așa cum îi știm nu au fost inventați. Ești în Mesopotamia și faci schimb direct de bunuri și servicii prin troc.

> Ca o notă, multe afaceri acceptă încă plăți non-monetare pentru servicii, iar guvernele tratează aceste tranzacții de troc la fel ca tranzacțiile cu bani pentru raportarea fiscală.

Taie foaia la linia punctată. Scopul tău este să schimbi „ce ai" de câte ori este nevoie până obții „ce vrei" inițial. Nu poți schimba „ce vrei" inițial. Ai cinci minute pentru a realiza acest exercițiu.

Când noul „ce ai” se potrivește cu „ce vrei” inițial, revino la locul tău. După ce timpul expiră, dacă nu ai găsit un partener de schimb, revino la locul tău oricum.

Ridică mâna dacă ai reușit să obții ce ai vrut după un schimb. Două? Trei?

Răspunde pe scurt, la următoarele întrebări.

1. De ce unii dintre voi au reușit să facă schimb și alții nu?

_____

_____

2. Care sunt beneficiile trocului?

_____

_____

3. Pe baza experienței din acest exercițiu, care sunt dezavantajele folosirii trocului?

_____

_____

Runda #2: Monedă Marfă

Avansăm în timp pe coasta de vest a Africii, undeva în jurul secolului al XIV-lea î.Hr. Trocul a devenit plictisitor și ineficient. Am evoluat ca civilizație și acum folosim monedă marfă.

Scoici Cowry în Monede _____

1,300 î.Hr.

1,000 î.Hr.

687 î.Hr.

Aceste proto-monede aveau formă ovală, erau fabricate din „electrum” (un aliaj de aur și argint) și aveau un desen doar pe o singură față.

Știați că:

Scoicile Cowry au fost acceptate ca mijloc legal de plată în unele părți ale Africii până în secolul al XX-lea.

1,300 î.Hr.

Scoicile Cowry sunt forma predominantă de plată în cea mai mare parte a Asiei, Africii, Oceaniei și în unele părți ale Europei

1,000 î.Hr.

Dinastia Zhou din China începe să folosească monede metalice.

687 î.Hr.

Regele Alyattes al Lidiei (actuala Turcia) ordonă baterea primelor monede metalice din lumea occidentală.

Istoria Banilor

Profesorul ți-a dat o macaroană (pentru simplitate). Să presupunem, prin convenție, că prețul fiecărui bun valorează o macaroană.

Scopul tău este din nou să obții ce „vrei”, dar acum, specia noastră a găsit o modalitate de a rezolva anumite probleme.

- De ce considerăm macaroana monedă marfă?
- Cum obținem lucrurile dorite acum?
- A fost runda cu macaroane mai ușoară?
- De ce crezi că banii au înlocuit mărfurile?
- În ce moduri este folosirea monedei marfă mai eficientă decât trocul?
- Care sunt dezavantajele folosirii macaroanelor ca bani?
- Ce crezi că s-a întâmplat când Spania a început să aducă bărci pline cu macaroane în comunitatea ta (aur și argint din Americi înapoi în Spania)?

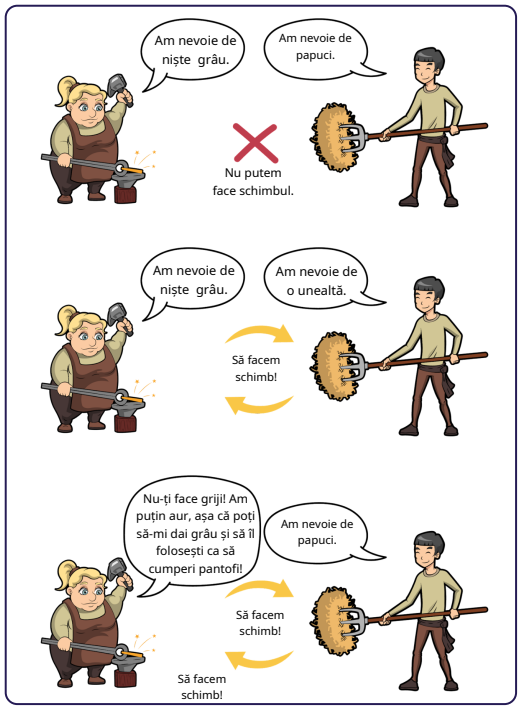
3.1 Evoluția de la troc la moneda modernă

3.1.1 Problemele formelor timpurii de bani

Urmărește acest scurt videoclip pentru a afla despre Originile Schimbului, în seria „Istoria Banilor de Hârtie.”

În economiile de troc, oamenii fac schimb pe baza valorii relative a bunurilor și serviciilor pe care le au. Economiile de troc sunt ineficiente și greu de gestionat, mai ales în societăți complexe.

Este necesară o dublă coincidență a dorințelor în orice sistem de troc, deoarece oamenii trebuie să găsească pe cineva care are ce își doresc, dar care vrea ce au ei de oferit la schimb.



Să presupunem că:

- Iosif vrea să schimbe banana lui cu nuca de cocos a lui Rareș.
- Dar Rareș vrea să schimbe nuca de cocos doar cu mango-ul lui Toma.
- Iar Toma vrea să schimbe mango-ul doar cu banana lui Iosif.
- Sunt blocați într-un ciclu nesfârșit de schimb de fructe fără dublă coincidență a dorințelor.
- Iosif sugerează să schimbe fructele pe o băutură răcoritoare, dar realizează că sunt pe o insulă izolată și nu există băuturi răcoritoare.
- Decid să stea pe plajă și să se bucure de fructe în liniște.

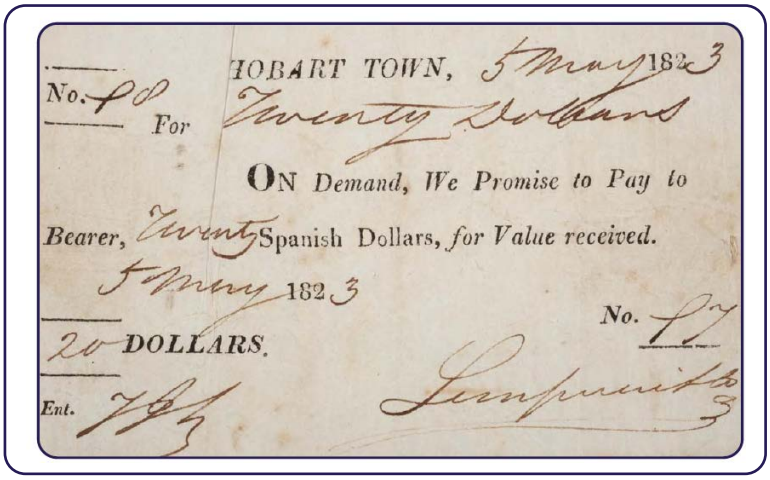
Acesta este al doilea episod intitulat „Nu doar tăiței", din seria „Istoria banilor de hârtie".

3.1.2 Dezvoltarea monedelor și a banilor de hârtie

Pe măsură ce tu și comunitatea ta deveniți mai implicați în comerț, realizați limitările trocului și ale altor forme de schimb non-monetar. Decideți să adoptați utilizarea monedelor metalice ca formă de bani.

Moneda marfă este moneda realizată din materiale metalice valoroase precum aurul și argintul. Acestea au fost folosite istoric ca rezervă de valoare, mijloc de schimb și, în trecut, ca unitate de cont.

Istoria Banilor



Totuși, pe măsură ce folosiți monedele metalice mai des, apar unele dezavantaje. Pot fi grele și incomode pentru tranzacții mari, iar unii profită de sistem topind monedele și creând altele noi din metale mai ieftine, ceea ce duce la creșterea prețurilor și subminează încrederea în sistem.

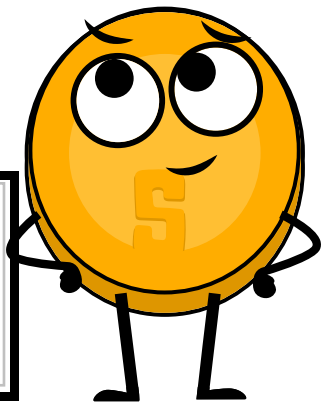
Pentru a rezolva aceste probleme, comunitatea începe să folosească chitanțe de hârtie ca formă de bani.

Aceste chitanțe, originare din China Antică, sunt o formă convenabilă și ușor de schimbat de monedă. Sunt garantate de aur și alte metale prețioase și pot fi convertite în aceste metale, așa cum s-a întâmplat între secolele XVII-XIX. Astfel, aveți o formă de bani mai portabilă și transferabilă, păstrând totodată valoarea și siguranța metalelor prețioase.

3.1.3 Tranziția de la monedă sănătoasă la monedă fără acoperire

Avansează până în secolul XVII în Suedia. Acum depinzi complet de bănci pentru a-ți depozita bunurile valoroase. Observi că bancherii emit mai multe chitanțe de hârtie decât au aur în depozit, creând mai mulți bani decât au active pentru a-i susține. Această practică le permite să profite de diferența dintre valoarea chitanțelor și valoarea aurului deținut pentru clienți.

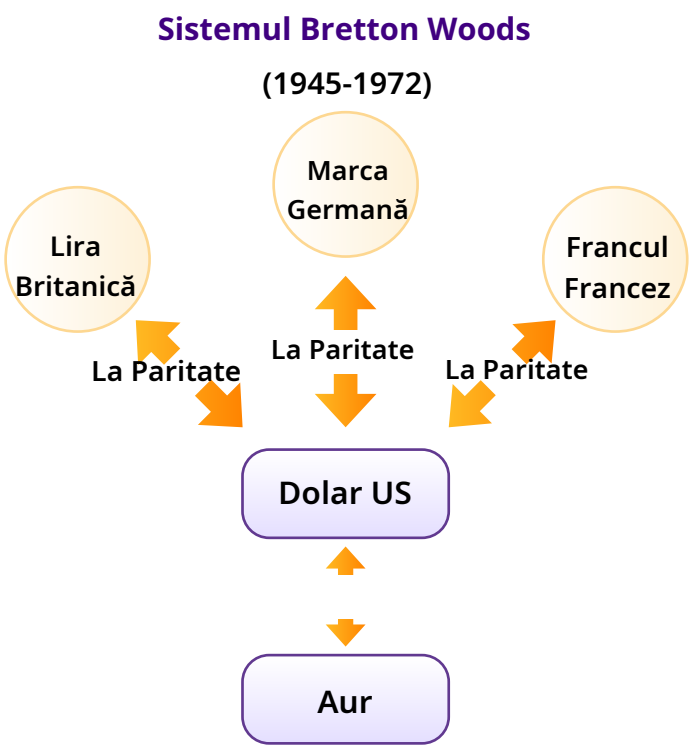
Ce se întâmplă când încerci cu adevărat să pui în practică doctrina banilor de hârtie? Află în episodul al patrulea din seria „Istoria banilor de hârtie”.



Realizăm că acesta este un moment de cotitură în modul în care funcționează banii. Se trece de la un sistem de monedă sănătoasă (susținută de metale prețioase) la un sistem de monedă fiat nesusținută de o marfă fizică. Această tranziție nu s-a produs peste noapte, ci a fost un proces gradual influențat de mai mulți factori. Revoluția industrială, cu producția în masă și urbanizarea, a jucat un rol, la fel și dezvoltarea sistemelor financiare avansate precum băncile și bursele. Apariția băncilor centrale și a altor autorități monetare a contribuit la centralizarea și controlul banilor, ducând la emiterea monedelor fiat pentru susținerea creșterii economice.

Totuși, apar și dezavantaje ale acestei centralizări, inclusiv consumul iresponsabil,creșterea datoriei, și manipularea cetățenilor prin stimulente economice.

Până la Primul Război Mondial, puteai converti banii de hârtie într-o cantitate prestabilită de aur. Dar cele două războaie mondiale și criza din 1929 au pus capăt acestui sistem. În 1944, acordul Bretton Woods a stabilit dolarul american ca monedă de rezervă mondială și a fixat valoarea dolarului la prețul aurului de 35$ pe uncie. Monedele altor țări au fost legate de dolar, ceea ce a ajutat la stabilizarea piețelor financiare internaționale.



Din păcate, sistemul a început să se destrame la sfârșitul anilor '60, ducând la „Nixon Shock” în 1971, când guvernul SUA a suspendat convertibilitatea dolarului în aur. Acesta marchează sfârșitul etalonului aur și începutul unei lumi conduse de crearea și acumularea de datorii.

În viața de zi cu zi, se observă că valoarea banilor nu mai este la fel de stabilă ca înainte. La fel cum o riglă elastică face dificilă măsurarea exactă a unei mese, trăind într-o lume fiat unde valoarea banilor este imprevizibilă, devine dificil să măsori corect valoarea bunurilor și serviciilor. Simți confuzie și neliniște adaptându-te la o lume unde valoarea banilor nu mai este legată de o marfă fizică precum aurul.

Vedem impactul acestei schimbări asupra economiei globale și începem să punem la îndoială stabilitatea și fiabilitatea monedelor fiat. Realizezăm că, în lumea modernă, dolarul nu mai este fix și constant ca atunci când era legat de aur, ci devine supus fluctuațiilor. Acest lucru face mai dificilă folosirea dolarului ca unitate de cont, deoarece valoarea sa este afectată de factori precum inflația, ratele dobânzilor, puterea economiei, evenimentele politice, speculațiile de piață și cererea în comerțul internațional. Poate fi o perioadă confuză și imprevizibilă în timp ce încerci să navighezi valoarea mereu schimbătoare a dolarului și impactul său asupra vieții tale.

În ciuda eforturilor de a îmbunătăți calitatea vieții prin sisteme monetare moderne, eficiență crescută, acces mai mare la informații și comunicare, majoritatea standardelor de trai ale oamenilor încep să scadă din cauza:

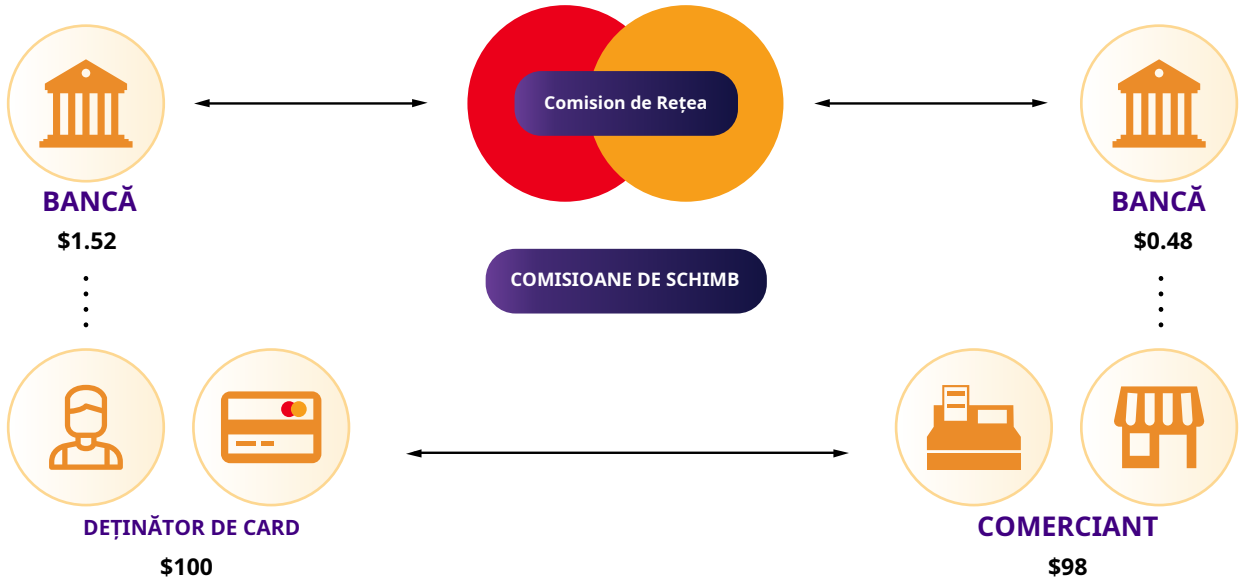
- Abuzului de centralizare
- Creșterii prețurilor
- Stagnării salariilor reale
- Slăbirii monedelor
- Nevoii de a cheltui mai mult pt. mai puține lucruri

Acest lucru creează provocări pentru cei cu resurse economice reduse, care pot avea acces limitat la educație, credit, resurse, rețele sociale și reprezentare politică, ducând la dezavantaje în capacitatea lor de a reuși.

Astfel, bogații par să devină tot mai bogați, iar săracii tot mai săraci.

3.1.4 De la hârtie la plastic

Astăzi, am parcurs un drum lung de la introducerea primului card de credit în anii '50. Cu o simplă trecere a cardului, putem cumpăra orice dorim, oricând dorim, fără bătăi de cap. E ca și cum am deschide o lume de posibilități infinite, iar entuziasmul descoperirii este palpabil... sau cel puțin așa credeam. Puțini știau că dependența de credit va avea efecte dureroase – precum creșterea costului total al bunurilor și stimularea unei economii sortite eșecului.



Pe măsură ce tehnologia avansează, la fel evoluează și modul în care gestionăm banii. Internetul devine un jucător important în lumea financiară, cu servicii bancare online și site-uri de comerț electronic care permit gestionarea și cheltuirea banilor exclusiv online.

Ascensiunea banilor digitali marchează următorul salt semnificativ în această evoluție, oferind noi posibilități și remodelând modul în care facem tranzacții financiare.

3.2 Moneda digitală

Spre deosebire de cele tradiționale, monedele digitale există doar în formă electronică. Sunt stocate și schimbate folosind calculatoare și software special.

Moneda digitală permite indivizilor să trimită bani prin internet. La fel cum emailul permite trimiterea instantanee de mesaje fără costuri de expediere, monedele digitale permit trimiterea și primirea instantanee de valoare cu costuri foarte mici.

Monedele pe care le folosim astăzi sunt tot mai digitale. Doar o mică parte din masa monetară există sub formă de monede și bancnote. Băncile și serviciile bancare oferă utilizatorilor aplicații pentru schimbul facil de bani online. Dar de unde vin banii?

În acest capitol, am fost martori la transformarea de la monedă sănătoasă, reprezentați de aur, la monedă fără acoperire sub formă de hârtie, și acum, monedă fiat digitală. În capitolul următor, vom explora cum funcționează sistemul monetar fiat actual și cum a apărut acesta.

Capitolul #4

Ce sunt banii fiat și cine îi controlează?

4.0 Introducere

4.1 Scurtă istorie a banilor fiat

4.2 Sistemul Fiat

4.2.1 Un sistem monetar prin decret

4.2.2 Rezerve fracționare: Un sistem alimentat de datorii

Activitate: Rezerve fracționare

4.2.3 Cine controlează sistemul fiat și cum beneficiază?

4.3 Monedele digitale ale băncilor centrale: Viitorul banilor fiat

Caietul elevului

Limba Română | 2025

Ce sunt banii fiat și cine îi controlează?

4.0 Introducere

> Istoria omenirii este istoria banilor care își pierd valoarea.
>
> **Milton Friedman**

Am văzut în capitolul precedent cum banii au evoluat în timp și cum sistemul nostru monetar a trecut de la bani siguri la bani nesiguri, modelând lumea în care trăim astăzi. Acest capitol aprofundează modul în care aceste evoluții au dus la sistemul fiat de astăzi și cum funcționează acesta.

Deci, cum arată acest sistem fiat și cum a apărut?

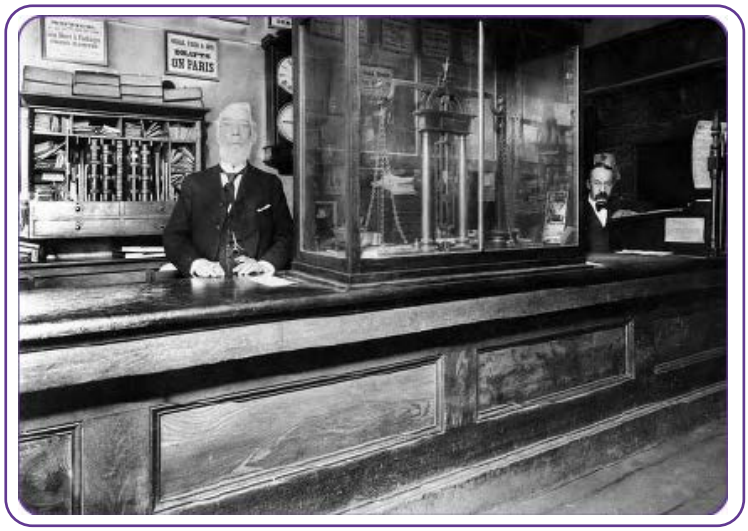
Pentru a răspunde la această întrebare, trebuie să ne concentrăm atenția asupra dolarului american, moneda de rezervă actuală a lumii, care joacă un rol dominant în lumea de azi. Fiecare țară, direct sau indirect, simte impactul deciziilor luate cu privire la dolarul american. Pentru a înțelege cu adevărat cum funcționează sistemul fiat în țara ta, este esențial să descoperi firele istorice care îl leagă de locul de naștere al sistemului fiat – Statele Unite ale Americii.

4.1 Scurtă istorie a banilor fiat

1,300 î.Hr.	1913	1933	1934	1944	1971	1980
Standardul Aur	Crearea Băncii Centrale numită „Federal Reserve”	Ordinul Executiv 6102. Fiecare cetățean a fost obligat să predea aurul la o rată de schimb de $20.67 pe uncie	Legea Rezervelor de Aur. Furtul averii oamenilor prin devalorizarea dolarului cu 40% la $35 pe uncie de aur	Acordul Bretton Woods: USD a devenit principala monedă de rezervă mondială	Șocul Nixon, care a dat naștere sistemului fiat prin eliminarea convertibilității dolarului american în aur	Valoarea aurului a crescut de la $35 pe uncie în 1970 la $870 pe uncie în 1980, ceea ce a cauzat o pierdere de valoare a banilor oamenilor de 96% în doar 10 ani

În secolul al XIX-lea, civilizațiile din întreaga lume prosperau pe un standard monetar solid, folosind metale prețioase precum aurul și argintul datorită rarității, durabilității și recunoașterii lor. Pe măsură ce comerțul global a crescut, transportul unor cantități mari de metal a devenit dificil, ducând la apariția depozitelor de aur și argint. Aceste depozite stocau în siguranță metalele valoroase ale oamenilor și ofereau certificate de hârtie care puteau fi răscumpărate pentru cantități specifice de aur sau argint. În schimbul depozitării banilor, indivizii primeau

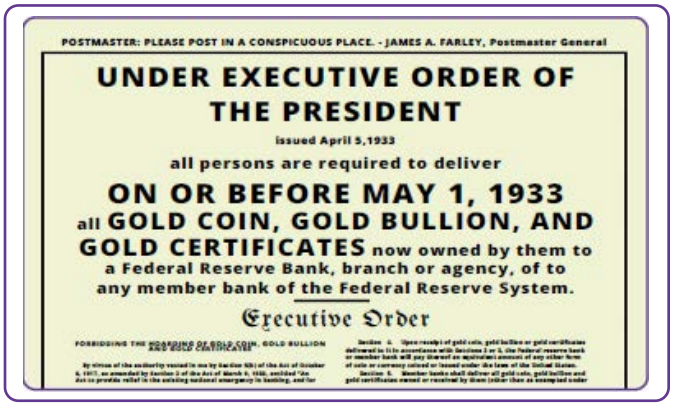
certificate de hârtie direct legate de cantitatea exactă de aur sau argint depozitată. Această legătură directă între certificatele de hârtie și banii marfă tangibili a marcat începutul a ceea ce recunoaștem astăzi ca bănci.



Inițial, băncile aveau scopul de a proteja banii clienților, dar ulterior au început să se implice în practici riscante de creditare, emițând certificate pentru aur pe care nu îl dețineau. Această practică a generat riscul de panică bancară (bank run) dacă prea mulți clienți solicitau banii simultan. Pentru a gestiona riscul, băncile au colaborat cu guvernele

pentru a crea un sistem care legaliza recreditarea. În 1913, au creat Federal Reserve, o bancă centrală responsabilă de salvarea băncilor aflate în dificultate. Guvernele au recunoscut valoarea aurului și argintului, ducând la conflicte și războaie pentru control. În anii premergători celui de-al Doilea Război Mondial, lideri precum Lenin, Stalin, Churchill, Roosevelt, Mussolini și Hitler au confiscat aurul în scopuri strategice.

La începutul anilor 1930, a avut loc o schimbare semnificativă în modul în care banii erau susținuți de active în Statele Unite. La acea vreme, o mare parte din averea oamenilor era stocată sub formă de aur. Totuși, în 1933, președintele Roosevelt a emis Ordinul Executiv 6102, care a cerut fiecărui cetățean să predea aurul. Nu a fost un schimb voluntar – oamenii au fost obligați să predea aurul, iar refuzul era pedepsit sever.


POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE. - JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5,1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, of to any member bank of the Federal Reserve System.

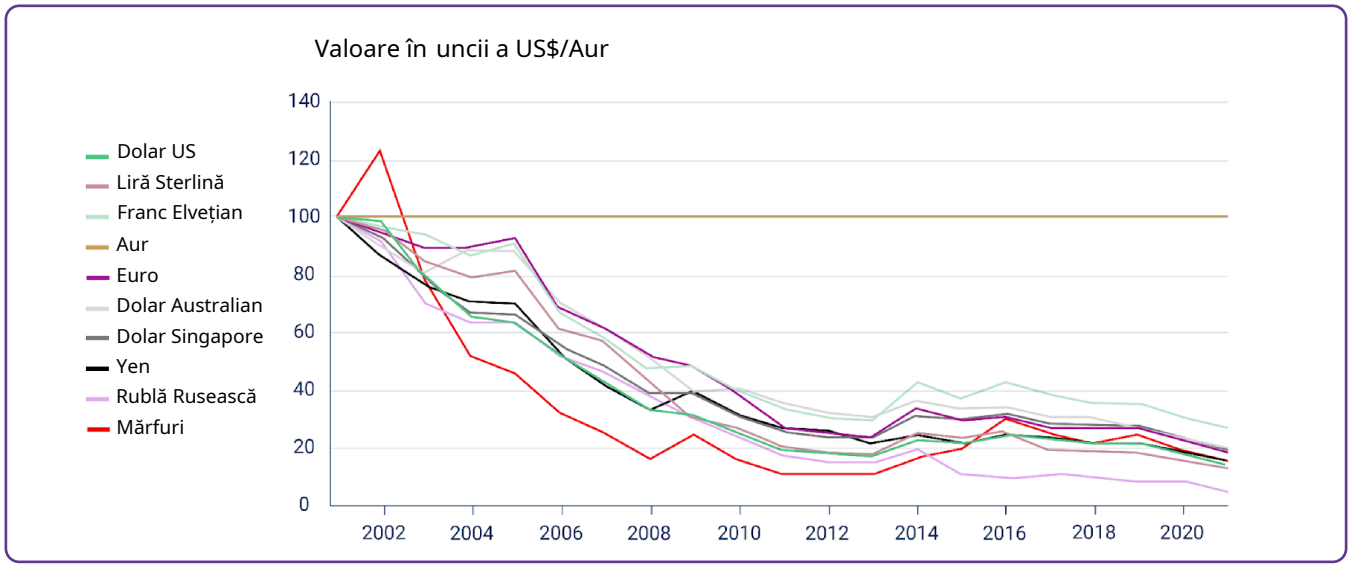
Executive Order

Guvernul a stabilit rata de schimb la 20,67$ pe uncie de aur. Asta însemna că pentru fiecare uncie de aur deținută, o persoană primea certificate de hârtie echivalente cu 20,67$. Oamenii au fost nevoiți să accepte acești dolari de hârtie, sperând că într-o zi îi vor putea schimba din nou pe aur.

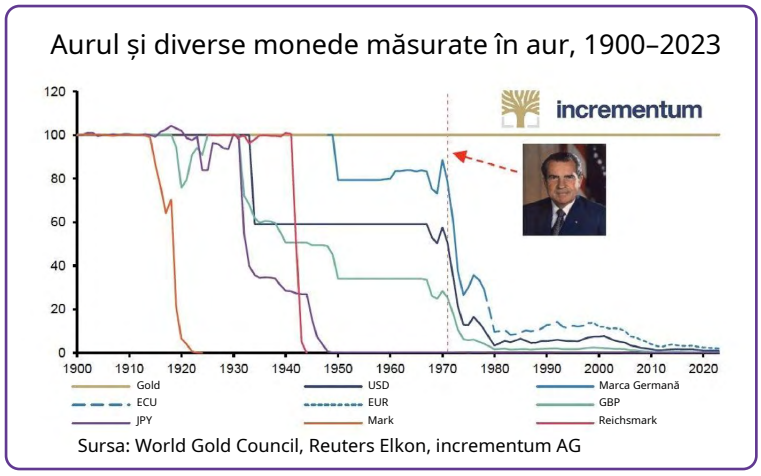
Ce sunt banii fiat și cine îi controlează?

În 1934, Legea Rezervelor de Aur a permis din nou schimbul dolarilor de hârtie pe aur. Totuși, exista o capcană: guvernul a devalorizat deliberat dolarul de hârtie, crescând rata de schimb la 35$ pe uncie de aur. Această devalorizare a afectat grav indivizii din clasele de jos și mijlocii, deoarece economiile lor, odată mai valoroase, au devenit mai puțin valoroase din cauza scăderii valorii dolarului de hârtie.

După al Doilea Război Mondial, acordul Bretton Woods din 1944 a stabilit dolarul american ca monedă de rezervă mondială, care putea fi schimbată pe aur. Totuși, această legătură între dolarul american și aur a fost ruptă în 1971, când președintele Nixon a pus capăt convertibilității dolarului american în aur. Acest moment a marcat o schimbare semnificativă, ducând la adoptarea unui sistem de bani fiat, unde valoarea monedei nu mai este susținută de o marfă fizică precum aurul, ci de încrederea și loialitatea oamenilor care o folosesc. Pe măsură ce guvernele și băncile centrale au păstrat cea mai mare parte a aurului oamenilor, valoarea aurului a crescut, ajungând la 870$ pe uncie în 1980.



În concluzie, povestea trecerii societății umane de la un standard monetar solid la unul nesigur (fiat) ne arată cum guvernele și băncile au capturat metalele prețioase de la cetățenii lor. În timp ce banii reali au ajuns în buzunarele guvernelor și băncilor, oamenii au rămas cu bucăți de hârtie a căror valoare provine doar din obligația impusă de guverne de a le folosi.



4.2 Sistemul Fiat

> Problema de bază cu moneda convențională este toată încrederea necesară pentru ca ea să funcționeze. Banca centrală trebuie să fie de încredere să nu devalorizeze moneda, dar istoria monedelor fiat este plină de încălcări ale acestei încrederi.
>
> **Satoshi Nakamoto**

Omenirea a trecut de la bani siguri controlați de mulți, la bani nesiguri controlați de puțini. Dar cum funcționează exact acest sistem?

4.2.1 Un sistem monetar prin decret

Sistemul fiat se caracterizează prin natura sa obligatorie, impusă oamenilor prin legi privind moneda legală. Termenul „fiat", provenit din latină, înseamnă „prin decret", reprezentând o directivă emisă de autorități.

Spre deosebire de banii susținuți de active tangibile precum aurul, moneda fiat nu are o astfel de susținere. În schimb, utilizarea sa este impusă prin lege. Monedele de zi cu zi precum dolarul, euro, lira, yuanul, leul și altele sunt monede fiat

> Legea privind moneda legală: O lege care obligă toți cetățenii să accepte un anumit tip de monedă.

Valoarea monedei fiat se bazează pe credința că poate fi schimbată pe bunuri și servicii și pe iluzia că își va păstra valoarea în timp. Moneda fiat este comparabilă cu un bilet la concert; valoarea sa nu stă în biletul de hârtie, ci în asigurarea că trupa (guvernul și banca centrală) va oferi un spectacol grozav (stabilitate economică).

Avantaje ale monedei fiat

- **Ușurință:** Moneda fiat este convenabilă pentru tranzacțiile zilnice.
- **Costuri și riscuri mai mici:** Moneda fiat nu necesită securitate ridicată ca aurul, fiind mai ieftină și mai sigură.

Dezavantaje ale monedei fiat

- **Riscuri de inflație:** Prețurile pot crește continuu, provocând inflație și cazuri istorice de hiperinflație.
- **Control și manipulare centralizată:** Grupuri mici pot influența sistemul, ducând la cenzură și confiscare.
- **Risc de contrapartidă** Dacă guvernul întâmpină dificultăți, moneda poate pierde valoare.
- **Posibilitate de abuz:** Sistemul poate fi abuzat, ducând la corupție și pierderea încrederii.

Ce sunt banii fiat și cine îi controlează?

Marfă vs. Fiat: Imaginează diferența

Ține minte: Înainte de apariția monedei fiat, guvernele băteau monede dintr-o marfă fizică valoroasă, rară și greu de obținut, precum aurul sau argintul, sau tipăreau bani de hârtie care puteau fi răscumpărați pentru o cantitate fixă de marfă fizică. Acesta era sistemul susținut de marfă (commodity-backed).

Acum, în sistemul fiat, este mai degrabă ca banii din Monopoly. Banii din sistemul fiat sunt bucăți de hârtie tipărite de banca centrală, iar politicile guvernului influențează direct valoarea lor. Guvernul și băncile centrale sunt practic „bancherii jocului Monopoly" care controlează modul în care funcționează jocul, cine primește ce și cât valorează. Cu alte cuvinte, guvernul promite să gestioneze bine sistemul monetar.

În concluzie, monedele fiat au valoare doar pentru că guvernul impune utilizarea lor; nu există utilitate în sine pentru moneda fiat.

Pe scurt, sistemul fiat este un joc al încrederii, unde valoarea banilor noștri depinde de promisiunile celor care conduc și oamenii pot doar spera că guvernul acționează în beneficiul tuturor. În continuare, vom vedea cum băncile creează bani noi, cine este implicat și cum afectează economia.

4.2.2 Sistemul de rezervă fracționară: Un sistem alimentat de datorii

> Este probabil un lucru benefic faptul că cetățenii acestei națiuni nu înțeleg sistemul nostru bancar și monetar, deoarece, dacă l-ar înțelege, sunt convins că o revoluție ar izbucni...
>
> **Henry Ford**

Rezerva fracționară este una dintre principalele părți ale sistemului fiat, permițând băncilor să împrumute o mare parte din depozitele clienților. Te-ai întrebat vreodată de ce băncile oferă atât de multe servicii clienților? Deși pare că sunt generoase, trebuie să ne amintim că băncile sunt afaceri, iar scopul lor principal este profitul. Dar cum obțin profit dacă lasă oamenii să împrumute bani?

Băncile generează venituri prin:

- Perceperea de dobânzi la creditele acordate
- Comision pentru retragerea de la ATM și administrarea contului
- Câștiguri din investiții (titluri sau investiții imobiliare)
- Investirea sau împrumutarea unui procent din credite.
- Perceperea de comisioane la conturile curente și de economii

Când o bancă primește un depozit, este obligată să păstreze doar o parte (rată a rezervei minime obligatorii) și poate împrumuta restul

De exemplu, dacă depui 100$ cu o rezervă minimă obligatorie de 10%, banca poate împrumuta 90$, păstrând doar 10$ ca rezervă. Împrumutatul depune 90$ într-o altă bancă, permițând ciclului să continue. În ciuda depozitului inițial de 100$, suma totală de bani din economie crește la 271$, apărând parcă din nimic – fenomen cunoscut sub numele de efect de multiplicare.

Acest proces duce la un sistem monetar bazat pe datorii, deoarece băncile creează monedă nouă cu fiecare împrumut, crescând masa monetară totală. Pe măsură ce sistemul de rezervă fracționară continuă, datoria totală din economie crește, contribuind la inflație.

Sistemul se bazează pe un ciclu continuu de creare de monedă prin creditare, asemănător cu o aprovizionare constantă de droguri pentru un dependent. Totuși, dacă băncile împrumută mai mulți bani decât au în rezervă și deponenții se grăbesc să retragă simultan, băncile pot da faliment.

Aici intervine banca centrală ca creditor de ultimă instanță, furnizând monedă nouă pentru a preveni falimentul băncilor. Banca centrală face acest lucru prin răscumpărarea de active sau injectarea directă de monedă în conturile băncilor. Practic, băncile sunt salvate de la faliment prin injectarea constantă de monedă nouă de către băncile centrale. Acest sistem alimentat de datorii, duce la cicluri de boom și bust.

Imaginează că ai un prieten care este și bancher, să-l numim Dax.

Lui Dax îi plac bicicletele și vrea să împrumute bicicleta ta pentru că are multe drumuri de făcut. Îi dai bicicleta, iar Dax începe să promită aceeași bicicletă multor altor prieteni în același timp. Cu o singură bicicletă reală pe care i-o împrumuți, Dax reușește să creeze mai multe biciclete imaginare și începe să le împrumute prietenilor. Fiecare dintre prietenii lui crede că poate merge cu bicicleta oricând dorește. Dar, iată răsturnarea de situație – există doar o bicicletă reală! Toate celelalte sunt imaginare și doar promisiuni.

Ce se întâmplă? Pe măsură ce mai multe biciclete imaginare circulă, toată lumea este fericită, cel puțin la început, pentru că inițial nimeni nu folosește bicicleta în același moment – se pare că nu există nicio problemă; se pare că există o abundență de biciclete pentru toți. Astfel, toți prietenii încep să facă mai multe planuri, gândindu-se la toate locurile unde vor merge cu bicicletele.

Totuși, aici magia începe să-și piardă farmecul. Într-o zi însorită, toți decid că e ziua perfectă pentru o plimbare cu bicicleta. Toți apar la ușa lui Dax, entuziasmați să ia bicicletele imaginare la o tură. Dar, realitatea lovește – există doar o bicicletă reală. Dezamăgirea apare, iar valoarea plimbărilor promise scade brusc.

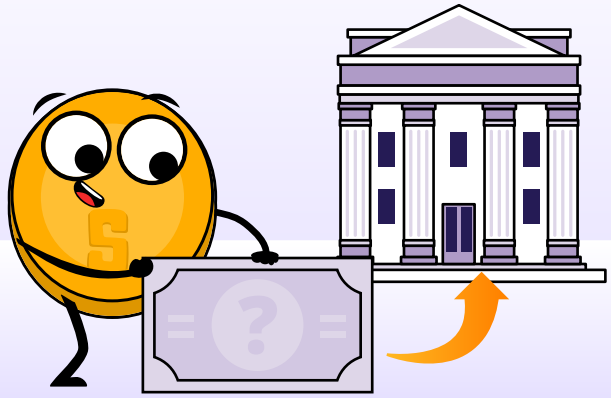
În lumea creditării cu rezervă fracționară, povestea este similară. Băncile împrumută mai mulți bani decât au de fapt, iar pentru o vreme toată lumea se bucură de beneficii. Circulă mai mulți bani și pare că există destui pentru toți. Dar, dacă prea mulți oameni încearcă să-și retragă banii în același timp, valoarea reală devine evidentă: nu există suficient pentru a onora toate promisiunile.

Acest scenariu afectează binele comun și valoarea tuturor celor implicați. Promisiunea abundenței se transformă într-o înșelătorie. La fel cum bicicletele imaginare își pierd valoarea percepută când toți vor o plimbare reală, valoarea banilor din economie poate scădea când toți vor să-și revendice partea reală. Când se întâmplă asta, oamenii realizează că banii pe care îi au la bancă nu sunt cu adevărat acolo, ceea ce duce la panică, retrageri masive și chiar la prăbușirea unor economii întregi. Cei care plătesc pentru aceste prăbușiri au fost, până acum, mereu aceeași: clasa de jos și mijlocie a lumii.

Ce sunt banii fiat și cine îi controlează?

Boom

Expansiunea creditului prin sistemul de rezervă fracționară (băncile comerciale creează monedă fiat și o împrumută clienților)

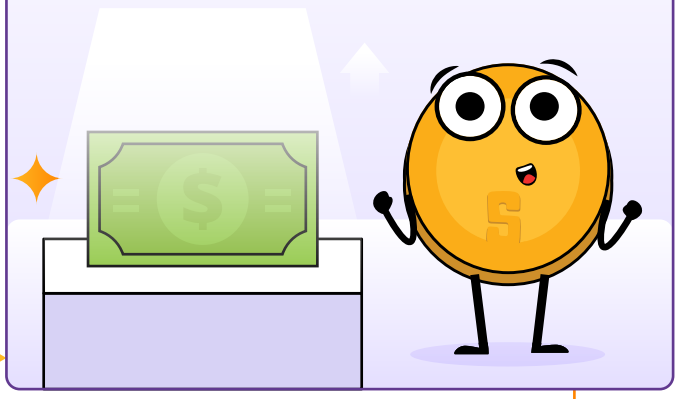


- Expansiunea masei monetare (moneda nou creată intră în sistem și mărește masa monetară)
- Supra-investiție (clienții folosesc creditele pentru a investi pe piețe, creând o creștere a cererii)
- Inflația prețurilor (prețurile cresc ca urmare a noii cereri)
- Lipsa cererii noi

Bust

- Prețurile scad (investitorii intră în panică și încep să vândă la prețuri mai mici deoarece nu există cerere reală)
- Persoane și companii nu-și mai pot plăti creditele (valoarea garanțiilor scade)
- Băncile dau faliment (dețin active care valorează mai puțin decât creditele acordate)
- Intervenția băncii centrale, salvând băncile

Băncile sunt salvate cu monedă nouă (banca centrală răscumpără activele deținute de bănci la un preț mai mare decât valoarea de piață sau creează direct monedă nouă și le-o oferă)



Repetare (mai multă expansiune a creditului, pregătind următoarea fază de boom)

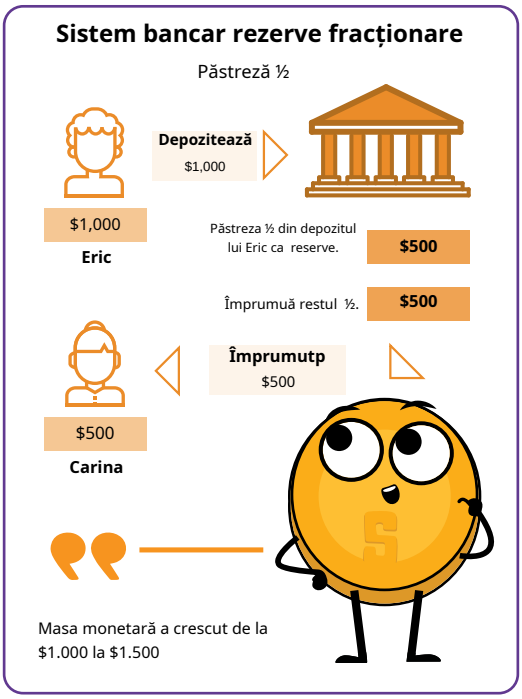
Activitate: Rezervă fracționară

Avem nevoie de următorii voluntari:

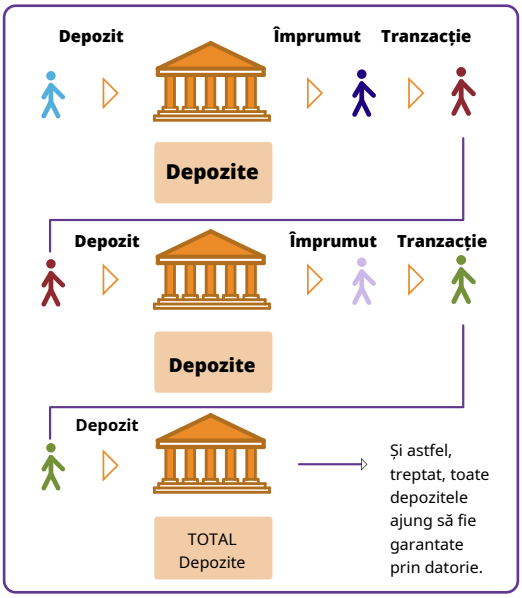
A = Depunător (Albastru deschis)
B = Casier bancar (Bancă)
C = Debitor nr. 1 (Albastru închis)
D = Proprietar de imobil/Depunător (Roșu)
E = Debitor nr. 2 (Mov deschis)
F = Proprietar galerie de artă (Verde)

În următorul exercițiu, vom explora cum sistemul de rezervă fracționară poate duce la devalorizarea monedei, inflație și scăderea puterii de cumpărare. Vom folosi un exemplu simplificat cu șase participanți, unul dintre ei fiind bancă, și un raport de rezervă folosit frecvent și astăzi: 10%.

- Persoana A tocmai a câștigat 100.000$ la loterie și îi depune la bancă (B). Cu un raport de rezervă de 10%, B trebuie să păstreze 10.000$ în seif și poate împrumuta restul de 90.000$.
- Persoana C împrumută suma maximă (90.000$) de la B și o folosește pentru a cumpăra o casă de la D
- Persoana D depune cei 90.000$ primiți de la C la bancă (B). Depozitele totale din bancă sunt acum 190.000$.
- Persoana E solicită un credit de la B, iar banca împrumută 90% din noul depozit, adică 81.000$.
- Persoana E folosește creditul de 81.000$ pentru a cumpăra o operă de artă de la F, care apoi depune banii la bancă (B). Depozitele totale înregistrate sunt acum 271.000$.



În acest scenariu, depozitul inițial de 100.000$ a dus la un total de 271.000$ în depozite după ce a circulat prin economie.



Dacă raportul de rezervă ar fi redus la 1%, suma de bani creată ar fi mult mai mare (100.000$ / 0,01 = 10.000.000$). În acest caz, câtă monedă ar fi creată cu acei 100.000$ dacă banii continuă să circule prin economie?

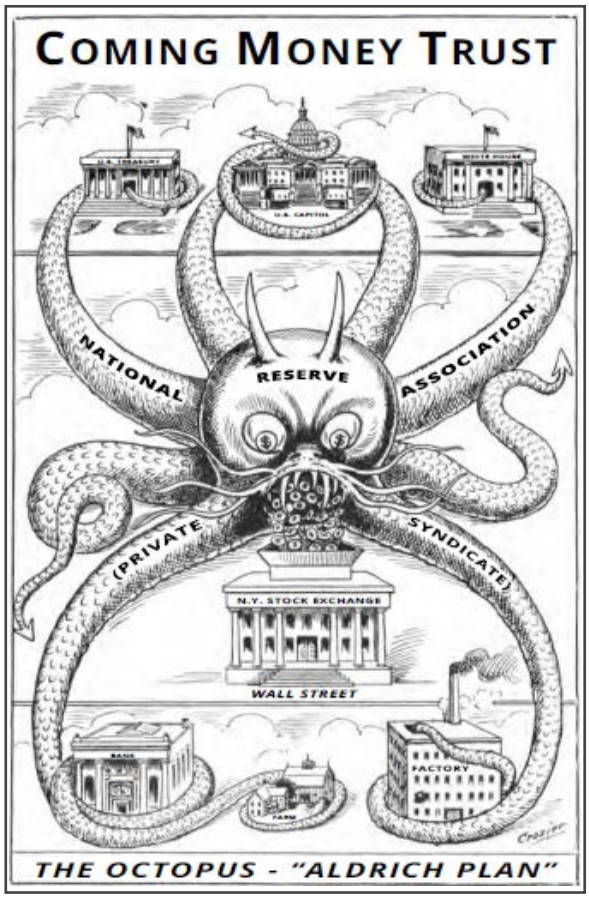
Este important de menționat că din 2020, Federal Reserve (Banca Centrală a SUA) a redus raportul de rezervă la zero procente pentru a stimula economia.

Ce sunt banii fiat și cine îi controlează?

4.2.3 Cine controlează sistemul fiat și cum beneficiază ei?

Există patru jucători principali: guvernul, indivizii bogați, sectorul financiar și banca centrală. Împreună, ei controlează sistemul fiat.

Guvernul: Guvernul este ca regizorul spectacolului fiat. Pe lângă colectarea taxelor, este finanțat prin datorii noi (obligațiuni) emise de Trezorerie. Când nu există suficientă cerere pentru aceste obligațiuni, orice datorie rămasă este cumpărată de banca centrală. Asta înseamnă că pot continua activitățile și urmări interesele fără aprobarea poporului. E ca și cum ai avea un card de credit fără să te îngrijorezi de plata imediată. Poate părea avantajos pentru guvern, dar vine cu un cost pentru ceilalți.



Indivizii bogați: Indivizii bogați beneficiază mult de pe urma sistemului fiat. Având posibilitatea de a acumula mai multe datorii, pot investi în active precum mărfuri, imobiliare și acțiuni, creând noi bogății aproape fără efort.

Sectorul financiar (bănci): Băncile și alte instituții financiare nu controlează direct sistemul fiat, dar beneficiază enorm de pe urma lui. Fără responsabilitate, pot accelera crearea de monedă nouă prin creditare fracționară, obținând venituri mai mari. Băncile sunt practic ferite de consecințe, fiind salvate cu monedă fiat nouă pentru a preveni colapsul sistemului.

Banca Centrală: Banca centrală este cea care trage sforile, controlând teoretic creșterea masei monetare. Dar iată trucul — banca centrală este supusă legilor guvernului, servind interesele acestuia. E ca un păpușar controlat de alt păpușar. Banca centrală pare a fi la conducere, dar de fapt servește indirect dorințele guvernului de a tipări bani din nimic când are nevoie.

Cum beneficiază: Aceste grupuri beneficiază în moduri diferite, creând o rețea complexă de control.

Guvernul obține fonduri fără consecințe imediate, indivizii bogați și băncile fac bani ușor, iar banca centrală menține spectacolul. Între timp, restul populației resimte efectele, confruntându-se cu provocări pe măsură ce sistemul evoluează.

În final, păpușarii sistemului fiat creează un spectacol unde puțini beneficiază enorm, iar mulți se întreabă despre corectitudinea scenei financiare în care se află.

Rolul băncilor centrale

Băncile centrale modelează discret modul în care funcționează o economie. Rolul lor oficial este să asigure stabilitatea, integritatea și „să mențină lucrurile stabile”, dar metodele lor dezvăluie o latură mai misterioasă.

Băncile centrale lucrează îndeaproape cu guvernele și trag sforile politicii monetare, controlând masa monetară cu instrumente precum ratele dobânzilor. În perioade de criză, tipăresc bani din nimic și îi injectează în economie prin băncile comerciale, făcând să pară că totul este în regulă.

Nu doar supraveghează; băncile centrale reglementează băncile comerciale, stabilesc regulile jocului și intervin când băncile au probleme (acționând ca împrumutător de ultimă instanță). Această rețea de control, deși pare protectoare, face economia și băncile și mai dependente de ele.

Înțelegerea modului în care apar trilioane de dolari din fonduri de stimulare și cine decide alocarea lor este esențială pentru a înțelege sistemul financiar mai larg. Guvernele folosesc mai multe instrumente pentru a gestiona masa monetară la momente specifice.

Băncile centrale și guvernele pot folosi instrumente de politică monetară și fiscală pentru a influența masa monetară și economia. De exemplu, Rezerva Federală a Statelor Unite (The Fed) folosește politica monetară pentru a ajusta ratele dobânzilor, afectând cantitatea de bani în circulație. Politica fiscală, pe de altă parte, implică utilizarea cheltuielilor și politicilor fiscale pentru a influența activitatea economică.

Rata de referință

Politică Monetară

Șomaj sub

6.5%

2% - 3%

Creștere anuală a Produsului Intern Brut

Rata inflației de bază între

2.0% - 2.5%

Politică Fiscală

Expansionistă

Are ca scop creșterea cheltuielilor consumatorilor și a investițiilor în afaceri pentru a stimula cererea agregată și creșterea economică.

Taxe mai minci

Creșterea cheltuielilor guvernamentale

VS

Politică Fiscală

Contractionară

Are ca scop reducerea cheltuielilor consumatorilor și a investițiilor în afaceri pentru a încetini creșterea economică nesustenabilă și pentru a preveni sau reduce inflația ridicată.

Scăderea cheltuielilor guvernamentale

Taxe mai mari

Politicile de curs valutar, șocurile de ofertă și controlul prețurilor sunt instrumente suplimentare pentru a reglementa masa monetară și a influența comerțul și economia. Deși aceste politici urmăresc stabilizarea prețurilor și controlul inflației, intervenția duce adesea la cicluri de boom și recesiune, creând provocări pentru toți cei care folosesc moneda controlată.
Exemplu: „Prea mare pentru a eșua" (Too big to fail) se referă la instituții financiare atât de mari și interconectate încât eșecul lor ar avea repercusiuni catastrofale asupra întregului sistem financiar. În timpul crizei financiare din 2008, mai multe bănci mari au fost considerate „prea mari pentru a eșua", determinând guvernul SUA să intervină și să ofere ajutoare pentru a preveni colapsul lor.
Unul dintre cele mai proeminente exemple de instituție „prea mare pentru a eșua" în timpul crizei financiare a fost banca de investiții Lehman Brothers. Când Lehman Brothers a intrat în faliment în septembrie 2008, a declanșat un efect de domino, inclusiv prăbușirea aproape totală a gigantului de asigurări AIG și o scădere masivă a pieței bursiere. Guvernul SUA a trebuit să intervină și să ofere ajutoare altor instituții financiare majore pentru a evita haosul și a proteja economia mai largă.
Unul dintre cele mai proeminente exemple de instituție „prea mare pentru a eșua" în timpul crizei financiare a fost banca de investiții Lehman Brothers. Când Lehman Brothers a intrat în faliment în septembrie 2008, a declanșat un efect de domino, inclusiv prăbușirea aproape totală a gigantului de asigurări AIG și o scădere masivă a pieței bursiere. Guvernul SUA a trebuit să intervină și să ofere ajutoare altor instituții financiare majore pentru a evita haosul și a proteja economia mai largă.

4.3 Monedele Digitale ale Băncilor Centrale: Viitorul banilor fiat

Monedele Digitale ale Băncilor Centrale (CBDC) sunt următorul pas al monedelor fiat. Spre deosebire de combinația dintre bancnote fizice, monede și plăți digitale, CBDC-urile sunt forme complet digitale ale monedelor fiat emise de guverne și controlate de băncile centrale.

Imaginează-ți moneda pe care o folosești zilnic, dar fără prezență fizică — fără monede care să zornăie în buzunar sau bancnote de împăturit. Ceea ce diferențiază CBDC-urile este nivelul crescut de control și monitorizare pe care îl oferă guvernelor și băncilor centrale. Cu CBDC-uri, autoritățile obțin o vizibilitate fără precedent asupra tranzacțiilor financiare, facilitând urmărirea și reglementarea fluxului de bani.

Guvernele și băncile centrale pot ajusta rapid forma și oferta CBDC-urilor, manipula ratele dobânzilor și aplica instrumente de politică monetară și fiscală cu o precizie mai mare. Practic, CBDC-urile oferă o modalitate mai eficientă pentru autorități de a influența și gestiona moneda fiat.

Deși CBDC-urile par viitorul banilor fiat, sistemul monetar actual funcționează deja pe un standard fiat pur. Monedele fiat nu mai sunt legate de aur, ceea ce a dus la o expansiune semnificativă a masei monetare fără restricții reale.

Acum că ai o imagine mai clară despre cum funcționează sistemul fiat, e timpul să explorezi consecințele sale în Capitolul 5.

Capitolul #5

Cum Problemele Duc la Soluții

5.0 Introducere în Problemă

5.1 Scăderea Puterii de Cumpărare

5.1.1 Inflația Monetară și Efectul asupra Puterii de Cumpărare

Activitate: Efectele Inflației - O Activitate de Licitație

5.2 Povara Datoriei Globale și Inegalitatea Socială

5.2.1 Impactul asupra Individului- Pierderea Puterii de Cumpărar

5.2.2 Impactul asupra Societății - Creșterea Inegalității Averii

Activitate: Consecințele Sistemului Fiat

5.2.3 Povara Datoriei Globale

5.3 Cypherpunks și Căutarea unei Monede Descentralizate

5.3.1 Cypherpunks

5.3.2 Sisteme Centralizate vs Sisteme Descentralizate

5.3.3 Scurtă Istorie a Monedelor Digitale

Caietul elevului

Limba Română | 2025

Cum Problemele Duc la Soluții

5.0 Introducere în Problemă

> Cine controlează volumul de bani din țara noastră este stăpân absolut asupra întregii industrii și comerțului... când realizezi că întregul sistem este foarte ușor de controlat, într-un fel sau altul, de câțiva oameni puternici de la vârf, nu va trebui să îți spună nimeni cum apar perioadele de inflație și depresie.
>
> **James A. Garfield, Președinte american**

În Capitolul 4, ai aflat că lumea financiară se bazează pe un sistem care s-ar putea să nu fie atât de solid pe cât pare. Sistemul fiat, susținut de adăugări constante de bani de hârtie, pare să favorizeze câțiva în detrimentul multora. Acest capitol dezvăluie ce înseamnă sistemul fiat pentru oamenii obișnuiți și societate. În final, explorăm povestea unui grup de indivizi care au observat problemele și au lucrat discret pentru a găsi o soluție ce ar putea schimba viitorul societății.

5.1 Scăderea Puterii de Cumpărare

5.1.1 Inflația Monetară și Efectul asupra Puterii de Cumpărare

Inflația monetară este creșterea masei monetare într-o economie, afectând direct omul de rând prin reducerea puterii de cumpărare. Ciclul inflației prețurilor începe atunci când există mai mulți bani în circulație. Acest lucru crește cererea pentru bunuri și servicii, ducând în cele din urmă la creșterea prețurilor.
Să ne imaginăm un grup de prieteni – Alex, Bob și Călin – fiecare cu un dolar în mână, iar la vânzare există o singură sticlă de apă. Situația inițială este simplă: trei persoane cu un total de trei dolari și o sticlă de apă. Acum, să presupunem că cineva – să zicem guvernul local – decide să le dea fiecărui prieten încă un dolar. Acum, au împreună șase dolari. Cu acești bani noi, toți vor să cumpere acea sticlă de apă. Deoarece toți trei vor aceeași sticlă, încep să liciteze unul împotriva celuilalt.

Cererea crescută, alimentată de banii suplimentari, îi determină să ofere mai mult decât prețul inițial pentru sticla de apă. În final, războiul licitațiilor duce la creșterea prețului sticlei de apă. Această situație reflectă o scădere a puterii lor de cumpărare. Chiar dacă au mai mulți bani, nu pot cumpăra la fel de multe sticle de apă ca înainte, evidențiind impactul inflației asupra valorii banilor lor.

În acest exemplu, prietenii au experimentat o scădere a puterii de cumpărare deoarece foloseau o formă de bani influențată de factori externi, precum dolarii suplimentari introduși de guvern. Lipsa controlului asupra masei monetare, combinată cu cererea crescută, a dus la creșterea prețurilor, făcând mai dificilă achiziționarea aceleiași cantități de bunuri cu dolarii suplimentari.

Acest lucru ilustrează cum puterea de cumpărare a prietenilor a fost afectată de factori dincolo de controlul lor, subliniind importanța înțelegerii și chestionării sistemelor care influențează valoarea banilor noștri.

Acum, să vedem cum se întâmplă acest lucru în viața reală.

Activitate: Efectele Inflației – O Activitate de Licitație

Obiectiv: Să înțelegem conceptul de inflație și modul în care aceasta afectează prețurile bunurilor și serviciilor într-o economie.

Definiții:

Masa Monetară: suma totală de bani aflată în circulație într-o economie la un moment dat. Aceasta include:

- Monedă fizică, precum monede și bancnote
- Conturi curente
- Conturi de economii
- Conturi Money Market
- Depozite la termen mici sub 100.000$

Licitație: O vânzare publică în care bunurile sau proprietățile sunt vândute celui care oferă cel mai mult.

Exercițiu în clasă. Urmați instrucțiunile de mai jos:

1. Veți primi o sumă aleatorie de bani Monopoly de la profesor. Aceasta reprezintă masa monetară dintr-o societate.
2. Notați masa monetară totală în tabelul furnizat.
3. Profesorul va licita un baton de ciocolată către elevi. Pentru a câștiga batonul, va trebui să faceți cea mai mare ofertă folosind banii Monopoly. Notați oferta câștigătoare lângă masa monetară.
4. Profesorul va adăuga apoi o sumă semnificativă de bani Monopoly la masa monetară totală. Aceasta reprezintă o creștere a masei monetare într-o economie. Mai târziu, veți învăța cum se adaugă sau se reduce masa monetară într-o economie.

Societățile pot fi adesea imprevizibile și nedrepte, exemplificate de simularea unui profesor care oferă aleatoriu o sumă semnificativă de bani doar câtorva elevi. Acest lucru imită situațiile reale în care distribuția inegală a resurselor și oportunităților poate apărea, evidențiind aleatorietatea și nedreptatea inerente în multe situații.

5. Profesorul va licita un al doilea baton de ciocolată către elevi folosind același proces ca înainte. Notați oferta câștigătoare lângă masa monetară din tabel.
6. Profesorul va repeta licitația pentru a treia oară.

Rundă	Masa Monetară	Oferta Câștigătoare
1		
2		
3		

Concluzie:

1. Cum a afectat creșterea masei monetare ofertele câștigătoare pentru batoanele de ciocolată?
2. Care este relația dintre creșterea masei monetare și inflație?
3. Cum este relevantă masa monetară în lumea reală?
4. Când se injectează bani noi în economie, ce credeți că se va întâmpla cu prețurile bunurilor și serviciilor? Credeți că schimbarea prețurilor este temporară sau permanentă și de ce? Cum credeți că schimbările de preț afectează cetățenii pe termen lung?

5.2 Povara globală a datoriei și inegalitatea socială

5.2.1Impactul asupra indivizilor - Pierderea puterii de cumpărare

Ștefan este student la facultate și locuiește într-un apartament mic. Lucrează part-time la o cafenea pentru a-și plăti cheltuielile de trai și taxa de școlarizare. De când a început să trăiască independent, Ștefan a devenit priceput la gestionarea propriului său registru.

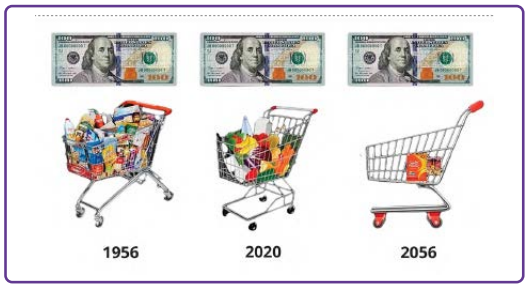
Un registru este o evidență detaliată a tuturor tranzacțiilor tale monetare. Fie că este vorba de bani câștigați sau cheltuiți, un registru te ajută să le urmărești pe toate.

La începutul anului 2023, și-a bugetat 10.000 USD pentru cheltuielile de trai pentru întregul an, incluzând chiria, mâncarea și alte necesități. Acestea au fost tranzacțiile sale pentru ianuarie 2023:

Data	Descriere	Suma	Tip	Sold
Chirie	Sold inițial			**$1,600**
01/01/2023	Chirie pentru ianuarie	**$800**	**Debit**	**$800**
01/05/2023	Alimente	**$100**	**Debit**	**$700**
01/15/2023	Salariu part-time	**$500**	**Credit**	**$1,200**
01/20/2023	Combustibil pentru mașină	**$350**	**Debit**	**$850**
01/30/2023	Manuale	**$150**	**Debit**	**$700**

Acest registru arată că soldul inițial al lui Ștefan a fost de 1.600 USD, din care a cheltuit (un debit) 800 USD pentru chiria lunară. Apoi a cheltuit 100 USD pe alimente și a primit 500 USD (un credit) ca salariu pentru jobul part-time, aducând soldul la 1.200 USD. Ulterior, a cheltuit bani pe combustibil și manuale, ajungând la un sold de 700 USD la sfârșitul lunii.

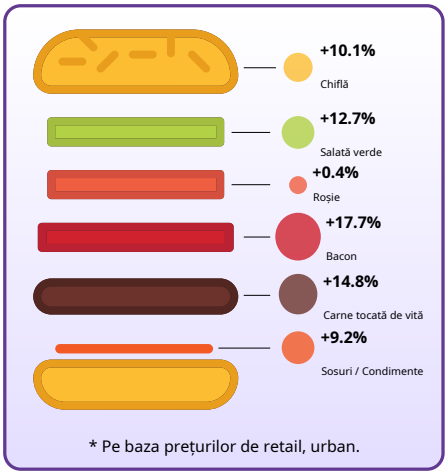
După douăsprezece luni, Ștefan ia prânzul cu bunicul său, căruia îi împărtășește detaliile bugetului său pentru 2024. Ștefan observă că bugetul său nu mai ajunge la fel de mult ca înainte și că costul vieții a crescut semnificativ în ultimul an. În timp ce Ștefan se întreabă cum este posibil acest lucru, bunicul îi arată următoarea imagine.



Ștefan nu-și crede ochilor. Acesta este momentul în care descoperă că prețul bunurilor și serviciilor crește drastic în timp, ducând la o scădere a puterii sale de cumpărare.

Bunicul spune: „În 1956, eram doar un tânăr la început de drum. Îmi amintesc că câștigam 380 USD pe lună ca muncitor într-o fabrică. Poate nu pare mult, dar era un salariu decent la acea vreme. De fapt, am reușit să economisesc suficient pentru a-mi cumpăra o casă în suburbii.”

Bunicul continuă: „Costurile lucrurilor erau foarte diferite în secolul trecut. De exemplu, în 2020, cumpărarea a 30 de batoane de ciocolată Hershey te-ar fi costat 26,14 USD. Totuși, dacă ne întoarcem în timp până în 1913, costul pentru aceeași cantitate de batoane de ciocolată Hershey ar fi fost doar 1,00 USD.”



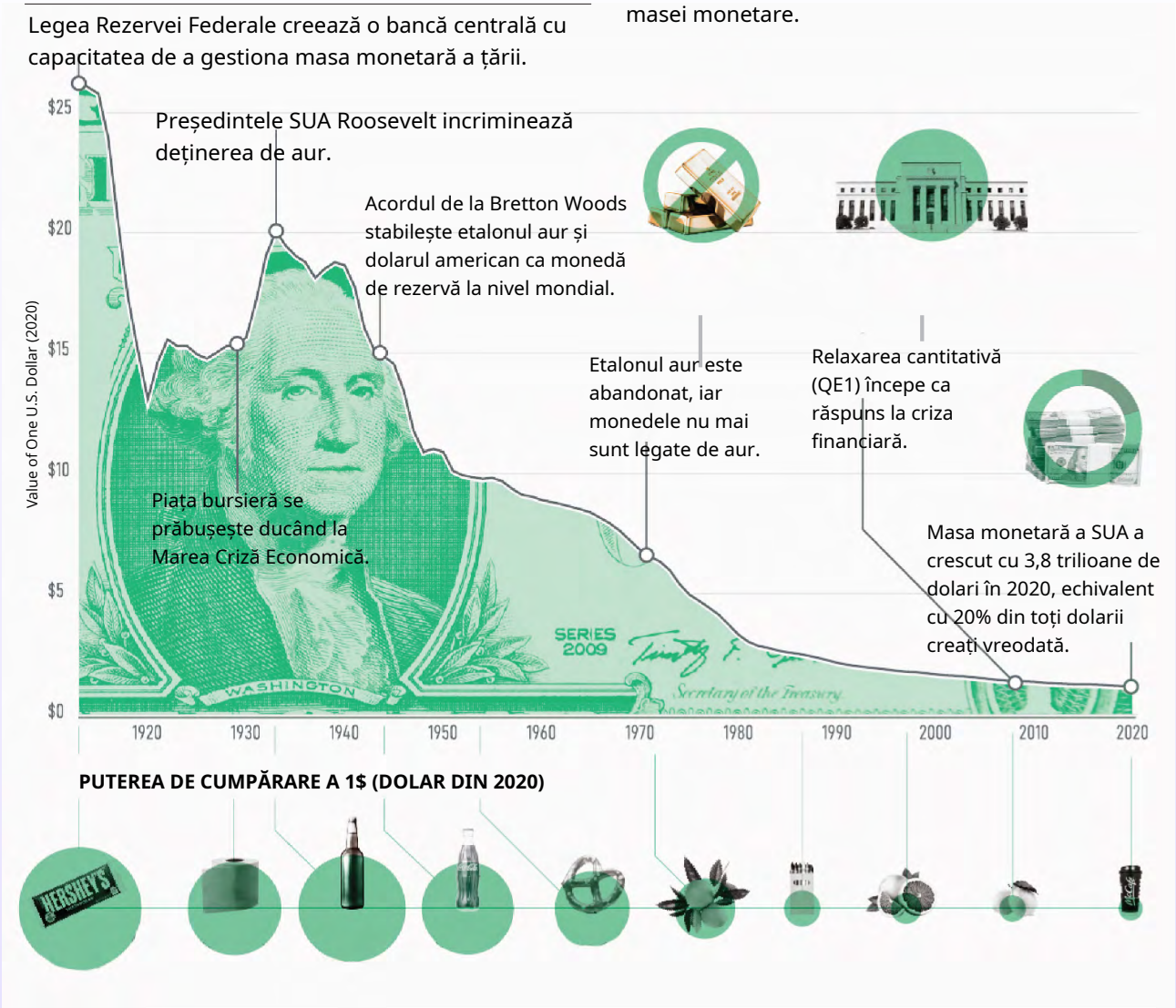
Această diferență semnificativă de preț evidențiază schimbarea puterii de cumpărare în timp și modul în care aceasta s-a modificat de-a lungul anilor din cauza inflației.

Cum Problemele Duc la Soluții

Valoarea unui dolar

Puterea de cumpărare a dolarului american

Puterea de cumpărare a dolarului american a scăzut drastic în ultimul secol din cauza creșterii inflației și a masei monetare.



$26.14	$15.14	$15.14	$14.71	$9.69	$6.39	$2.28	$1.61	$1.20	$1.00
30 batoane de ciocolată Hershey's	10 role de hârtie igienică	10 sticle de bere	20 sticle de Coca-Cola	10 pungi de covrigi	17 portocale	2 cutii de creioane	4 grapefruit	2 lămâi	1 cafea McDonald's
1913	**1929**	**1933**	**1944**	**1953**	**1971**	**1987**	**1997**	**2008**	**2020**

Ștefan: „Ce? E nebunie. Nu-mi pot imagina cât de mică ar fi fost chiria mea atunci comparativ cu acum."

Bunicul: „Ei bine, da, chiria ta ar fi fost mult mai ieftină atunci. Am un alt exemplu pentru a ilustra acest lucru: pe atunci, 1,00 USD îți cumpăra cam 10 pungi de covrigei. În 2020, am plătit 9,69 USD pentru aceeași cantitate. Imaginează-ți cât ar costa 10 pungi de covrigei astăzi."

Ștefan: „Wow, e foarte interesant, bunicule. Cum ai experimentat tu asta când erai mai tânăr?”

Bunicul: „Oh, Ștefan, toate lucrurile erau mult mai ieftine când eram tânăr. O pâine costa doar 0,18 USD, iar un galon de benzină doar 0,29 USD. Este incredibil cât de mult au crescut costurile de trai.”

După conversația cu bunicul său, Ștefan merge acasă să se uite din nou la registrul său. Descoperă rapid că trebuie să bugeteze cu 1.000 USD în plus pentru 2024 pentru a putea cumpăra același coș de bunuri și servicii pe care l-a achiziționat în anul precedent. Asta înseamnă că puterea sa de cumpărare a scăzut cu 1.000 USD, deoarece acum trebuie să cheltuiască mai mulți bani pentru aceleași bunuri și servicii. În timp ce salariul lui Ștefan crește doar puțin, costurile sale de trai cresc vertiginos în fiecare an.

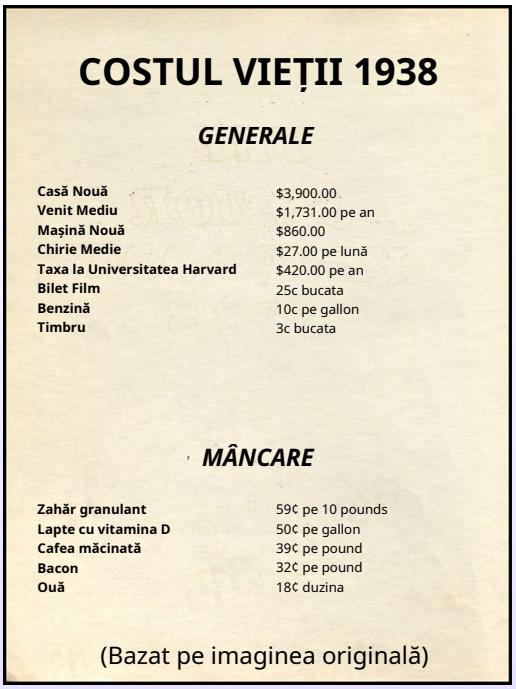
Tabelul următor arată costurile lui Ștefan în primul și al doilea an, precum și procentul de creștere a prețului.

Pentru ca Ștefan să aibă același standard de viață, va trebui să lucreze mai multe ore pe săptămână pentru a primi încă 1.000 USD.

Conform informațiilor de la Biroul de Statistică al Muncii, prețurile de astăzi sunt de aproximativ 30 de ori mai mari decât erau în 1913. Asta înseamnă că un dolar astăzi poate cumpăra doar aproximativ 3% din ce putea cumpăra atunci.

Articol	Cost Anul 1	Cost Anul 2	% Creștere
Chirie	$4,000	$4,500	12.5%
Alimente	$2,000	$2,300	15%
Necesități	$4,000	$4,500	5%
Total	**$10,000**	**$11,000**	**10%**

Pentru a ilustra, cineva îi oferă lui Ștefan o alegere de călătorie în timp – fie să ia 100$ în 1913, fie să aștepte până în 2023 și să primească doar 3$ – este ca și cum ai alege între o sesiune de cumpărături din trecut sau să primești doar câteva mici delicii astăzi.



COSTUL VIEȚII 1938

GENERALE

Casă Nouă	$3,900.00
Venit Mediu	$1,731.00 pe an
Mașină Nouă	$860.00
Chirie Medie	$27.00 pe lună
Taxa la Universitatea Harvard	$420.00 pe an
Bilet Film	25c bucata
Benzină	10c pe gallon
Timbru	3c bucata

MÂNCARE

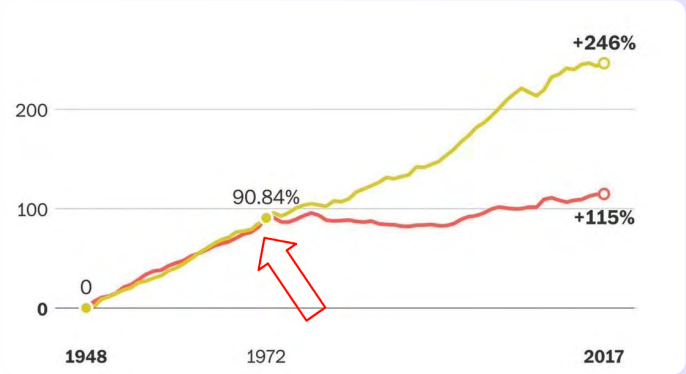
Zahăr granulant	59¢ pe 10 pounds
Lapte cu vitamina D	50¢ pe gallon
Cafea măcinată	39¢ pe pound
Bacon	32¢ pe pound
Ouă	18¢ duzina

(Bazat pe imaginea originală)

Cum Problemele Duc la Soluții

Când ne gândim la cifre, Ștefan câștigă mult mai mulți dolari într-un an decât a făcut vreodată bunicul său, dar dolarii pe care îi deținea bunicul lui Ștefan erau mult mai valoroși și puteau cumpăra mult mai mult atunci.

Creșterea productivității și a compensației pe oră
1948 —2017



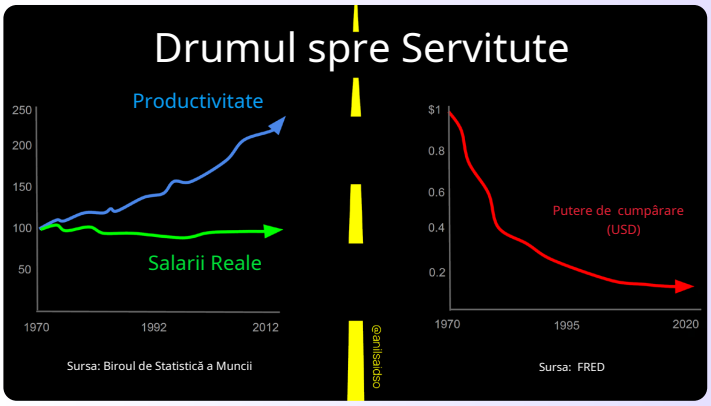
NOTĂ: Compensația include salariile și beneficiile pentru lucrătorii din producție și cei nesupervizori.

În lumea de azi, impactul semnificativ al inflației descurajează oamenii să economisească bani.

În schimb, majoritatea aleg să își cheltuiască banii imediat, deoarece valoarea lor scade rapid. Această perspectivă pesimistă le afectează capacitatea de a planifica pentru viitor.

După cum se vede în grafic, creșterea salariului mediu al unei persoane rămâne stagnantă atunci când este ajustată la inflație, ceea ce înseamnă că nu primesc măriri de salariu la același ritm cu scăderea valorii banilor, deși muncesc mai mult.

Exemplul lui Ștefan este doar unul dintre multele. În lumea fiat, este destul de comun ca guvernele să creeze bani din nimic pentru a-și promova propria agendă, lăsând indivizii din întreaga lume să suporte consecințele. Prețurile produselor de zi cu zi, de la pâine la locuințe, alimente la vacanțe, cresc în fiecare an. În timp ce bogații beneficiază de inflație datorită deținerii de active, oamenii obișnuiți văd cum banii lor munciți din greu își pierd valoarea. Rezultatul? Oamenii și familiile din întreaga lume se luptă din cauza scăderii puterii lor de cumpărare.



Oamenii din întreaga lume ajung să lucreze mai multe joburi și mai multe ore doar pentru a menține același standard de viață. Este ca și cum ai fi pe o bandă de alergare – alergi tot mai repede, dar nu ajungi niciodată înainte. Sistemul fiat îi face pe indivizi să simtă că sunt într-o cursă perpetuă împotriva creșterii prețurilor.

În încercarea lor de a ține pasul cu costurile în creștere, mulți apelează la credit, care este ca și cum ai pune un plasture mic pe o rană foarte adâncă. Oamenii iau împrumuturi sau iau decizii impulsive doar pentru a supraviețui. Banii rapizi devin o necesitate, iar indivizii ajung într-un ciclu în care supraviețuirea de azi are prioritate față de planificarea pentru mâine.

Sistemul fiat, cu tipărirea constantă de bani, afectează psihologia umanității. Instigă o preferință de timp ridicată – o concentrare pe câștigurile pe termen scurt în detrimentul planificării pe termen lung. La fel ca o soluție rapidă pentru o ușurare imediată, indivizii din lumea fiat tind să prioritizeze beneficiile pe termen scurt. Este un instinct de supraviețuire, creând un ciclu de dependență în care indivizii caută orice mijloc de a obține bani rapizi, chiar dacă nu este sustenabil.

În esență, impactul sistemului fiat conturează o imagine provocatoare pentru indivizii din întreaga lume. În sistemul fiat, prețurile cresc, veniturile stagnează, iar lupta pentru supraviețuire devine o bătălie zilnică. În timp ce anumite grupuri se îmbogățesc, majoritatea indivizilor din întreaga lume rămân dependenți de un sistem care îi face tot mai săraci.

5.2.2 Impactul asupra societății - Creșterea inegalității averii

Într-o societate bazată pe o moneda sănătoasă, deciziile financiare ale guvernului sunt legate de aprobarea poporului. Totuși, în sistemul fiat, guvernele pot intra în datorii nelimitate pe spatele cetățenilor.

Puterea de a tipări bani la discreție duce adesea la centralizarea politică. Sistemul fiat permite guvernelor să acumuleze datorii masive, luând decizii care le avantajează pe ele, nu pe majoritate. Superputerile, precum Statele Unite, obțin un avantaj competitiv datorită acestui fenomen. Ele pot tipări bani la nesfârșit pentru a-și finanța planurile, inclusiv războaie. Această abilitate permite acestor națiuni dominante să controleze, să influențeze și să se implice în conflicte geopolitice, creând un dezechilibru global de putere. Războaiele și acțiunile majore de control devin fezabile financiar pentru superputeri, în timp ce alții, fără aceeași flexibilitate financiară, se confruntă cu limitări.

În sistemul fiat, averea nu se distribuie uniform. Din contră, tinde să se concentreze în mâinile câtorva aleși. Acest fenomen seamănă cu un joc de Monopoly în care câțiva jucători dețin aproape toate hotelurile și proprietățile, iar majoritatea se chinuie să supraviețuiască. Sistemul fiat a devenit un instrument pentru anumite grupuri de a concentra averea. Tipărirea de bani permite guvernelor și colaborarea lor strânsă cu băncile centrale să injecteze mai multă monedă în economie, iar cei care primesc acești bani nou creați sunt cei cu avere și statut existent – entități și indivizi puternici. Aceste grupuri beneficiază de banii proaspăt tipăriți înainte ca efectele negative, precum scăderea puterii de cumpărare, să înceapă să se manifeste în economie.

Cum Problemele Duc la Soluții

Inegalitatea averii nu este doar despre cei care au și cei care nu au; este despre suprimarea mobilității economice. Cei din medii mai puțin privilegiate găsesc tot mai dificil să urce pe scara economică, asemănător cu a începe o cursă cu un rucsac greu în spate. Creșterea decalajului dintre bogați și săraci provoacă probleme pentru toți, cei bogați influențând politicile în favoarea lor. Acest lucru îngreunează viața oamenilor obișnuiți, ducând la tulburări sociale, lipsă de încredere în instituții și comunități care se destramă ca un castel de cărți.

Acesta este un fenomen global, care afectează societățile din țările dezvoltate și în curs de dezvoltare deopotrivă. Cei bogați, acționând adesea la scară transnațională, folosesc sistemul financiar global în avantajul lor, lărgind și mai mult prăpastia dintre clasele superioare și cele inferioare.

În sistemul fiat, a intra în datorii a devenit norma pentru omenire. Guvernele, instituțiile, afacerile și indivizii din întreaga lume se regăsesc scufundați într-o mare de datorii.

Schimbarea psihologică spre considerarea datoriilor ca fiind acceptabile își are rădăcinile în designul sistemului fiat. În ultimele decenii, a devenit tot mai ușor pentru entități să contracteze datorii substanțiale, iar pentru oamenii obișnuiți devine adesea o necesitate din cauza creșterii prețurilor și costurilor de trai.
Consumerismul, dorința constantă de a cumpăra și consuma, îi determină pe oameni să achiziționeze mai mult decât au nevoie, rezultând în supraconsum și risipă. Deși poate părea o goană nesfârșită după cumpărături, costul real depășește eticheta de preț, afectând sănătatea psihologică și bunăstarea oamenilor.

Devine clar că sistemul fiat nu este doar un mecanism economic. Mai degrabă, este un sistem care modelează întreaga societate umană. De la concentrarea puterii la dinamica globală, disparitățile de avere și normele sociale, sistemul fiat influențează direct modul în care națiunile funcționează și cum cetățenii obișnuiți își trăiesc viața.

Activitate: Consecințele sistemului fiat

1. Există și alte consecințe pe care indivizii și societatea în ansamblu le experimentează ca rezultat al sistemului fiat?

2. Care sunt consecințele în țara ta ca urmare a sistemului fiat? Ce s-a întâmplat de-a lungul istoriei și cum a afectat acest lucru oamenii din tara ta?

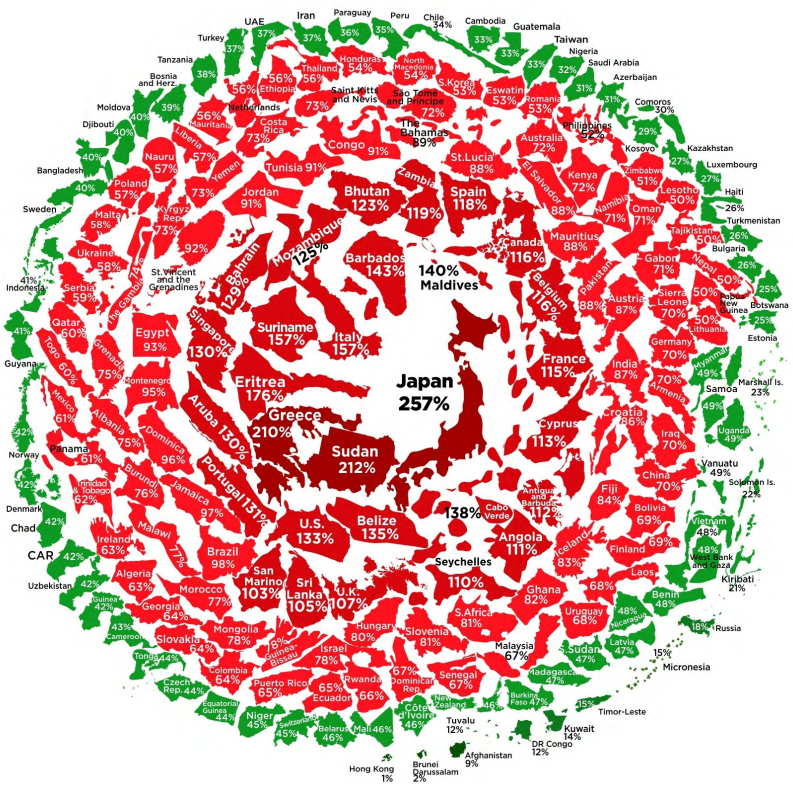
a. Exemple personale: sesiune interactivă

5.2.3 Povara globală a datoriei

Ca rezultat al sistemului fiat, guvernele din întreaga lume se regăsesc prinse într-o rețea uriașă de datorii, captivate de ceea ce se numește „spirala globală a datoriei”. Imaginează-ți un scenariu în care împrumuți mai mulți bani decât vei putea vreodată să rambursezi. Acest lucru se întâmplă la scară largă la nivel mondial. Guvernele, copleșite de datorii, au fost prinse într-un joc periculos de acumulare a mai multor datorii decât pot plăti vreodată. Este o poveste despre cheltuieli nesăbuite, împrumuturi și lipsă de previziune care acum împinge națiunile din întreaga lume la marginea dezastrului financiar.

În prezent, guvernul federal al SUA a adăugat o sumă uluitoare de 10 trilioane de dolari de datorie nouă din 2019. Datoria totală a crescut vertiginos de la aproximativ 23 trilioane de dolari în ultimul trimestru al anului 2019 la o sumă astronomică de 34 trilioane de dolari astăzi. Ritmul în care guvernele din întreaga lume generează datorii noi nu încetinește; de fapt, se accelerează. Anul 2023 a fost proiectat să fie cel mai generator an de datorii de la vremurile turbulente din 2021, marcate de pandemia Covid.

Starea datoriei guvernamentale la nivel mondial



Raportul datorie/PIB în 2021 (%)

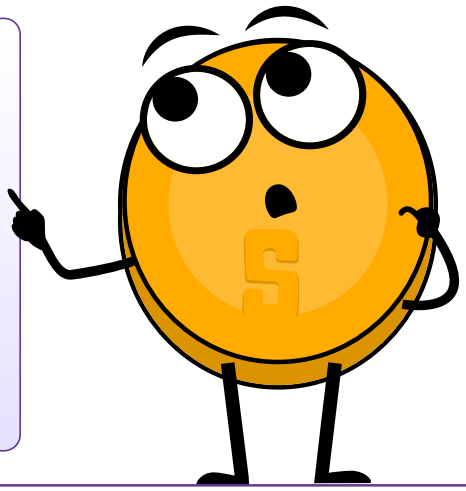
- 200% sau mai mult
- 100% — 199.9%
- 50% — 99.9%
- 20% — 49.9%
- 10% — 19.9%
- Mai puțin de 10%

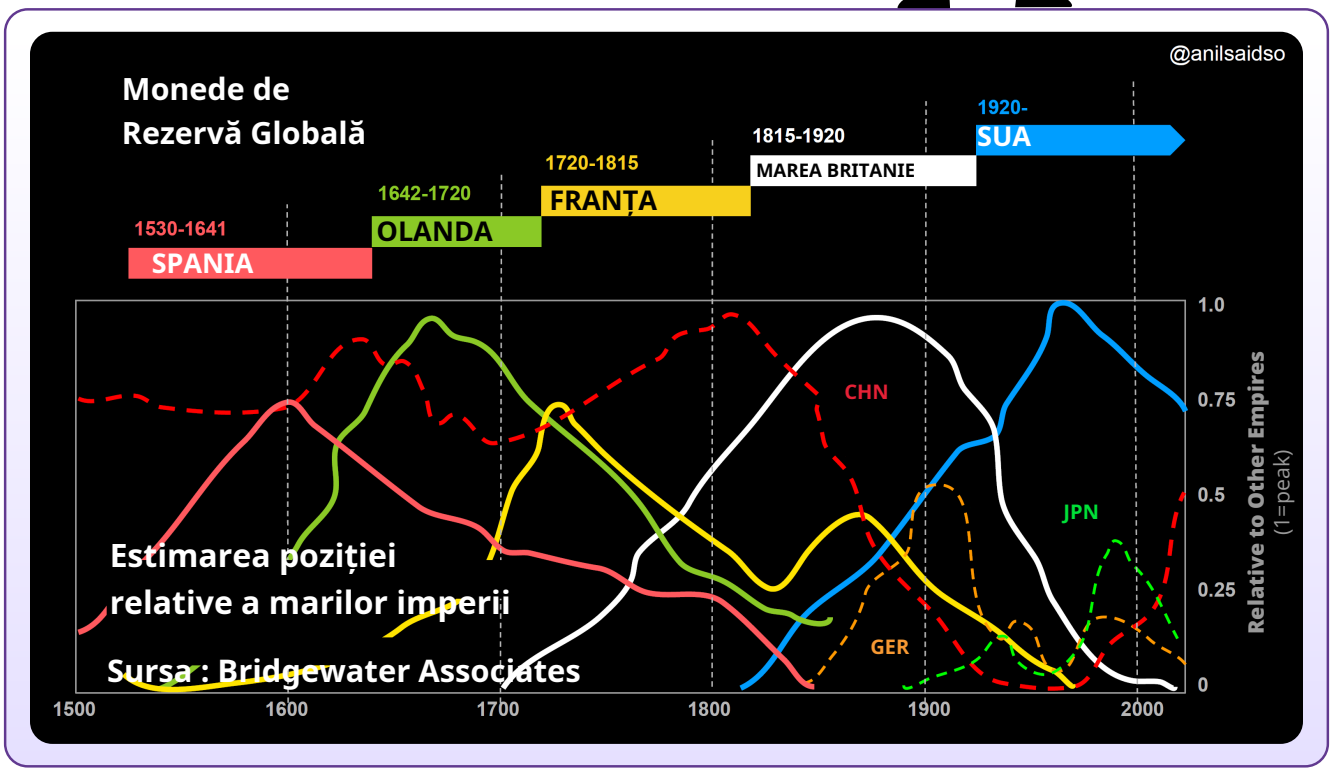
Deci, ce înseamnă acest lucru pentru indivizii și societățile care deja trebuie să facă față consecințelor sistemului fiat? Spirala datoriei în care sunt prinși este ca un bulgăre de zăpadă care se rostogolește la vale—devine tot mai mare și nu știm cum să o oprim.

Consecințele menționate anterior, de la inegalitatea bogăției la tulburări sociale, nu vor dispărea. Din contră, povara globală a datoriei a ajuns la un punct fără întoarcere, asigurând că lucrurile sunt sortite să se înrăutățească.

Cum Problemele Duc la Soluții

> Nu cred că vom mai avea vreodată bani buni până nu luăm acest lucru din mâinile guvernului... tot ce putem face este, pe o cale subtilă și ocolită, să introducem ceva ce ei nu pot opri.
>
> **Friedrich Hayek**





5.3 Cypherpunks și căutarea unei monede descentralizate

Am observat o capturare progresivă a banilor de către bănci și guverne de-a lungul istoriei, ceea ce a dus la sistemul fiat pe care îl cunoaștem astăzi și la consecințele sale dezastruoase pentru societate. Dar apariția noilor tehnologii precum criptarea și internetul a permis apariția unor idei noi, cum ar fi banii digitali independenți—liberi de intervenția guvernului, deschiși și accesibili tuturor. Să explorăm călătoria celor care conduc această mișcare revoluționară: cypherpunks.

5.3.1 Cypherpunks

> Calculatorul poate fi folosit ca un instrument pentru a elibera și proteja oamenii, mai degrabă decât pentru a-i controla.
>
> **Hal Finney**

A doua jumătate a secolului XX a fost martora unor descoperiri tehnologice majore, precum calculatorul și internetul, deschizând calea către o nouă eră digitală.

Un grup de oameni a descoperit că aceste inovații masive vor transforma în curând modul în care funcționează societatea. Ei au prevăzut atât potențialul, cât și pericolul calculatorului personal, fie ca un instrument care să ofere libertate individului, fie ca un instrument de control și supraveghere totală.

Acești oameni se numeau Cypherpunks. Ei au apărut ca un grup de activiști, criptografi, programatori și susținători ai confidențialității, care împărtășeau o viziune comună: urmărirea confidențialității, securității și a unui viitor digital descentralizat. Termenul "Cypherpunk" este o fuziune între "cypher", care se referă la codul criptografic, și "punk", reprezentând ethosul contracultural al rebeliunii.

Cypherpunks credeau în puterea criptografiei de a proteja libertățile individuale. Obiectivele lor includeau dezvoltarea de instrumente pentru securizarea comunicațiilor online, anonimizarea activităților pe internet și stabilirea monedelor digitale care să funcționeze dincolo de controlul autorităților centralizate.

Cypherpunks au înțeles consecințele sistemului fiat și au văzut amenințarea unui "viitor orwellian". Ei credeau că trebuie să se asigure că calculatorul personal și internetul vor deveni lucruri bune pentru umanitate, nu instrumente care să amplifice controlul statului asupra oamenilor săi.

DEFINIȚIA UNUI VIITOR ORWELLIAN:

Un viitor orwellian se referă la o viziune distopică inspirată de lucrările lui George Orwell. Termenul este asociat cu o societate de coșmar, totalitară, caracterizată prin control guvernamental opresiv, supraveghere extinsă, propagandă și manipularea informațiilor. Termenul "orwellian" descrie adesea un scenariu în care libertățile cetățenilor și autonomia individuală sunt sever restricționate, disidența este suprimată, iar realitatea este distorsionată pentru a servi interesele unui regim autoritar și puternic. Conceptul poartă numele lui George Orwell, care, în scrierile sale, a avertizat asupra pericolelor puterii guvernamentale necontrolate și erodării drepturilor fundamentale ale omului.

Cum Problemele Duc la Soluții

Figuri cheie din mișcarea Cypherpunk au inclus personalități precum Eric Hughes, Timothy C. May și John Gilmore. În 1992, Eric Hughes a scris "A Cypherpunk Manifesto”, prezentând principiile grupului. Manifestul sublinia importanța confidențialității, criptării și nevoia ca indivizii să preia controlul asupra identității lor digitale.

Urmărește acest videoclip și descoperă povestea Cypherpunks!

Una dintre cele mai notabile invenții ale Cypherpunks a fost crearea de instrumente și protocoale criptografice. În 1991, Phil Zimmermann a introdus PGP (Pretty Good Privacy), un software de criptare a emailurilor care a devenit un proiect emblematic. PGP le-a permis utilizatorilor să trimită mesaje criptate pe internet, fără ca nimeni altcineva să le poată decripta, cu excepția destinatarului. Înainte de aceasta, orice mesaj trimis pe internet putea fi interceptat și citit de alții, precum guvernele.

Cypherpunks au considerat că descoperirea criptării, împreună cu internetul și calculatorul, oferea o bază solidă pentru crearea de rețele descentralizate în spațiul digital, permițând indivizilor să comunice și să tranzacționeze pe internet în mod privat și fără interferența unei autorități centrale.

Cypherpunks au fost pe drumul cel bun pentru a promova un viitor mai luminos pentru umanitate, în care tehnologia să fie un instrument pentru maximizarea libertății, nu al controlului. Singurele piese lipsă erau o rețea descentralizată și o monedă digitală.

5.3.2 Sisteme Centralizate vs. Decentralizate

Sisteme Centralizate: Un Conducător, Multe Probleme

Într-un sistem centralizat, totul gravitează în jurul unei autorități principale, ca o clădire înaltă într-un oraș. Această autoritate controlează modul în care funcționează întregul sistem. Gândește-te la băncile tradiționale ca exemplu, unde un grup restrâns ia toate deciziile.

Exemplu real: În 2022, în timpul protestelor pașnice din Canada, băncile au înghețat conturile protestatarilor, arătând cum o autoritate centrală poate interveni și controla accesul la finanțe.

Probleme ale Sistemelor Centralizate:

- Punct central de eșec: Dacă ceva nu merge bine cu autoritatea centrală, întregul sistem poate prăbuși.
- Control: Un grup restrâns de la vârf deține tot controlul și puterea, luând adesea decizii care îi avantajează mai mult pe ei decât pe toți ceilalți.
- Ineficiență și intermediari: Ca ambuteiajele dintr-un oraș, sistemele centralizate pot deveni lente și costisitoare din cauza intermediarilor inutili.
- Lipsă de autonomie: Oamenii s-ar putea să nu poată lua propriile decizii financiare; totul este decis de autoritatea de la vârf.
- Cenzură și restricții: La fel ca unele zone dintr-un oraș care pot fi blocate, sistemele centralizate pot bloca sau limita accesul la anumite resurse financiare.
- Provocări de scalare: Când mai mulți oameni au nevoie de servicii financiare, sistemele centralizate pot avea dificultăți să țină pasul.
- Riscuri de securitate: Problemele cu autoritatea centrală pot pune întregul sistem în pericol de atacuri cibernetice.
- Lipsă de transparență și încredere: Mecanismele interne ale sistemelor centralizate pot fi greu de înțeles, ceea ce face dificilă încrederea oamenilor în ele.

Sisteme Decentralizate: Puterea aparține Oamenilor

Acum, gândește-te la un sistem descentralizat ca la o pădure mare. Fiecare copac reprezintă o parte separată, iar întreaga pădure reprezintă sistemul complet. Spre deosebire de un oraș cu un singur punct central, un sistem descentralizat este ca o pădure rezistentă care poate continua chiar dacă o parte are probleme.

- Exemplu real: Rețeaua Tor și browserul său creează un sistem descentralizat unde oamenii pot rămâne anonimi pe internet, iar rețeaua este dificil de oprit sau cenzurat.

Beneficii ale Sistemelor Decentralizate:

- Reziliență și fiabilitate sporite: Nu există un singur punct de eșec, ceea ce face sistemul puternic, chiar dacă apar unele probleme.
- Securitate crescută: Cu protecția/encripția potrivită, un sistem descentralizat rezistă mai bine controlului unei singure autorități.

- Suveranitate sporită: Oamenii au mai mult control asupra banilor, datelor și deciziilor lor.
- Transparență îmbunătățită: Toată lumea vede aceleași informații, ceea ce face sistemul mai de încredere.
- Natură permisivă și nelimitată: Oricine poate participa, ceea ce face sistemul financiar incluziv.
- Oportunități egale: Toți au șansa să contribuie și să aibă un cuvânt de spus.
- Confidențialitate sporită: Datele sunt distribuite între mai mulți participanți și sunt în mare parte pseudonime, ceea ce face sistemele descentralizate mai private.

Deși sistemele descentralizate au multe avantaje, luarea deciziilor împreună poate fi puțin dificilă. Este nevoie ca toți să colaboreze.

Schimbarea modului în care este exercitată puterea

În lumea sistemelor centralizate și descentralizate, totul ține de cine deține puterea. Sistemele centralizate dau puterea unui grup restrâns, iar cele descentralizate o distribuie, permițând tuturor să aibă un cuvânt. Această schimbare însemnă un viitor mai echitabil și mai democratic, unde oamenii influențează sistemul care le modelează viața.

5.3.3 Scurt Istoric al Monedelor Digitale

Unul dintre cele mai importante concepte discutate de Cypherpunks a fost banii digitali. Cypherpunks au realizat că statul și banii trebuie să fie separați pentru ca viitorul să fie în beneficiul binelui comun. Munca revoluționară a lui David Chaum privind protocoalele criptografice pentru tranzacții sigure și private a pus bazele. Dezavantajul era că acest protocol necesita o autoritate centrală pentru a funcționa eficient, ceea ce ridica îngrijorări legate de un singur punct de eșec și de potențiala cenzură.

În anii ce au urmat, mai mulți Cypherpunks au încercat să îmbunătățească ideile unii altora pentru a crea o soluție viabilă pentru o monedă digitală liberă de controlul guvernului. Tabelul de mai jos descrie câteva inovații cheie dezvoltate de Cypherpunks în căutarea lor de a crea bani digitali:

Nume și Dată	Descriere	Limitări
E-Cash (1982)	E-Cash al lui David Chaum a fost un concept timpuriu de bani electronici, axat pe confidențialitate prin tehnici criptografice.	Necesita o autoritate centrală, ridicând îngrijorări privind un singur punct de eșec și potențiala cenzură.
DigiCash (1990)	DigiCash, fondată de David Chaum, a urmărit crearea unei forme digitale de monedă cu accent pe confidențialitate.	Modelul centralizat a contribuit la falimentul său în 1998.

B-money (1996)	B-Money, propus de Wei Dai, a fost o propunere teoretică pentru un sistem anonim, distribuit de bani electronici.	Necesita o autoritate centrală, ceea ce ridică îngrijorări legate de un singur punct de eșec și de cenzură.
Hashcash (1998)	HashCash, dezvoltat de Adam Back, a fost un sistem proof-of-work conceput pentru a limita spam-ul pe email și atacurile denial-of-service.	Nu a abordat direct problema double-spending asociată monedelor digitale.
Bit Gold (1998)	Bit Gold, propus de Nick Szabo, a descris un sistem descentralizat de monedă digitală cu elemente de proof-of-work.	Nu a fost niciodată implementat, a rămas un concept teoretic.
e-Gold (2004)	e-Gold a fost o monedă digitală centralizată susținută de aur fizic, permițând utilizatorilor să cumpărați și să transferați unități e-Gold.	Problemele legale au dus la închiderea sa în 2009, evidențiind provocările monedelor centralizate.

Despite the Cypherpunks' numerous attempts made over the decades to create a digital currency free from the control of any one group or government, their efforts faced practical challenges and couldn't fully materialize in the real world. The Cypherpunks concluded that it was not easy to build a digital form of cash that was secure, scalable, and had the potential to become widely adopted.

However, the story takes a turn when one individual, learning from the Cypherpunks' lessons elevated the concept of a decentralized digital currency to new heights. In the following chapters, we'll explore how this person's contribution, building upon 40 years of prior work, ultimately led to the creation of a functional system.

Chapter #6

An Introduction to Bitcoin

6.0 Satoshi Nakamoto and the Creation of Bitcoin

6.1 How Does Bitcoin Work?

6.1.1 The Nakamoto Consensus Mechanism

6.1.2 The Players of the Game

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

6.2 Bitcoin as Sound Digital Money

6.2.1 Introduction

6.2.2 Bitcoin's Features

Activity: Class Discussion - Is Bitcoin Sound Money?

6.2.3 Embracing Personal Responsibility

Caietul elevului

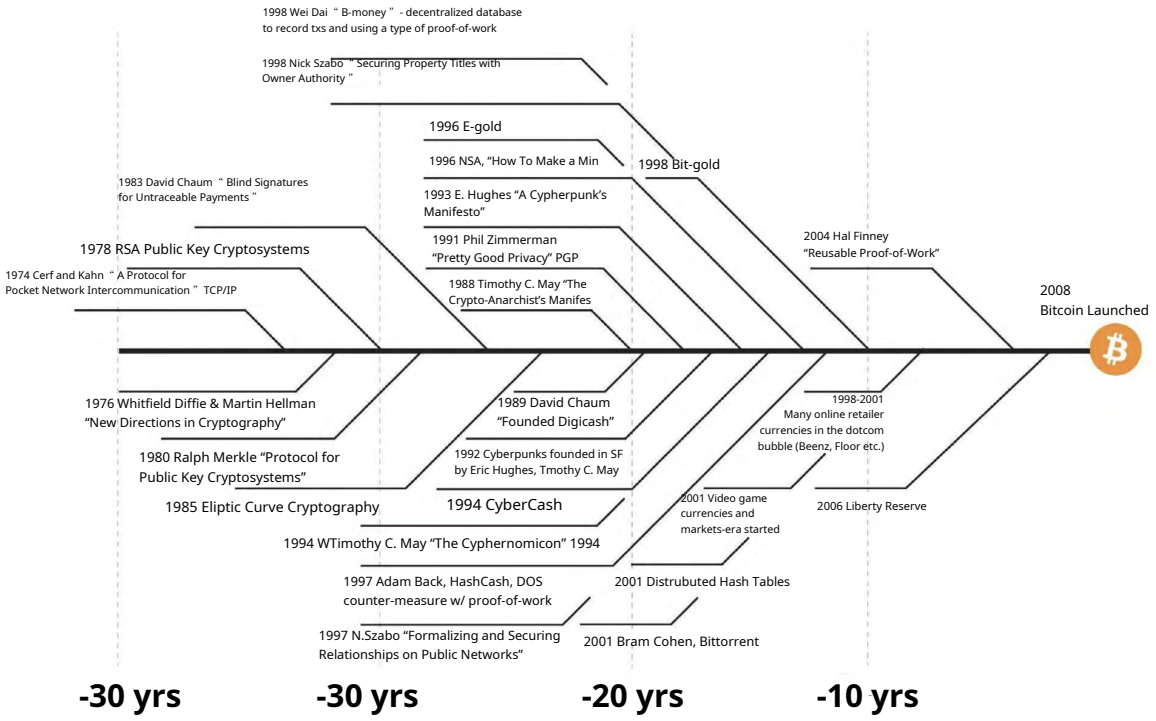
Limba Română | 2025

An Introduction to Bitcoin

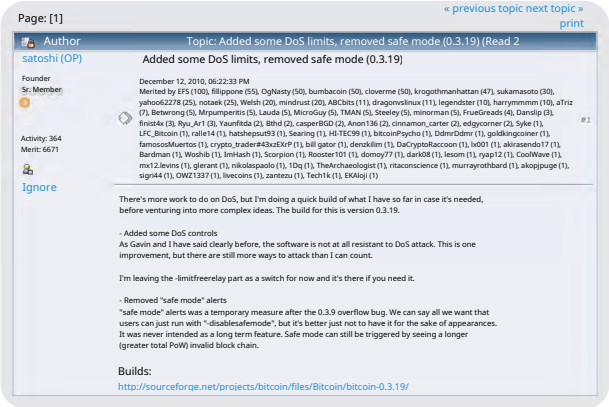
6.0 Satoshi Nakamoto and the Creation of Bitcoin

> A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990s. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized non-trust-based system.
>
> **Satoshi Nakamoto**

Bitcoin prehistory: — It's the result of 40 years of research, development and demand



As you read in the previous chapter, multiple Cypherpunks attempted to create an alternative money system. This chapter continues the story of one of them: a visionary mind by the name of "Satoshi Nakamoto." This anonymous person (man, woman, or group), long before Bitcoin, was one of the cryptography enthusiasts like computer scientists and hackers, engaging in discussions to find practical solutions to replace the fiat system.

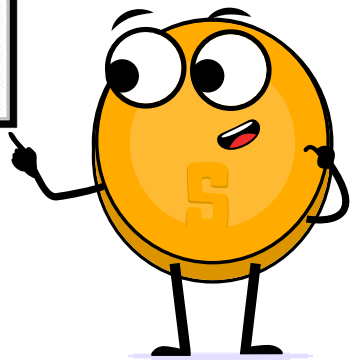


Chapter #6

Primul Meu Bitcoin

In October 2008, Nakamoto unveiled a groundbreaking whitepaper titled, “Bitcoin: A Peer-to-Peer Electronic Cash System” on a cryptography mailing list. This document laid the foundation for a decentralized peer-to-peer protocol, designed to facilitate secure online transactions without the need for intermediaries.

Nakamoto's vision was clear: to create a purely peer-to-peer version of electronic cash, free from the control of powerful governments and financial institutions.



Fast forward to January 3, 2009, when Nakamoto mined the first Bitcoin block known as the "genesis block." This marked the official launch of the Bitcoin network, a new money system built on trust and security through a decentralized ledger. In the months and years that followed, more and more enthusiasts started to join and contribute to the idea.

Bitcoin Genesis Block

Raw Hex Version

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

In 2011, after the Bitcoin network proved it could operate successfully without the need of its influential creator, Nakamoto sent an email to a fellow Bitcoin developer, announcing they were removing themselves from the Bitcoin scene and giving its future away to other “good hands” that shared their vision.

Although Nakamoto’s identity remains a mystery until this very day, their goal for creating Bitcoin was never a mystery. In essence, Nakamoto created it to take the power away from the few and give it back to the many by creating an alternative in the form of a decentralized, open-source, transparent money system, separating money from the state. Creating Bitcoin was Nakamoto’s response to the 2008 financial crisis that hurt regular people worldwide while enriching the elite class — again. Bitcoin was Nakamoto’s answer to the corruption and fragility of the fiat system. Nakamoto set the foundation for a new revolution and walked away from it instead of claiming credit.

In the years that followed, Bitcoin started to grow quickly and emerged as a symbol of hope, empowerment, and resilience, challenging the fiat system and providing a secure, censorship-resistant means of financial transactions. Bitcoin is an open-source protocol, meaning that no one has the power to own or control it. Its design is public and open for anyone to participate.

Today, Nakamoto's dream of a borderless, transparent, and secure financial system lives on, empowering the global freedom revolution we are witnessing today. Every day, ordinary people are opting out of the fiat system and into the world of Bitcoin. Bitcoin hubs — the so-called Bitcoin circular economies — have been launched by freedom enthusiasts in regions all over the world. Even entire countries looking for an alternative path, like El Salvador, are starting to adopt Bitcoin in their own ways.

6.1 How Does Bitcoin Work?

6.1.1 The Nakamoto Consensus Mechanism

So, how does Bitcoin work? Bitcoin has lots of features, and the rabbit hole goes deep — very deep. Fortunately, if you enter the Bitcoin world for the first time, you do not have to perfectly understand how it works to start using it.

The same counts for using the internet: most people do not know how the TCP/IP protocol works, yet they send emails and, messages, and post content on their social media accounts every day. The same goes for driving a car — most people do not know exactly how a car works, yet they do know how to drive.

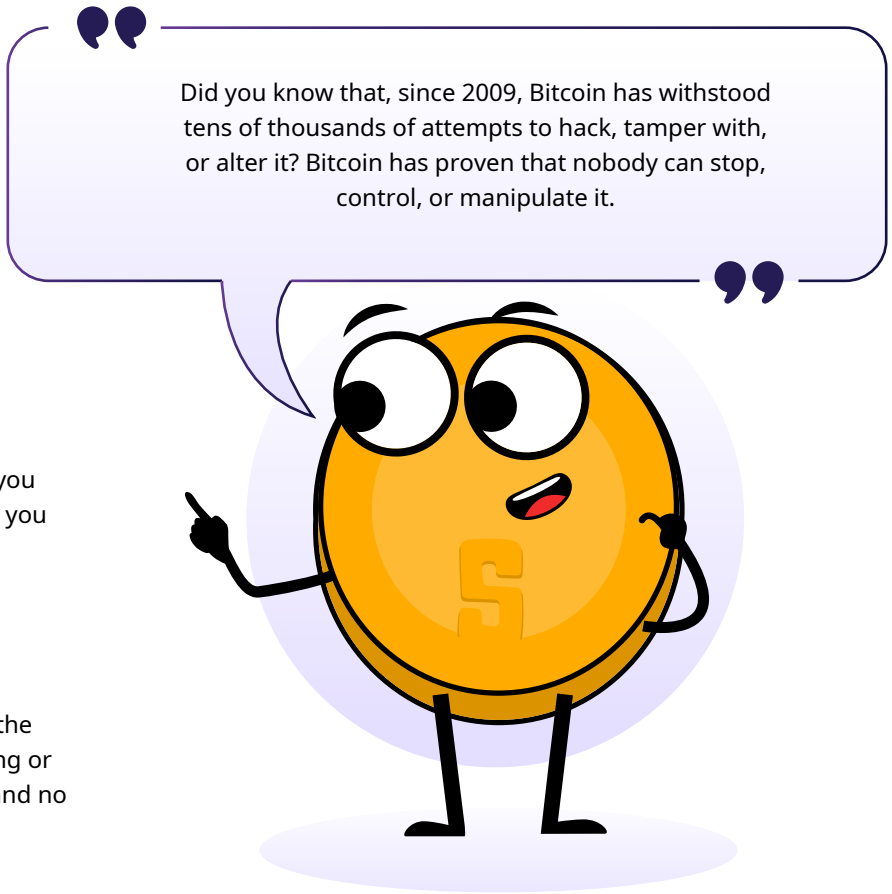
However, Bitcoin is not yet widely adopted. It is still a pretty new technology, like the internet was during the 90s. Because of this, it can be helpful to grasp the basics of Bitcoin in a simple, less technical way.

Chapter #6

The key idea behind how Bitcoin operates can be condensed into one sentence: Bitcoin is an agreement among people online. You can think about it like playing a board game with friends. With a game like Monopoly, you are in agreement with the other players about specific rules. One of the rules of Monopoly is that only special “Monopoly bills” are to be accepted. If James, (one of the players), went against the rules by using toilet paper to buy a house instead of Monopoly bills, the other players would tell James he is a cheater and would simply stop playing with him. In short, to play the game, you have a consensus on a set of rules with each other and you do not drift away from those rules, otherwise you will be rejected.

This is essentially how Bitcoin works. Bitcoin is a network of people that agree on the same set of rules. These rules are mathematically bound, written in computer code, and accepted directly by everyone who runs the Bitcoin software. The rules of Bitcoin apply to all participants equally, which means that everyone either follows the rules of the game or cannot play because the network will reject them.

For example, one of the rules of Bitcoin is, "There will never be more than 21 million bitcoins." If someone wanted to create a million extra bitcoins for themselves, it would be of no use to them because they would automatically be identified and rejected by everyone else. This is what makes Bitcoin so robust.



It does not matter who you are or where you come from; if you enter the Bitcoin world, you need to play by the same set of rules as everyone else.

This also applies to all the people and entities with an enormous amount of control and influence in the fiat world. In the Bitcoin world, there is no room for cheating or sabotage — everyone is treated equally, and no one can change that.

6.1.2 The Players of the Game

To better understand the decentralization of Bitcoin, we need to dive deeper into the different roles within the network. In the Bitcoin world, various participants play distinct yet harmonious roles, contributing to the network's seamless functioning.

1. Miners: The Architects of Security

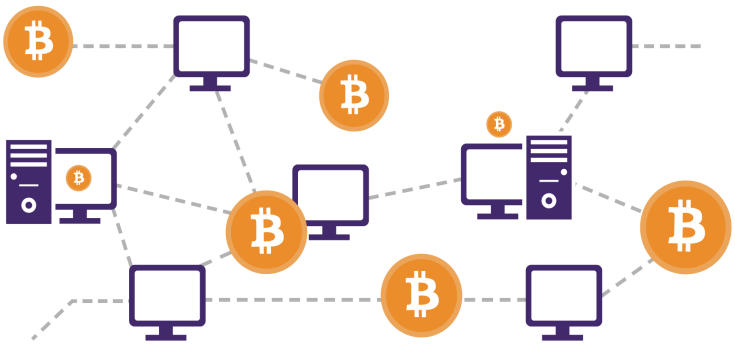
Miners are the backbone of Bitcoin. These are people or groups of people who work behind the scenes to maintain and secure the network through a mechanism called Proof-of-Work (PoW). These players are armed with special computers that have heavy computational power. They make their hardware available to the Bitcoin network, competing with each other in a worldwide lottery to add new blocks of transactions to Bitcoin's decentralized ledger (the blockchain). Their commitment ensures the the ledger's immutability and guards against malicious attacks.

Mining's decentralized nature allows anyone with sufficient computing resources to participate. Because of their hard work, the miners who solve the puzzle the quickest are rewarded in the form of bitcoins.

Bitcoin miners are distributed all over the world, safeguarding the network against centralization and ensuring Bitcoin's security stays robust and distributed.

2. Nodes: Gatekeepers of Validation

Bitcoin nodes are ordinary people who live across the planet. These participants serve as the Bitcoin network's gatekeepers by running Bitcoin software on their small computers on which they maintain a copy of the entire ledger. Nodes validate transactions and ensure that all participants adhere to the consensus rules.



By distributing the responsibility of validation across a network of nodes, Bitcoin remains resilient against attacks and maintains its trustless nature. Nodes play a crucial role in upholding the integrity of the ledger, contributing to the Bitcoin's decentralization ethos.

3. Users: Empowered Participants

Users — the lifeblood of the Bitcoin network — are individuals who engage in transactions. You can think of users as regular people who just live their lives but have also empowered themselves by integrating Bitcoin. For example, some users save their money in bitcoins while others, like citizens of El Salvador, use it as money to buy groceries and receive their salary in bitcoin.

Bitcoin empowers users by eliminating the need for intermediaries like banks and governments, allowing for direct peer-to-peer transactions. This also means that users have full control over their money, and transactions.

4. Developers and Projects: Architects of Innovation

The monetary system of the future won't build itself on its own, nor will it be globally adopted in an ethically correct way without effort. That’s where Bitcoin developers and projects come into play.

Developers wield their technical expertise to enhance and innovate the Bitcoin protocol. These individuals contribute code, propose improvements, and address vulnerabilities, ensuring the network evolves in response to all types of challenges. Bitcoin's open-source nature invites collaboration, allowing developers worldwide to contribute to its growth.

The beauty of this decentralized development prevents a single entity from monopolizing control over the protocol. This happens through a consensus-driven process. Developers propose ideas and changes, and only those with the best ideas who are aligned with the broader vision for a better world receive support from the community, empowering Bitcoin's transparent and democratic evolution until it’s ready for 8 billion people.

Bitcoin projects involve diverse groups, from mission-driven nonprofits and corporations to groups and individuals that create valuable content. These people work together on a specific goal or focus within the bigger Bitcoin mission toward collective freedom.

Bitcoin projects play a crucial role in shaping and promoting the adoption of Bitcoin, working toward a future that prioritizes the empowerment and freedom of the human race.

4. Developers and Projects: Architects of Innovation

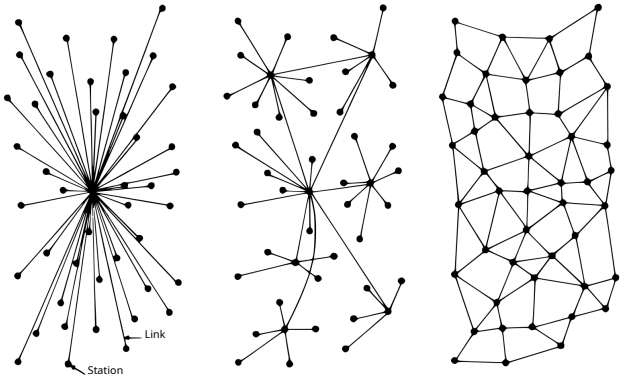
Bitcoin's decentralization can be thought of as a synergetic musical orchestra, a balancing act where all the different musicians make the most beautiful music together. There is no boss in the Bitcoin network; instead, miners, nodes, users, developers, and projects perform their roles with autonomy and collaboration.

The decentralized ledger, maintained by nodes, guarantees transparency, while the proof-of-work mechanism provides security and deters centralization in mining. Users experience financial sovereignty and empowerment free from the control of the fiat system. Developers, guided by consensus, ensure the protocol adapts to meet the evolving needs of humanity. Bitcoin projects, in their own unique ways, contribute to the broader mission of collective freedom.

An Introduction to Bitcoin

As you can see, every participant plays a vital role in shaping Bitcoin's adoption and empowering humanity. Each participant in this decentralized orchestra contributes to the resilience and longevity of Bitcoin, creating a trust-free, borderless, and empowering ecosystem.

In summary, the symphony of decentralization in Bitcoin resonates as a testament to Satoshi Nakamoto's vision and the immense passion of a global community seeking freedom and empowerment.



CENTRALIZED (A) | CENTRALIZED (B) | DISTRIBUTED (C)

Class Exercise — Consensus Building in a Peer-to-Peer Network

Objective

To understand how consensus is achieved in a group and learn about cryptography and the consensus layer of Bitcoin.

Materials

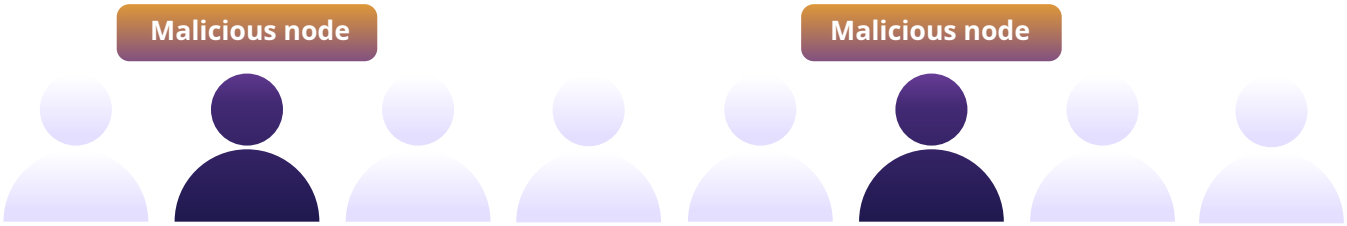
Message with encrypted and unencrypted instructions for actions ("attack" or "do not attack").

Activity Preparation

The teacher will select a group of three or four students before class to be malicious nodes in the following activity. The teacher will assign these malicious nodes a cryptographic puzzle as homework in the previous class.

Exercise Steps:

1. The teacher will select one student in the group as an “originator” who will receive a message on a piece of paper that says "ATTACK" and a series of numbers that says, "4-16-14-21-1-21-21-1-3-11-”.
2. The students will form a circle in the designated space, ensuring the selected students who will be malicious nodes are separated to improve the effectiveness of the lesson.



3. Once the group has formed a circle, the originator will pass the note to the individual to the right side of the circle.
4. After everyone has read the message, the originator will give the signal to the group by saying “now,” and the group will react to the message simultaneously. If the message reads “ATTACK,” then all participants will take a step forward.
5. After the initial reaction, some students (those who received the encrypted message and interpreted it correctly) will remain still, while the rest will follow the original instruction, revealing a lack of consensus.

Conclusion:

Discuss why consensus was not achieved, introducing the concept of the Byzantine Generals' Problem, how it relates to the need for a common goal, and later discussing how Bitcoin provides a solution to this problem.

An Introduction to Bitcoin

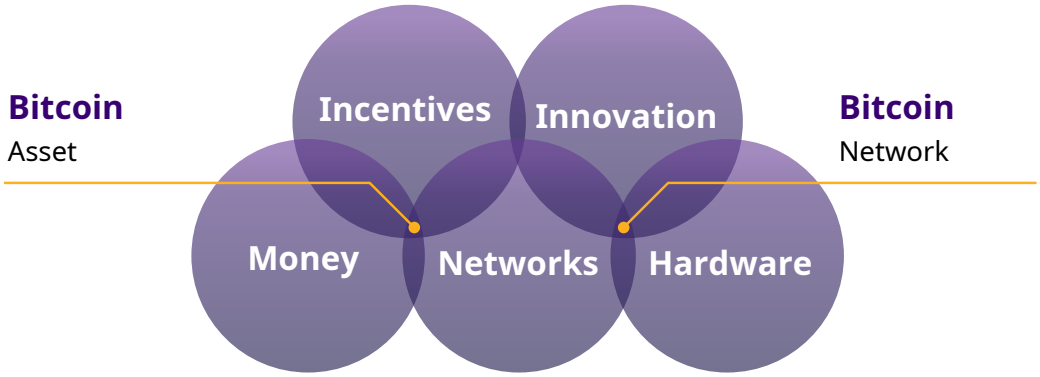
6.2 Bitcoin as Sound Digital Money

6.2.1 Introduction

Activity:

Watch 1.5 min video, “What Is Bitcoin?

In simple terms, Bitcoin is money. Bitcoin is not an investment but rather a safe, empowering way of saving your hard-earned money.
Having bitcoins won’t make you rich because it won’t give you a return of more bitcoins. Its value, measured against a fiat currency, does go up, but this is only because of its growing adoption and the devaluation of fiat currencies.



Bitcoin is a new form of money; it is, “The Internet of Money," which means that it is open for anyone to join and start exchanging value with other users. Even the most isolated and poor communities in the world finally have access to a monetary system. Just like everyone who has a phone and an internet connection can use a search engine, Bitcoin makes it possible for everyone with a phone and internet connection to access a new, global monetary system.

Faster, Cheaper Payments

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

Financial Inclusion

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

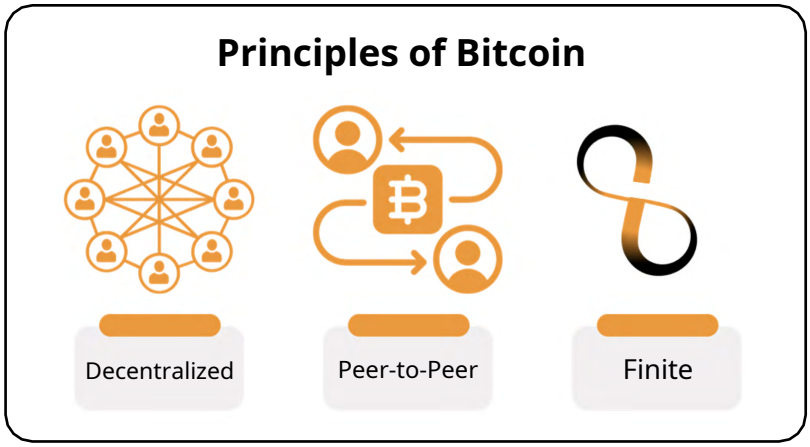
Increased Privacy

Bitcoin transactions are public but your identity is not.

Bitcoin is completely digital and borderless. It doesn't matter where you are located because it lives on computers and smartphones from all over the world. Lots of users worldwide run the Bitcoin software and a copy of its ledger.

This software and record of all transactions has a very low chance of disappearing as there are countless copies of it. To shut it down, you would need to shut down the entire internet, forever, which is extremely unlikely to happen.

Finally, Bitcoin is scarce, which means that the number of bitcoin tokens that can exist is absolutely limited. No one can counterfeit Bitcoin — not even the most powerful governments and financial institutions.



6.2.2 Bitcoin's Features

The Evolution of Sound Money

As you learned in Chapter 2, the lifecycle of sound money progresses through three stages to receive general acceptance from society: from being a store of value to becoming a medium of exchange and, finally, a unit of account.

The first stage of money, a store of value, is when a currency starts gaining trust as a stable (or appreciating) asset over time. People who recognize this early seek to protect their wealth by storing it in this form of money, especially during a time of geopolitical and macroeconomic uncertainties.

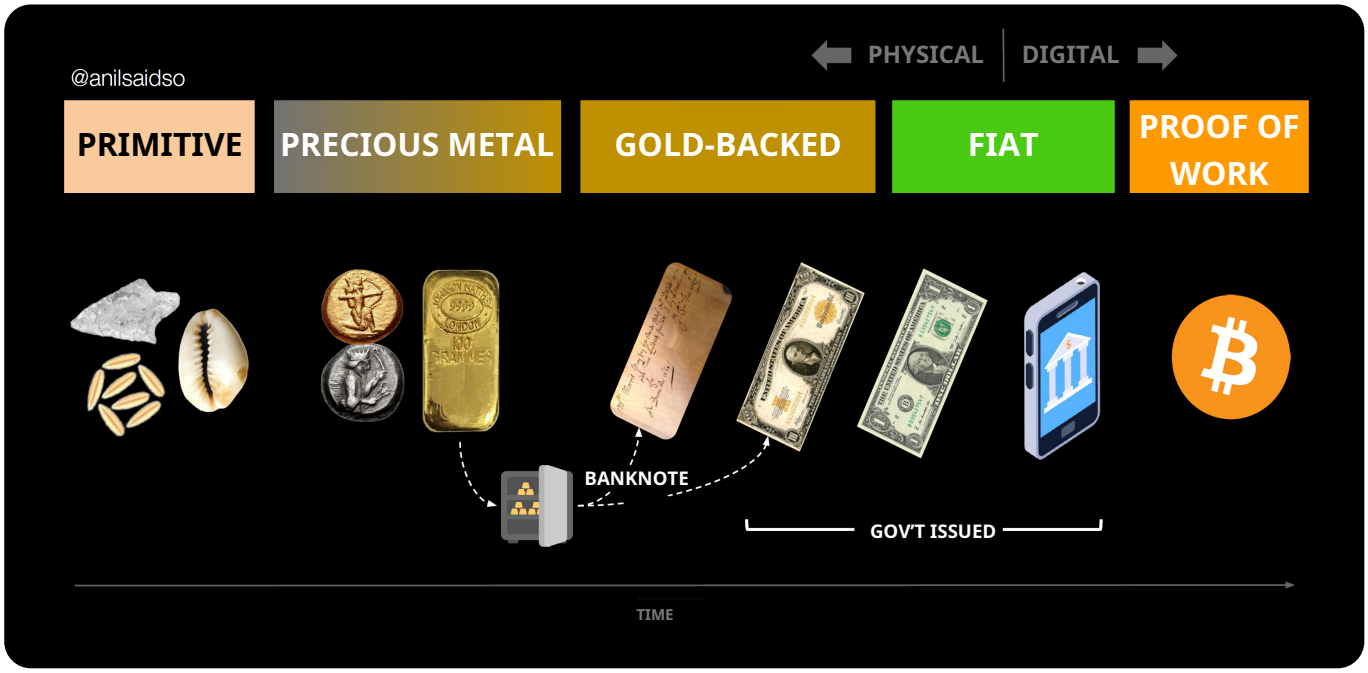
Some groups, like media outlets, call Bitcoin a form of "digital gold." This is because Bitcoin firmly established itself as a store of value during the past decade. Every day, more and more people start to view Bitcoin as a hedge against inflation, like gold was historically.

The next stage is when confidence in a currency's stability solidifies. This is when the currency transitions into a medium of exchange, facilitating transactions in people's daily lives. During this stage, the currency starts to become widely accepted for the exchange of goods and services.

Bitcoin is progressively moving toward becoming a medium of exchange. With growing merchant acceptance and the development of the protocol, Bitcoin transactions are becoming more efficient and commonplace in daily commerce. One example of this is El Salvador, where Bitcoin is officially recognized as legal tender. Each day, more and more ordinary citizens and businesses are using Bitcoin as a medium of exchange.

In the final stage, a currency achieves the status of a unit of account, serving as a common measure for pricing goods and services. This is the stage in which it becomes the standard metric against which all other values are measured.

The journey toward becoming a unit of account is a more extended (long-term) process. The world currently measures goods and services only in fiat currencies, therefore, Bitcoin needs broader adoption and integration into various financial systems. However, the foundation is already laid as businesses and individuals begin to consider and denominate values in Bitcoin.



As you can see, Bitcoin is well on its way in this evolutionary cycle of sound money. When Bitcoin becomes fully integrated into the global financial system, it could become a standard unit of account, reshaping the entire global monetary system.

Properties of Money

As you learned in Chapter 2, over time, humanity has figured out that real sound money must possess certain properties to be effective. These properties are durability, divisibility, portability, acceptability, scarcity, and fungibility.

Let's see if Bitcoin passes the test.

Durability: Bitcoin is purely digital and thus completely durable.

Divisibility:

For comparison, the fiat currency USD can be divided to the cent (.01). Bitcoin can be divided into what is known as a satoshi or sat (.00000001). And because of Bitcoin's digital character, it can be divided even more in the future if humanity needs it. Bitcoin is currently the most divisible monetary asset in the world.

Portability:

In April 2020, $1.1 billion was transferred in just a few minutes, and it only cost 68 cents. No other way of paying can move that much money at such a low cost so quickly, and all on its own. This is what makes Bitcoin the most easily movable form of money in the world.

Acceptability:

Bitcoin is still in its early stages of becoming a medium of exchange, and compared to fiat currencies, acceptability is currently low.

Scarcity:

There will only ever be 21 million bitcoins in existence. By code, it is impossible for this amount to ever increase, which means that Bitcoin is not only scarce but the scarcest monetary asset in the world.

Fungibility:

Each unit of bitcoin is the same as any other unit and can be interchanged and transacted over the Bitcoin protocol on a like-kind basis, which makes it a fungible currency.

Bitcoin vs. Gold vs. US Dollar

Properties of Money	Gold	Fiat	Bitcoin
Durability	Moderate	Moderate	High
Portability	Moderate	High	High
Divisibility	Moderate	Moderate	High
Fungibility	High	High	High
Scarcity	Moderate	Low	High
Verifiable	Moderate	Moderate	High
Established History	High	Moderate	Low
Censorship Resistant	Moderate	Moderate	High
Smart/Programmable	Low	Moderate	High

"Bitcoin vs Gold vs US Dollar" Bitcoin Magazine, https://bitcoinmagazine.com

Bitcoin is a type of smart money that's programmable, can't be taken away, and has all the qualities that make it great for saving and easy for merchants who want fast transactions.

Since it's a transparent digital ledger, Bitcoin can be super efficient in catching fraud and figuring out risks in its services. It has the good aspects of gold, such as there only being a limited amount of it, but it also has the benefits of fiat currencies because you can divide it and carry it around easily. Plus, it brings in new features that work well in our digital world.

What do you think? Bitcoin is not yet widely recognized and adopted, but is it sound money?

Activity: Class discussion - Is Bitcoin Sound Money?

Now that we have discussed Bitcoin in greater detail, let's look at our money comparison table from Chapter 2 again and see how Bitcoin compares with other forms of money:

"Bitcoin will become obsolete"	Cows	Cigarettes	Diamonds	Euros	Bitcoin
Portable					
Portable					
Uniform					
Acceptable					
Scarce					
Divisible					
Total					

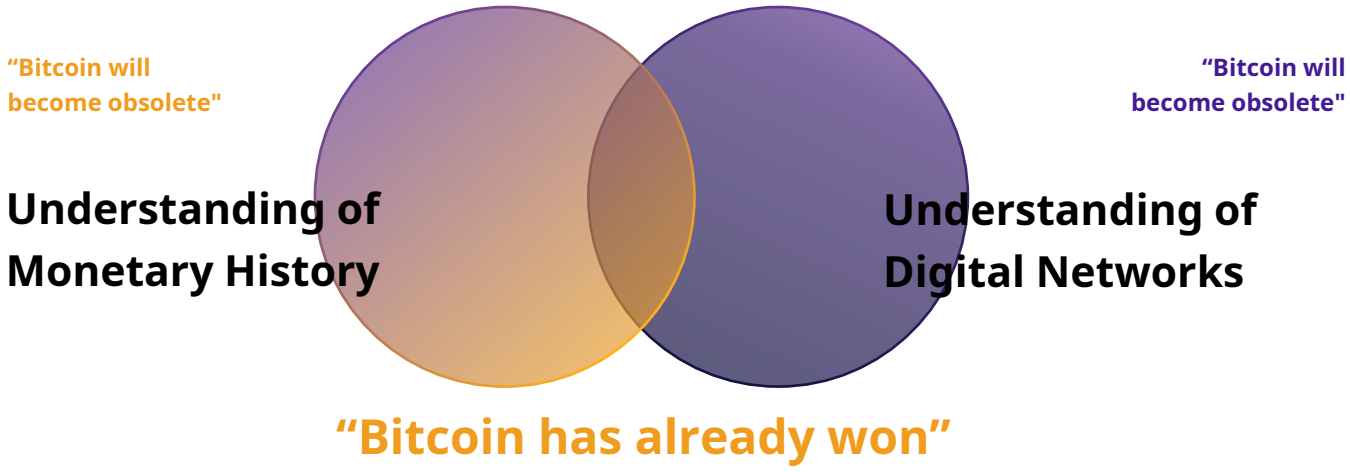
6.2.3 Embracing Personal Responsibility

> The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.
>
> **Andreas M. Antonopoulos**

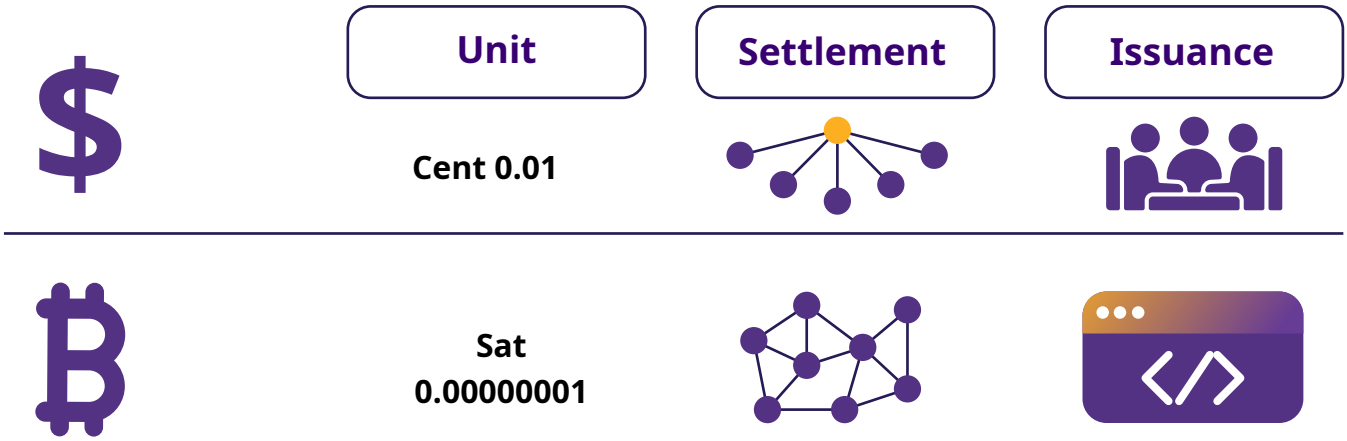
An Introduction to Bitcoin

In the fiat world, people rely on governments, banks, and established payment providers. The heads of these (financial) institutions set the rules of the network, and the participants, mostly ordinary citizens, must comply with these rules. It doesn't matter where you live - there are always a set of standard procedures that instruct you on what to do and how to do it. Over time, this led to a cycle of hardship, particularly for families that struggle with the increasing challenges of daily life.

Because of this system, people are accustomed to putting the responsibility for their finances in the hands of others. For example, most people rely on someone else to help them, especially when something goes wrong (like losing access to your bank account).



As you know, the monetary system of Bitcoin is very different. Bitcoin operates in a way, and rulers have been replaced by an autonomous system of rules. There is no dictator or leader, which also means that no one will dictate to you what you need to do. If you want the newfound freedom and empowerment of Bitcoin, you will need to learn how it works and integrate the technology in a way that works for you personally.



With Bitcoin, you are fully in control of your funds, but with this additional control comes increased responsibility. For example, losing access to your bitcoins by losing your keys to your digital wallet means you have lost your savings — permanently. There's no customer service hotline to call or someone else to turn to - when there is a problem, you need to take care of it yourself.

Fortunately, this will not happen to those who decide to take full responsibility over their own lives. Using Bitcoin is not inherently complicated; it’s just a new concept. Any discomfort arises because it's unfamiliar, but if you are willing to learn how to use Bitcoin and fully embrace the responsibility of safeguarding your wealth, Bitcoin becomes an empowering tool — you are in control, and no one can seize your wealth.

In summary, the key lies in action, understanding Bitcoin's workings, and implementing it according to your unique needs and life philosophy. Next, we’ll begin to use bitcoins by setting up a Bitcoin wallet, sending and receiving our first transactions, and reviewing security best practices.

Chapter #7

How to Use Bitcoin

7.0 Introduction

7.1 Acquiring and Exchanging Bitcoin

7.1.1 P2P: Physical

7.1.2 P2P: Online

7.1.3 Centralized Exchanges

7.2 An Introduction to Bitcoin Wallets

7.2.1 Self-Custodial vs. Custodial Wallets

7.2.2 Different Types of Bitcoin Wallets

7.3.3 Open Source vs. Closed Source

Activity: Class Evaluation of Bitcoin Wallets

7.3 Setting Up a Mobile Bitcoin Wallet

Activity: Setting Up/Recovering a Bitcoin Wallet

7.4 Receiving and Sending Transactions

Activity: Bitcoin Transactions in Action

7.5 Saving in Bitcoin

7.6 Don’t Trust, Verify

Caietul elevului

Limba Română | 2025

How to Use Bitcoin

7.0 Introduction

> Why would anyone trust nerd money vs. central bank money? Nerds brought you the internet. Banks brought you the Great Depression.
>
> **Andreas M. Antonopoulos**

Now that we have a better understanding of what Bitcoin is and its purpose, it's time to learn how to use it practically. In this chapter, we'll guide you through the process of acquiring bitcoins step-by-step, explore the various types of wallets available, help you set up your own Bitcoin wallet, and even practice sending and tracking a bitcoin transaction on the network. It's time to turn your understanding into action!

7.1 Acquiring and Exchanging Bitcoin

There are many ways to acquire bitcoin. For example, you can:

- Get paid in bitcoins in exchange for your work and pay for other people's products and services with bitcoins (more on that in Chapter 8)
- Mine bitcoins (more on that in Chapter 9)
- Exchange your fiat currency for bitcoins or exchange your bitcoins for fiat currency in person.
- Exchange your fiat currency for bitcoins or exchange your bitcoins for fiat currency online.

Below, we'll explore exchanging fiat currency for bitcoins and vice versa, both through in-person transactions and online methods, as they are the most common options.

7.1.1 Peer-to-Peer: In Person

Engaging in peer-to-peer (P2P) transactions to acquire and sell bitcoin involves directly exchanging your fiat currency (or any other goods or services) for bitcoins with another individual, eliminating the need for a bank or other party to be involved in the transaction.

Both parties mutually determine the exchange amount and rate. The buyer provides the cash, the seller transfers the bitcoins, and the transaction concludes. While it's easier to do P2P exchanges physically by meeting with the other individual directly in the real world, you can also do so from virtually anywhere thanks to the internet. Additionally, exchanging bitcoins for fiat currency follows a similar process in reverse.

7.1.2 Peer-to-Peer: Online

Enter P2P platforms, where Bitcoin buyers and sellers meet in cyber space to conduct transactions without any intermediaries, directly on the internet.
With such platforms, you don't have to trust anyone with your information or money; you can meet other peers and trade with them directly.

On most P2P platforms, peers have to escrow some of the funds to ensure they will comply with their part of the deal. Escrow means putting the money in a safe place that the platform controls until both parties do what they promised. It's like a trusted friend holding onto your stuff until everyone keeps their word.

7.1.3 Centralized Exchanges

Using centralized exchanges may be the easiest way to acquire and sell bitcoins but it also involves significant trade-offs. Centralized exchanges are companies that allow clients to buy and sell bitcoins directly through them. However, this convenience comes at a cost.

Centralized Exchanges and Their Trade-Offs

It's important to note that when buying bitcoins through a centralized exchange, you are often required to provide personal information and verify your identity. This creates a risk of identity theft and exposes your personal information to potential threats. Additionally, centralized exchanges hold your bitcoins for you, which means you are not in control of your money until you withdraw it from them.

To add to these concerns, centralized exchanges can misappropriate users' funds or lend more bitcoins than they have in reserves until they collapse. Yes, just like banks! However, in the Bitcoin world, there is no central bank to bail out fraudulent banks by printing more currency because you can't print more bitcoins!

7.2 An Introduction to Bitcoin Wallets

Unlike physical money, bitcoins are not actually present in a Bitcoin wallet. Instead, they live on the distributed ledger that the Bitcoin network constantly verifies and secures. So, how can you own bitcoins?

You have ownership of your bitcoins only when you own the private keys allowing you to sign transactions and transfer ownership of your bitcoins to someone else. This is the act of sending bitcoins.

With that in mind, let's take a look at two concepts we describe when using the term "wallet":

- A master private key (like a password) from which you can generate public keys that you can share with others to receive and send bitcoins.
- The mobile or desktop interface from which you can interact with the Bitcoin network to retrieve your bitcoin balance, send and receive transactions, and broadcast them to the network. Different types of wallets, along with their benefits and tradeoffs, will be described in the next section.

7.2.2 Different Types of Bitcoin Wallets

Before detailing the different types of Bitcoin wallets and their characteristics, let's make an important distinction between self-custodial and custodial wallets, as shown in the table below. You can see the benefits and risks of using each wallet type and who controls the bitcoins in each case. Self-custodial means the user holds the private keys, which means they are in true possession of their bitcoins, while in the second type, a third party, holds their bitcoins.

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, so 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 private key, giving them full access to move any bitcoin that wallet controls 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 bitcoins secure.
- Self-custody ensures that third parties cannot confiscate your bitcoins without your consent.
- Self-custody gives peace of mind in times of uncertainty, knowing your bitcoins are 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 self-custodial or a custodial wallet. This table shows the differences with the 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 a recovery phrase and at least one private key	Store the recovery phrase in a secure location	Start using the wallet to receive and send bitcoins
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 bitcoins

NOT YOUR KEYS

NOT YOUR COINS

"Not your keys, not your coins" 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.

Whoever accesses your private keys will gain ownership of your bitcoins. This is why it is of the utmost importance to protect them by keeping them away from prying eyes! We'll see a few ways you can do that later in the book.

For what follows, we'll be talking about self-custodial wallets only, where the user owns their keys and has complete control over their bitcoins.

Don't worry if it seems complicated or you don't understand everything - this is a journey, and you willunderstand more as you start using Bitcoin more!

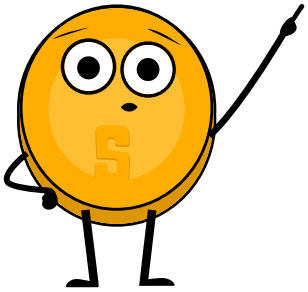
7.2.2 Different Types of Bitcoin Wallets

Depending on where your private key is created and stored, we commonly use different names to describe Bitcoin wallets. If the keys are stored on your smartphone, we call it a “mobile wallet.” If they’re stored securely on a dedicated device, we call it a “hardware wallet.” If the key is only stored on paper, then it is called a “paper wallet.”

The different names we give to Bitcoin wallets depending on their structure:

Wallet Type	Description	Advantages	Disadvantages	Example User
Online Wallet	A wallet 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 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 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 bitcoins and is comfortable with using a desktop computer.
Hardware Wallet	A physical device that stores bitcoins 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 bitcoins 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 bitcoins and is willing to take added precautions to ensure its security.

Because the keys can be moved from one device to another, the “status” of your Bitcoin wallet is not definitive. For example, if I generate the keys of my Bitcoin wallet on a computer and later upload them to my phone, the “desktop wallet” then becomes a “mobile wallet.”



When it comes to storing your bitcoins, it’s not just about who has control over them — there are many other risks to consider. That’s why it’s important to find a storage solution that is both secure and convenient.

When you analyze the trade-offs of the various types of wallets, you will learn that there is no ideal wallet to satisfy 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 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.

7.2.3 Open Source vs. Closed Source

Another important factor to keep in mind when choosing a Bitcoin wallet is knowing if the application or software is open-source.

Open-source code is very important because it allows the community to review the code and continue developing the project if the team were to stop working on it.

How to Use Bitcoin

Just as Bitcoin's code is completely open for everyone to review, use, and modify, so should be the code of the wallet you use to store your bitcoins.

Activity: Class Discussion and Evaluation of Bitcoin Wallets on bitcoin.org

Go to the following website: https://bitcoin.org/en/choose-your-wallet and use your new knowledge of Bitcoin wallets to select the best one based on the criteria we discussed today.

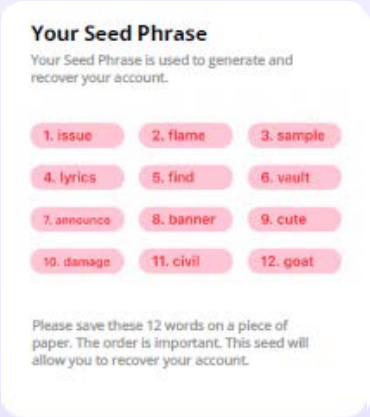
7.3 Setting up a Mobile Bitcoin Wallet

Now that we have a better understanding of Bitcoin wallets and the differences between them, we'll see how to use one in practice. For this example, we'll create a mobile wallet directly on our smartphone.

Activity: Setting Up/Recovering a Bitcoin Wallet

If students do not have cell phones, the teacher will provide one for 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 (sometimes called a seed phrase). Be sure to write it down and keep this in a safe place! This recovery phrase allows you to recover full access to your funds if needed.

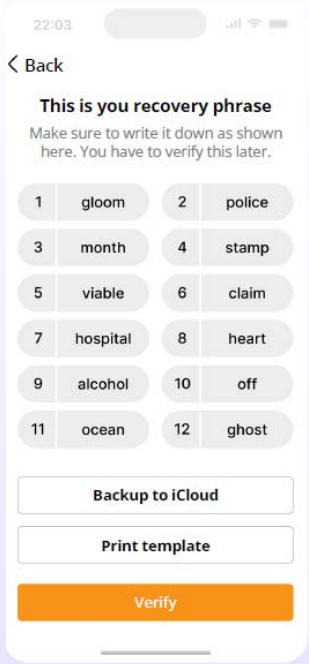
Remember that if you lose or forget this sequence of words, you will not be able to access your bitcoins if you lose access to your wallet.

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.

Think of your public key as your email address — you want to share this with others so that they can send you bitcoins — or, in the case of an email address, an email.

Think of your private key as the password to your email – you wouldn't want to share this with anyone, as it would give them access to your email.

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



Class Exercise: Option 2 - Restore a wallet (Time-Limited).

Download a Bitcoin wallet and add some satoshis 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] when finished.
4. You will see an "Import Successful" message when your wallet has been successfully imported.

7.4 Receiving and Sending Transactions

A bitcoin transaction is a transfer of ownership of existing bitcoins to a new owner. However, instead of transferring actual coins, all the nodes in the network update their local copy of the public ledger to reflect the change in ownership.

When sending a bitcoin transaction, the sender signs a message that only they can sign with their private key, signaling to the network that the ownership of the bitcoins has changed to the recipient's address.

The bitcoins will now be tied to an address that only the new owner can send from, giving them ownership of the bitcoins.

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 Eliana

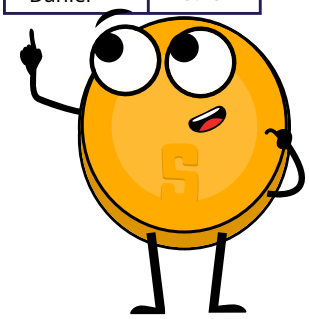
Jim ▶ **Eliana 0.50 BTC**

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

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.

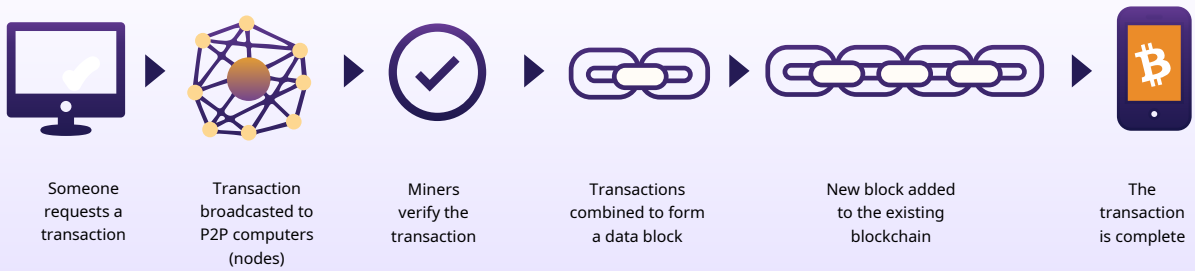
Let's say Jim owes Eliana 0.5 BTC and is ready to pay her back. Both have digital wallets.



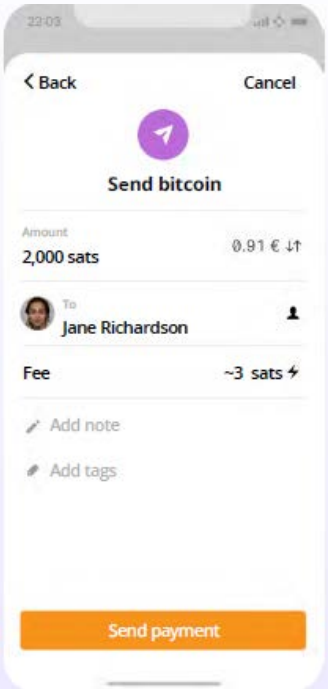
- Eliana shares her address with Jim.
- Jim uses his wallet software to create the transaction, which includes Eliana's address, the amount to be transferred (0.5 BTC), and a fee for the miner.
- After signing the transaction, it is broadcast to the network, where it is verified by nodes. Nodes check the transaction for validity and ensure that Jim has enough funds. If he does not, they reject the transaction immediately.
- Once the transaction is verified, miners add it to the blockchain and the funds are transferred to Eliana's address.
- Eliana can then use her private key to access the transferred funds in her wallet.

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

How a Bitcoin Transaction Works



Receiving Bitcoin Transactions:



To receive bitcoins, 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" bitcoins.

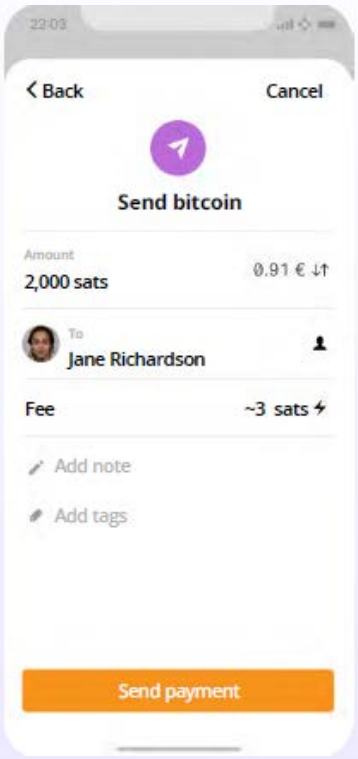
You can then share your Bitcoin address with the sender in one of several ways:

1. 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.
2. 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 bitcoins.
3. 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.

How to Use Bitcoin

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

Next, we will take a look at sending bitcoin transactions.



Sending Bitcoin Transactions:

To send bitcoins, you will need a few things: a Bitcoin wallet, the recipient's Bitcoin address, and the amount of bitcoins 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 number of bitcoins 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 you double-check the transaction details one more time to ensure that you are sending the correct amount of bitcoins to the correct wallet address.
7. Confirm the transaction and wait for the network to confirm the transaction

Now you know how to evaluate, select, and set up a self-custodial Bitcoin wallet. Sending bitcoins from one wallet to another on the Bitcoin network is called sending an "on-chain" transaction. This is because the transaction occurs on the main Bitcoin network blockchain. On-chain transactions are the safest way to transact with bitcoins. However, on-chain transactions are slower and can be significantly more expensive than other options, such as the Lightning transactions we will discuss in Chapter 8.

Activity: Bitcoin Transactions in Action

Objective: To understand the underlying concepts and mechanics of a peer-to-peer bitcoin transaction.

Before we get started, here's a quick reminder on the key players in a bitcoin transaction:

- Senders and receivers are the parties who wish to transact with each other.
- 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.
- Miners are responsible for adding new transactions to the blockchain.

Understand your role. You have been assigned one of the following: 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.
- Miners will be responsible for adding the transactions to the blockchain.

Both nodes and receivers have to verify transactions

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.

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. **Coin Sent** Verify and validate transactions. You are responsible for checking that the transaction is valid.
   - Verify that the sender's address and the receiver's address are 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

How to Use Bitcoin

4 **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 earn a point. At the end of the activity, the miner with the most points wins.

**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.your digital wallet.

Coin Sent	Sender	Sender Signature	Receiver	Date & Time	Approval

6 **Discuss the concepts learned with your class.**

7.5 Saving in Bitcoin

Bitcoin is a way to safeguard your money against inflation and protect it from being controlled by anyone else, if you do it correctly. Saving in bitcoins provides a vehicle to store, accumulate, and build wealth over time. As you understand by now, the type of money you choose to save is one of the most important decisions you can make.

Choosing wisely allows you to build a better future for yourself and your family.

Peace of Mind: When stored properly, Bitcoin is the only form of property no one can take away from you.

7.6 Don’t Trust, Verify

Whatever you do in Bitcoin, remember this: “Don’t Trust, Verify.” There are no leaders in Bitcoin. You should never blindly follow someone’s claims. Rather, you should always question what you’re being told and verifyit for yourself. By following this mantra, you’ll protect yourself from losing your bitcoins. This goes for claims such as “the next Bitcoin” just as it does for “investment opportunities” or promises of “quick and easy profits.”

In summary, Chapter 7 has given you the important skills to use Bitcoin in your everyday life. You have learned how to get and exchange bitcoin in different ways and how to keep it safe using various wallets. By setting up your mobile Bitcoin wallet and making transactions with others, you now have the hands-on experience to confidently use Bitcoin day-to-day. By understanding Bitcoin as a way to save money and following the idea of “Don’t Trust, Verify," you're now in control of your money.

In the upcoming chapter, we will explore the Lightning Network. We will look at how this innovative technology is changing the way people worldwide access and use money. From everyday transactions to more advanced applications, you will learn how the Lightning Network empowers individuals, communities, and businesses by providing them access to financial services.

Chapter #8

Lightning Network: Using Bitcoin in Your Daily Life

8.0 Introduction

Activity: Watch “Bitcoin Lightning Network Explained: How It Actually Works”

8.1 The Lightning Network

8.2 Different Types of Lightning Wallets

8.2.1 Self-Custodial vs. Custodial Wallets

8.2.2 Open Source vs. Closed Source

8.3 Setting Up a Bitcoin Lightning Wallet

8.4 Sending and Receiving Lightning Transactions

Activity: Lightning Wallet Relay Race

8.5 Buying Coffee and Groceries with Bitcoin

8.5.1 Online: Payment Plugins — Ecommerce

8.5.2 In Person: Find a Merchant in Your Area

8.5.3 Transitional Tools: Gift Cards and Payment Cards

8.5.4 Circular Economies and Bitcoin as a Medium of Exchange

Caietul elevului

Limba Română | 2025

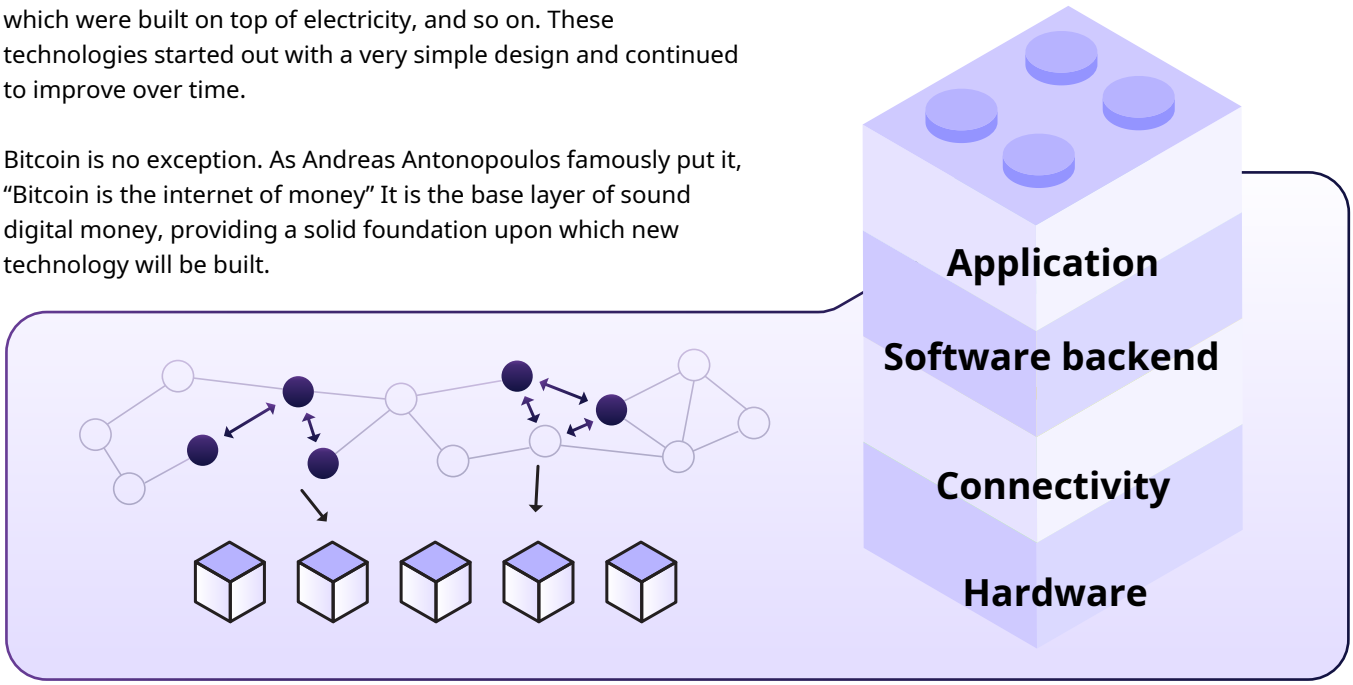
Lightning Network: Using Bitcoin in Your Daily Life

8.0 Introduction

> We’re building the Visa network for bitcoin. But what I think is powerful, is unlike Visa, anybody can build on top of it.
>
> **My First Bitcoin**

Technologies typically grow and expand in layers, like a stack. Think of your favorite website, email, or social media: they were built on top of the internet protocol, which was built on top of computers, which were built on top of electricity, and so on. These technologies started out with a very simple design and continued to improve over time.

Bitcoin is no exception. As Andreas Antonopoulos famously put it, “Bitcoin is the internet of money” It is the base layer of sound digital money, providing a solid foundation upon which new technology will be built.



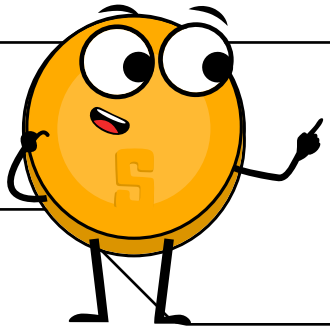
One of these layers is called the Lightning Network. This is like a super-fast highway for Bitcoin, helping people send and receive bitcoins quickly and with very low fees. It allows users to make instant, small transactions on top of the regular Bitcoin network. This makes buying a coffee or paying a friend simple and fast!

Remember: A satoshi is like the smallest coin of bitcoin. Just like a dollar can be broken into cents, one bitcoin can be split into smaller units called satoshis. One bitcoin equals 100 million satoshis, making satoshis the tiniest bits of value in the Bitcoin system. In this chapter, when we talk about sending bitcoins through the Lightning Network, we'll call it "sending sats," which are just smaller parts of a bitcoin.

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

Chapter #8

Activity: Watch this video on the Lightning Network



8.1 The Lightning Network

As we've just seen, the Lightning Network serves as a payment system, facilitating quick and cost-effective transactions with bitcoins. It operates by establishing a shared wallet where both parties hold some bitcoins. They can conduct numerous transactions with each other without the need to record each one on the main ledger. The final balance is then recorded on the ledger once the transactions are complete.

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 bitcoins and then making unlimited transactions with each other without touching the main blockchain. When they're done, the final balance is recorded on the main blockchain.

Picture a day spent doing some work in a café. Anticipating a full day's stay, you open a tab and prepay some money instead of paying each time you order something. When you're ready to leave at the end of the day, you and the owner review the tab to settle the final bill. If you paid more money up front than the total amount of your final bill, you will receive back whatever amount you did not spend.

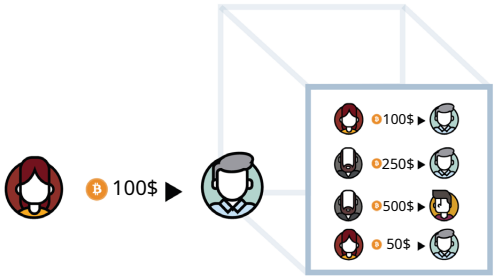
Now, envision thousands of people doing the same thing simultaneously and allowing others to use their tabs to connect with more people. That's the Lightning Network!

With Lightning, you can make payments to anyone on the network, not just the person you share a direct tab with. Your payment can navigate through the network until it reaches its destination, even if you don't have an open channel with the recipient.

Let’s take a look at the difference between on-chain transactions (the type we discussed in Chapter 7) and off-chain transactions (Lightning Network).

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 more secure but slower.

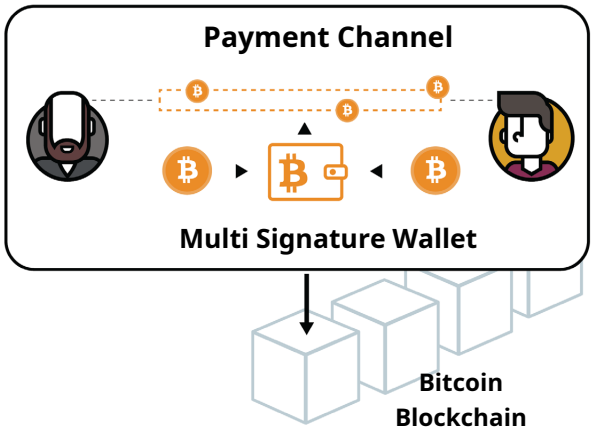


Lightning Network: Using Bitcoin in Your Daily Life

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 features like the speed and cost of transactions are more important. Compared to on-chain transactions, they are less secure.



Payment Network	Bitcoin Network	Lighting 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 charge-backs 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.

8.2 Different Types of Lightning Wallets

A Lightning wallet is a bit different than a Bitcoin wallet, though it performs the same function: receiving and sending bitcoins. The difference is that a Lightning wallet allows you to send bitcoins on the Lightning Network, which itself is a second layer on top of the Bitcoin network.

Just as we saw in the previous chapter with Bitcoin wallets, Lightning wallets have different characteristics that need to be considered before choosing one.

8.2.1 Self-Custodial vs. Custodial Wallets

Lightning wallets can be broken down into very specific categories, but for the sake of simplicity, we'll divide them into two: self-custodial and custodial.

Just like Bitcoin wallets, a self-custodial Lightning wallet is one where you control the keys to the wallet, whereas a custodial Lightning wallet is one where someone else controls the keys.

When using a custodial wallet, you're only given access to the wallet but you depend on someone else for permission to use your money; you're giving up ownership of your money for convenience.

This can be acceptable for small amounts, although it's recommended to use a self-custodial wallet once you have an understanding of the technology.

For what follows, we'll be talking about self-custodial Lightning wallets only.

8.2.2 Open Source vs. Closed Source

Just like with the Bitcoin wallets we saw in the previous chapter, Lightning wallets can be open-source or closed source. Always use open-source wallets as they are completely open for review and vetted by the community.

An open-source application also means that anyone can contribute to the improvement of the software, making it a better choice for users.

8.3 Setting up a Bitcoin Lightning Wallet

Setting up a self-custodial Bitcoin Lightning wallet is the same as setting up a self-custodial on-chain Bitcoin wallet.

Lightning Network: Using Bitcoin in Your Daily Life

Class Exercise — Option 1: Download a new self-custodial lightning wallet

How to Create and Use a Bitcoin Lightning 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 (sometimes called a seed phrase). Be sure to write it down and keep this in a safe place! This recovery phrase allows you to recover full access to your funds if needed.

Remember that if you lose or forget this sequence of words, you will not be able to access your bitcoins 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. Generate a Lightning invoice, address, or QR code to receive bitcoins. Transfer bitcoins to your wallet. With a self-custodial wallet, you cannot always buy bitcoins directly with fiat, so you might need to purchase and transfer them from an exchange first.

Your Seed Phrase Your seed phrase is used to generate and recover your account.

Issue	Flame	Sample	Lyrics	Find
Issue	Scissors	Banner	Cute	Damage
Issue	Goat			

Please save these 12 words on a piece of paper. The order is important. This seed will allow you to recover your account.

*Note: If you are using a custodial wallet, you will not need to follow some of the steps in section 8.3. Using a custodial wallet comes with risk, as you will not be in control of your private key, which means you will not be in control of the money you keep in your wallet.

Now that we have set up our Bitcoin Lightning wallet, let's look at receiving and sending Lightning transactions and how they differ from the on-chain transactions we sent in Chapter 7.

8.4 Sending and Receiving Lightning Transactions

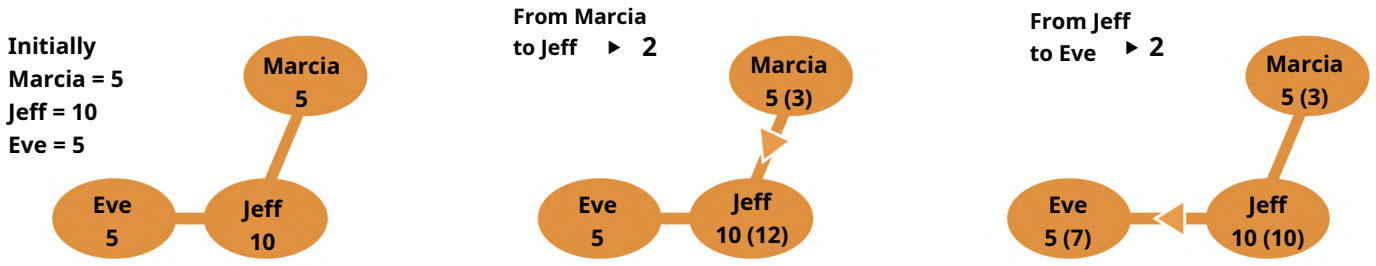
With a Lightning wallet, using Bitcoin is fast, cheap, and private, making transactions between two people easy. You can quickly send and receive bitcoins for everyday things like buying coffee or shopping.

Let's look at a few examples of the Lightning Network in action.

Example 1:

Below, both Marcia and Eve have 5 units of currency each. 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.

2 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 network's security by adding an additional layer of protection between Marcia and Eve. This can increase the users' confidence 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 network's growth and development.

In summary, on-chain transactions are slower but more secure, while off-chain (Lightning Network) ones are faster but less secure. You should consider the trade-off 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.

The Lightning Network vs. The Traditional Banking System

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

Benefits	Lightning	Traditional Banking Syste
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

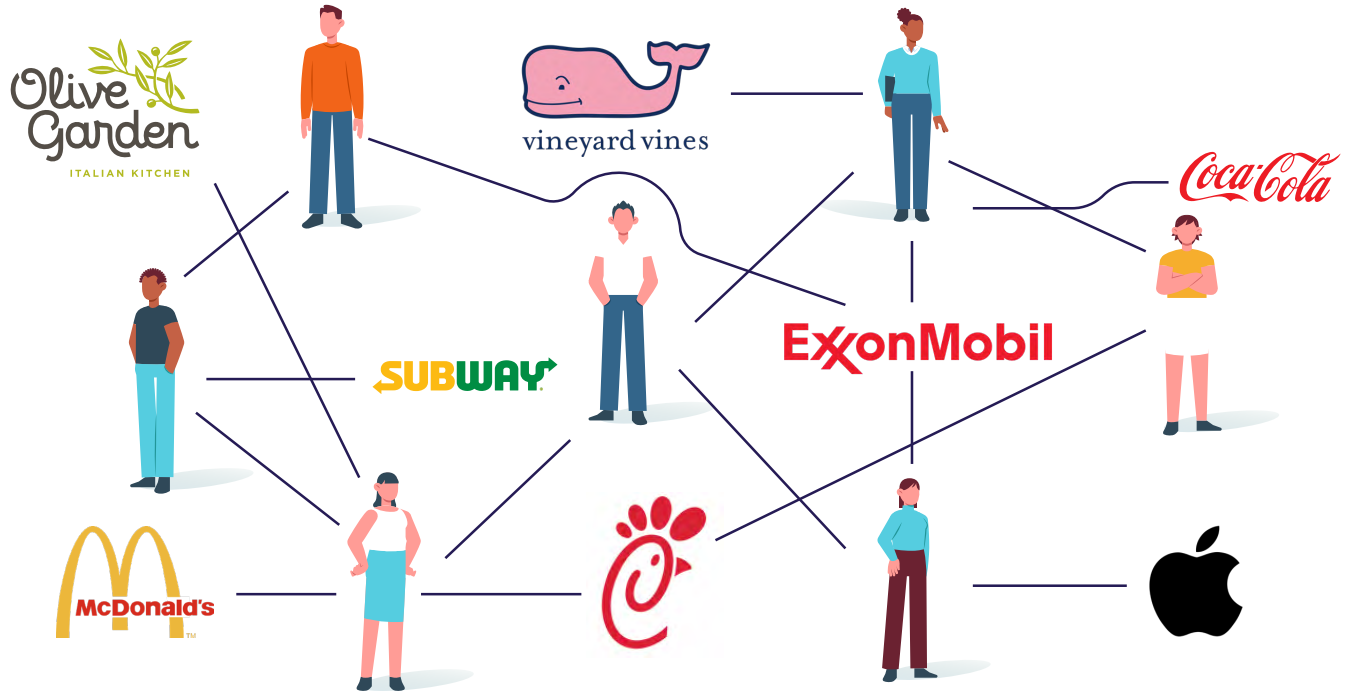
Capacity of 7 transactions per second.

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 wallet by sending some bitcoins 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 bitcoins she is comfortable with, but it's important to note that the amount of bitcoins 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 bitcoins from her Lightning wallet to a specific address provided by McDonald's. This moves her bitcoins 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 bitcoins, the channel tracks that Mina now has 0.9995 bitcoins. And if she buys a milkshake for 0.0003 bitcoins the next day, the channel tracks that Mina now has 0.9992 bitcoins.

Lightning Network: Using Bitcoin in Your Daily Life

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 bitcoins 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.

Now that we have set up our Lightning wallet and read about how to use the Lightning Network to send transactions, we are going to play a game where we send satoshis (the smallest unit of bitcoin) to other students in the class over the Lightning Network.

This is a map of the entire world. With the Lightning Network, you can send satoshis to any user with a Bitcoin Lightning wallet. The payment will arrive in a few seconds and will only cost a few cents.

Check it out for yourself:

Primul Meu Bitcoin

Activity: Class Exercise - Lightning Wallet Relay Race

1. First, you will need to download a Lightning wallet onto your phone or computer.
2. Follow the instructions for installing the wallet on your device in Section 8.3 of this chapter.
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. Generate a Lightning invoice, address, or QR code to receive bitcoins.
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 you want to send.

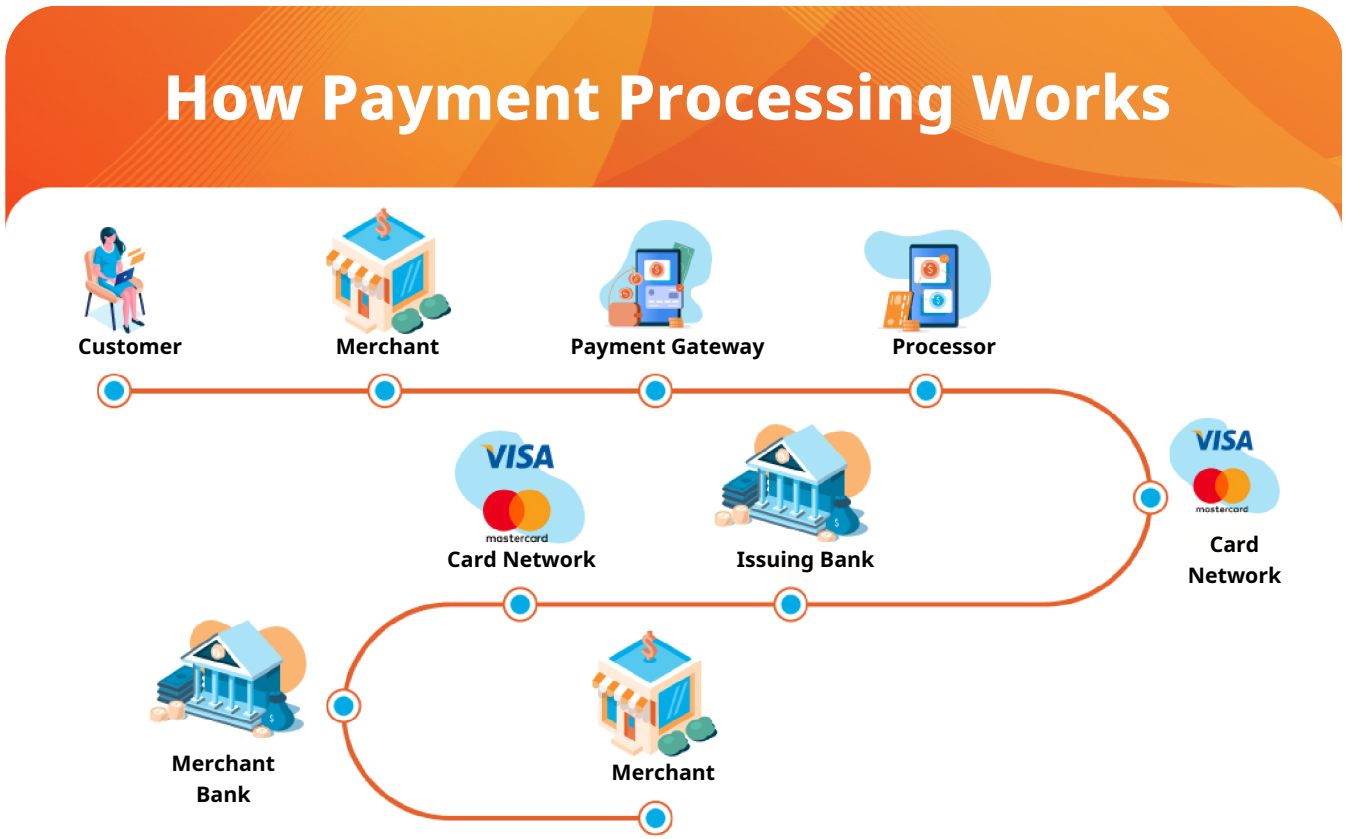
5 If your group is the first to successfully send the satoshis to the last person, you win! (And get to keep the sats).

Discuss any difficulties your group had with the activity. Was sending a transaction easy, fast, and inexpensive? Do you think the Lightning Network is easy to use and understand?

8.5 Buying Coffee and Groceries with Bitcoin

Have you ever wondered if you could use bitcoins to buy your daily cup of coffee or stock up on groceries? Turns out you can. There are many options, both online and in person, that let you pay with bitcoins. We'll explore some of those options and tools that will help you find local stores so you can spend bitcoins.

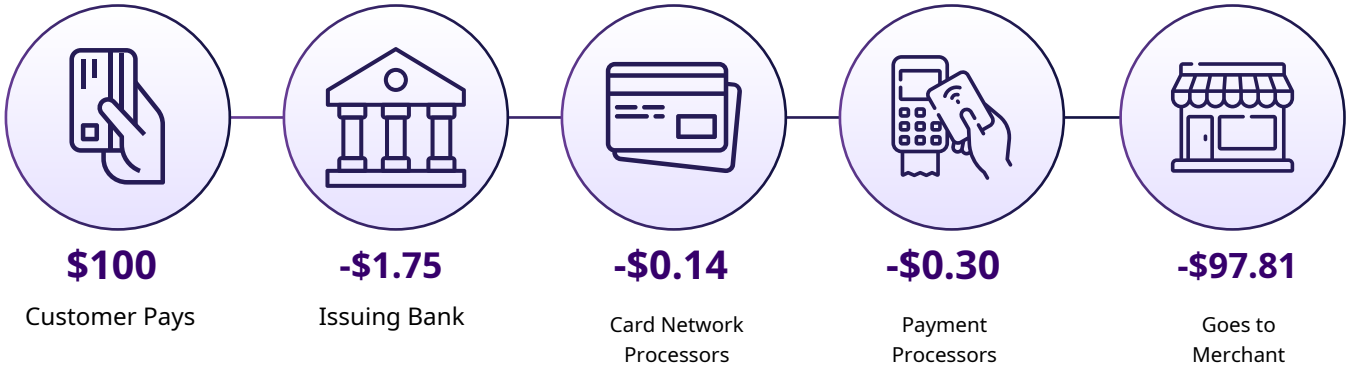
Even though paying with a credit card or an app can seem easy to understand for the person paying, the processing of the payment is actually very complex and involves many different parties.



When you buy things, there are many parties involved, and each party charges a fee. For store owners, these fees can be a lot — more than 3% of the price, which is a big amount for them.

And that's not to mention currency exchange fees!

Credit Card Processing Fees



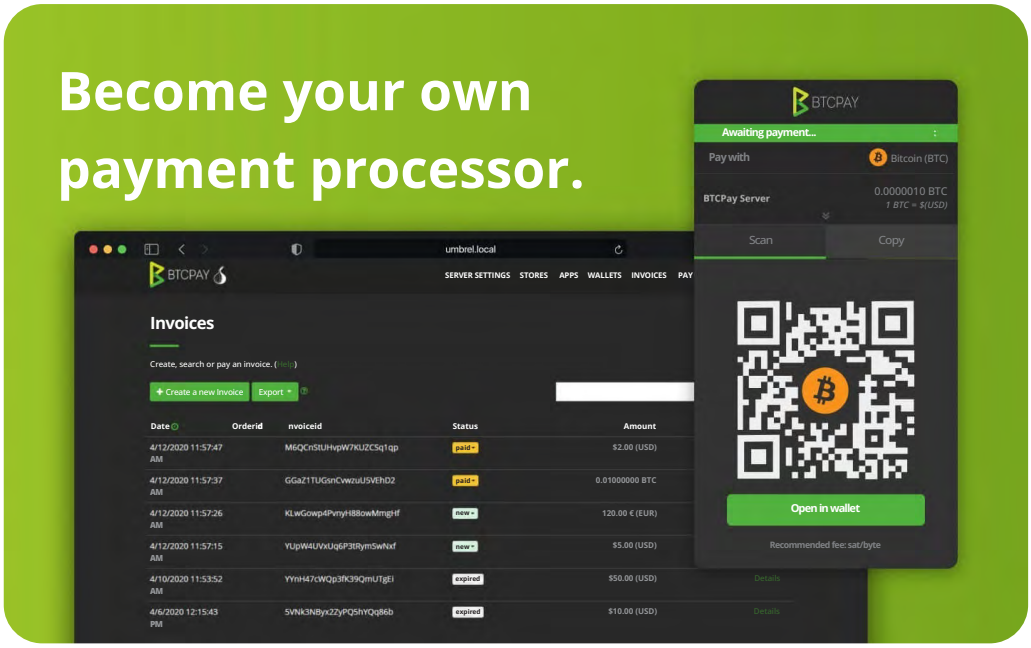
With Bitcoin and the Lightning Network, businesses can receive instant payments from all over the world viaan open, secure, internet-native, borderless, and censorship-resistant monetary system.

Next, we will look at a few ways merchants can easily accept payments in bitcoins.

8.5.1 Online: Payment Plugins — Ecommerce

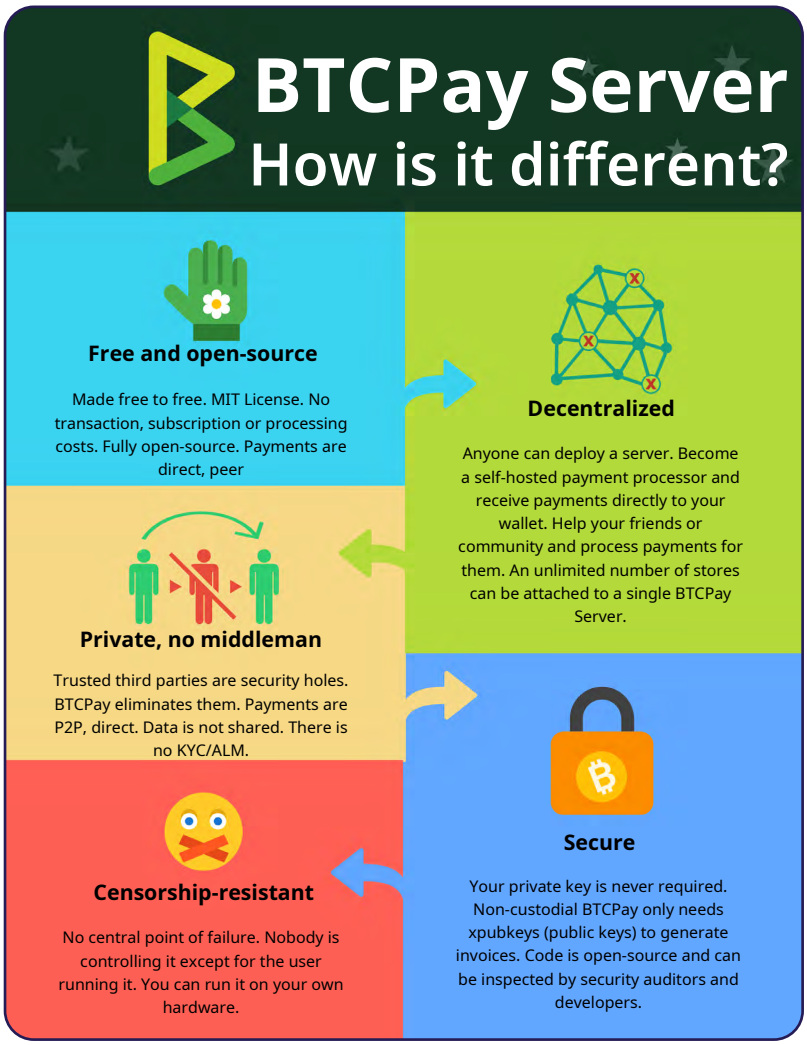
BTCPay Server is an open-source payment processor that allows merchants to accept payments in bitcoins with little technical knowledge. It's completely free and doesn't charge any commission.

Online businesses can integrate BTCPay Server seamlessly by adding the BTCPay plugin to their website.



Because BTCPay Server is an open-source project, not a company, you can contribute to the project once you learn more about it and computer programming.

Check out BTCPayServer at https://btcpayserver.org/ for more information on how to use this payment system for your in-person or online business.

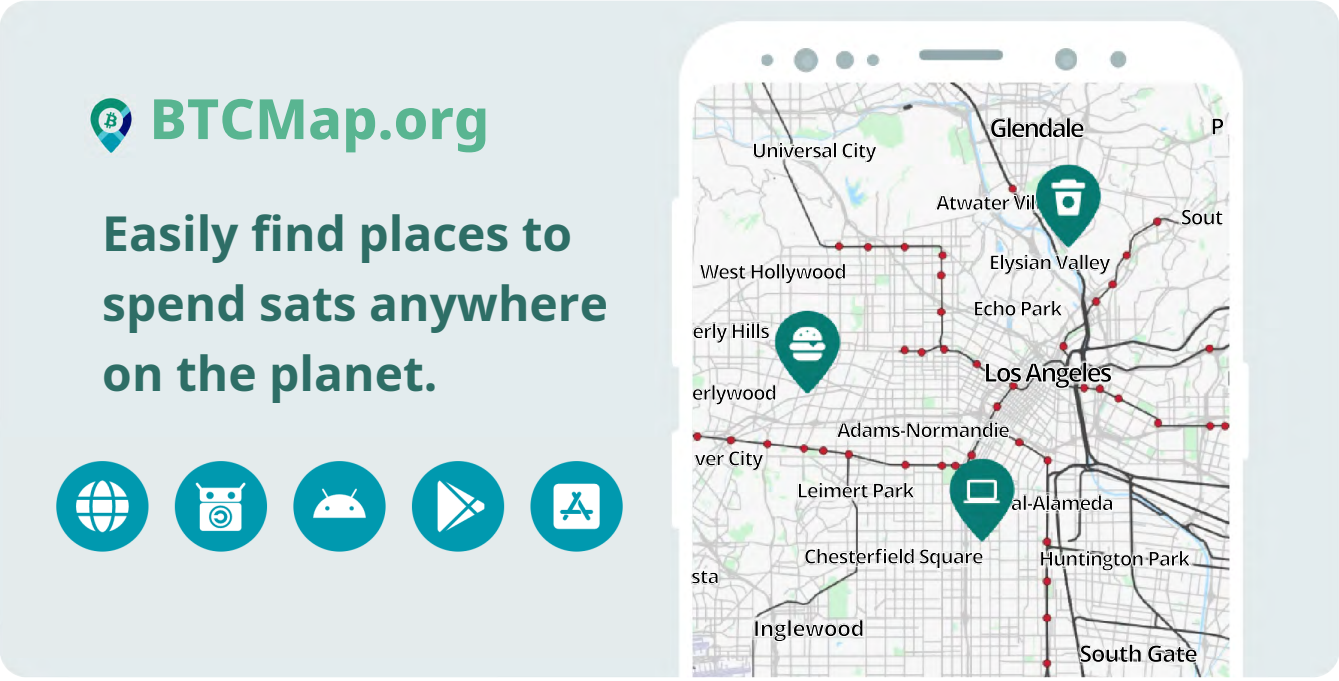


8.5.2 In-Person: Find a Merchant in Your Area

Physical shops can also use BTCPay Server to accept payments, or they can simply download a Bitcoin wallet and accept Bitcoin payments directly from their phone.

To find a merchant that accepts Bitcoin in your area, go to BTCMap.org and search for your region.

BTCMap.org is an open-source map where merchants that accept Bitcoin can list their businesses. It's apowerful tool for people who wish to spend their bitcoins.



8.5.3 Transitional Tools: Vouchers, Gift Cards, and Payment Cards

To purchase products or services from businesses that do not yet accept Bitcoin, there is an intermediary tool you can use: gift cards.

Some businesses focus on buying and selling gift cards in exchange for bitcoins. That means you can acquire a gift card for the store you'd like to go to in exchange for bitcoins and then spend the gift card directly at the store.

Plane tickets, hotels, games, SIM cards... you can buy almost anything with bitcoins and gift cards!

8.5.4 Circular Economies and Bitcoin as a Medium of Exchange

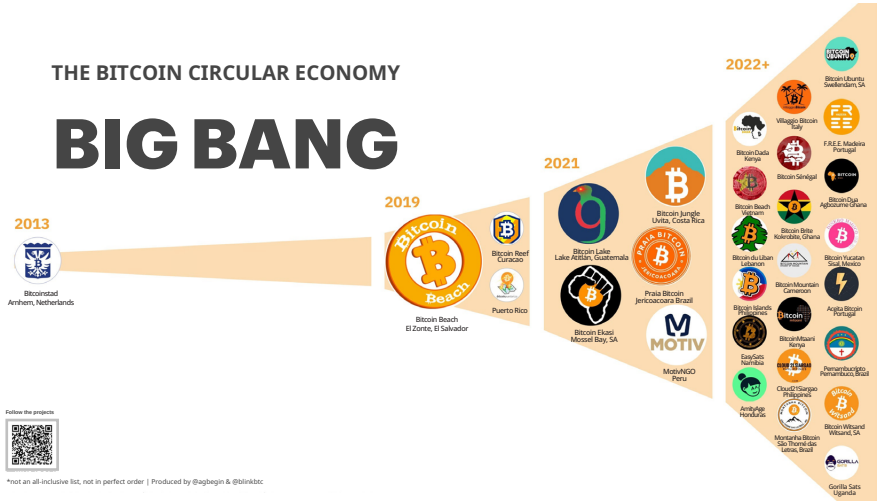
The concept of the circular economy comes from the idea of minimizing waste in an economy by reusing and recycling as many products and byproducts as possible.

Drawing from this concept, a Bitcoin circular economy is one where the transactions are made in bitcoins and where the money in the form of bitcoins stays and grows within the economy, benefitting its individuals and businesses.

Lightning Network: Using Bitcoin in Your Daily Life

The Lightning Network enables Bitcoin circular economies to flourish all around the world thanks to near-instant and low-fee bitcoin transactions.

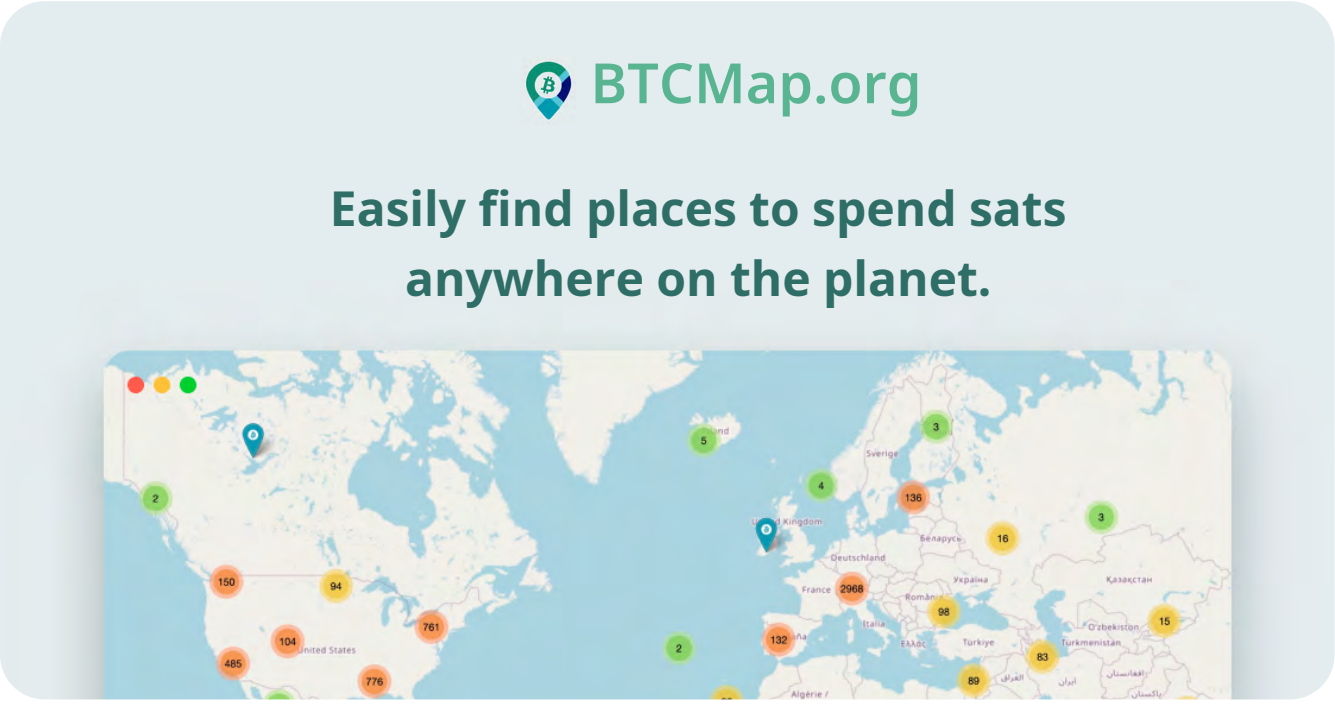
The first Bitcoin circular economy ever created is located in Arnhem, Netherlands. It was created way before the Lightning Network existed, but back then, on-chain fees were really low!



The second one was Bitcoin Beach, located in El Zonte, El Salvador. It leveraged the power of the Lightning Network to provide the community, which was mostly unbanked, with instant digital payments directly with their smartphones!

Today, hundreds of circular economies are being created all around the world, powered by Bitcoin, the Lightning Network, and educational resources.

On BTCMap.org, you can also look for Bitcoin communities where you will meet other Bitcoin users and find businesses that accept Bitcoin. Some of our teachers and students have actually added businesses and circular economies to BTCmap.org, and once you are ready, you can too!



Resource: btcmap.org/communities

As we wrap up Chapter 8, you've gained insights into using Bitcoin in your daily life through the Lightning Network. The Lightning Network makes transactions quicker and more accessible, offering a preview of how Bitcoin will continue to change and evolve in layers.

In Chapter 9, we will investigate the technical side of Bitcoin. From cryptography to nodes, miners, andmore, get ready to take a closer look at how Bitcoin really works.

Chapter #9

An Introduction to the Technical Side of Bitcoin

9.0 Introduction

Activity: Watch “How Bitcoin Works under the Hood”

9.1 Public and Private Keys: Security through Cryptography

9.1.1 Cryptography Public/Private Keys

9.1.2 Hashing Explanation

Activity: Generate SHA 256 Hash

9.2 The UTXO Model

9.3 Bitcoin Nodes and Miners

9.3.1 What Is a Bitcoin Node and How Do I Set One Up?

Activity: Watch Video on Bitcoin Nodes

9.3.2 What Is a Bitcoin Miner and How Does Mining Work?

9.4 What Is the Mempool?

Activity: Mempool

9.5 How Bitcoin Transactions Work from Start to Finish

Caietul elevului

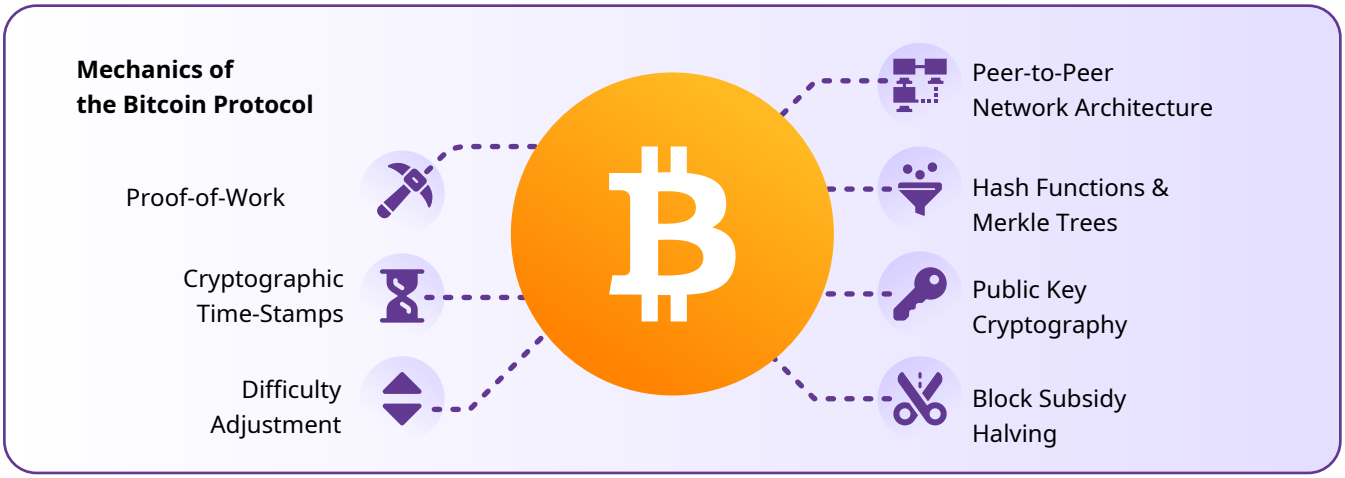
Limba Română | 2025

An Introduction to the Technical Side of Bitcoin

9.0 Introduction

> Bitcoin is not "unregulated"; it is regulated by algorithm instead of being regulated by government bureaucracies. Uncorrupted.
>
> **My First Bitcoin**

In this chapter, we will take a closer look at the technology that enables the Bitcoin network to operate in a fully decentralized way. We will explain in simple terms what happens when you send a bitcoin transaction, how those transactions are processed, and what miners and nodes do in the Bitcoin network. We are going to cover some challenging and technical concepts in this chapter. One important thing to remember: many people don't understand how the internet works, yet they are able to use it every day to send emails, contact friends on social media, and even pay their bills. Learning the technical side of how Bitcoin works is a long journey that not everyone may want to take, even if they decide to use it as money. While we do encourage you to keep learning about the technical aspects of Bitcoin, we will keep this chapter focused on basic key concepts.



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

Let's jump in by watching a video that shows how the Bitcoin network works.

Activity: Watch "How Bitcoin Works under the Hood"

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

Chapter #9

Primul Meu Bitcoin

Next, we'll take a closer look at the technology that makes this system possible.

9.1 Public and Private Keys: Security through Cryptography

> What Bitcoin gives us is a hard promise: the program will execute exactly as specified.
>
> **My First Bitcoin**

9.1.1 Cryptography Public/Private Keys

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

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

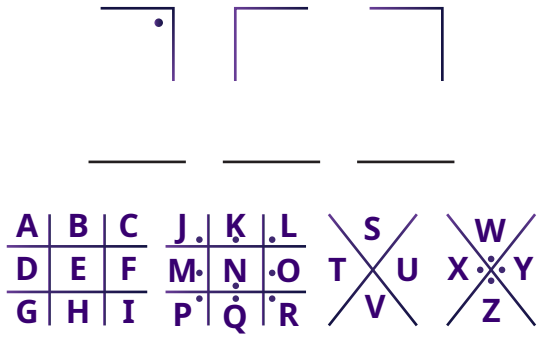
- Decryption, on the other hand, is the process of taking the encrypted information and making it readable again, like unlocking the safe and being able to read the information inside.

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

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:



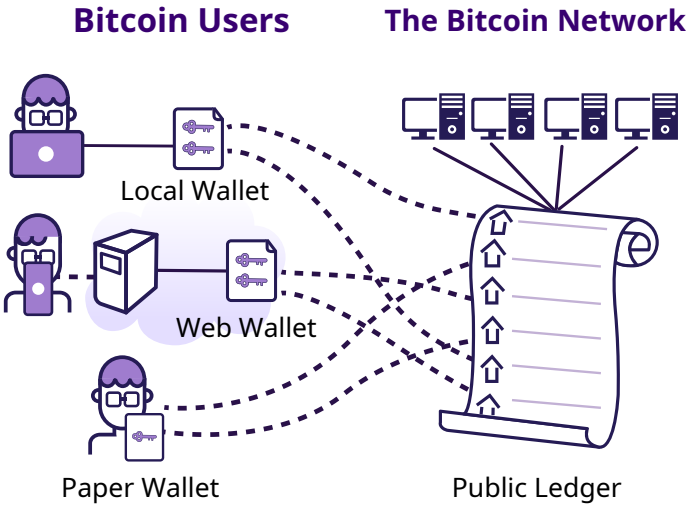
So, how does cryptography work in bitcoin transactions?

In traditional private-key cryptography, John and Arel would have to first share a secret key, like a password or the Pigpen Cipher. John would then use this key to encrypt his message before sending it to Arel. Arel, who also knows the secret key, would then use the same key to decrypt and read the message. However, if someone else is in possession of the key and intercepts the message, they could decrypt it and read it.

An Introduction to the Technical Side of Bitcoin

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

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



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

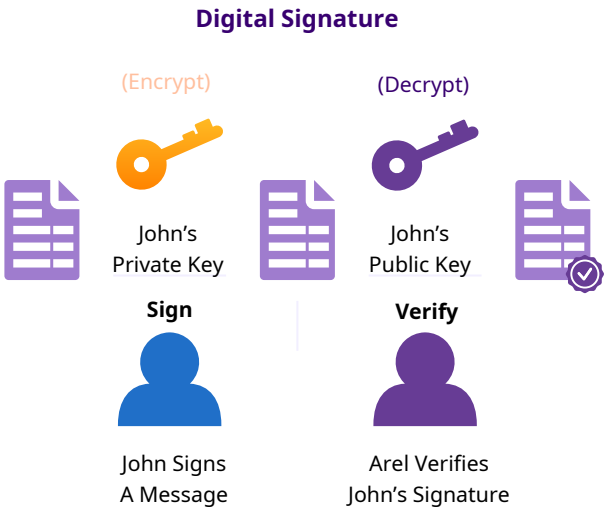
In Bitcoin, public key cryptography is not used to send encrypted messages. Instead, it is used to create unique digital signatures that make bitcoin transactions immutable. A digital signature is a way to prove a bitcoin transaction's authenticity, similar to when you write your signature on a physical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

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."

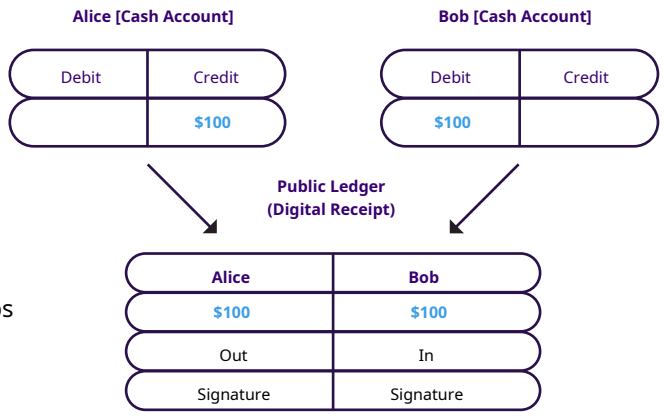
Digital signatures are created to identify unique transactions.



Chapter #9

Primul Meu Bitcoin

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



How this works in a real bitcoin transaction in simple terms:

1. **Creating the Transaction:**

   A user initiates a bitcoin transaction by specifying details such as the recipient's address and the amount of bitcoins to be sent.

1. **Digital Signature Generation:**

   The sender generates a unique digital signature using their private key. This signature is a unique cryptographic code that verifies the transaction's authenticity.

2. **Broadcasting the Transaction:**

   The signed transaction is broadcasted to the Bitcoin network, indicating the intent to transfer ownership of bitcoins from the sender to the recipient.

3. **Verification on the Network:**

   Nodes on the Bitcoin network receive the transaction and use the recipient's public key to decrypt and verify the integrity of the transaction. Simultaneously, they use the sender's public key to verify the digital signature.

4. **Confirmation on the Bitcoin Network:**

   If the verification is successful, the transaction will be added to the ledger, which serves as a secure, transparent record of all transactions. Once confirmed, the ownership of the bitcoins is officially transferred from the sender to the recipient.

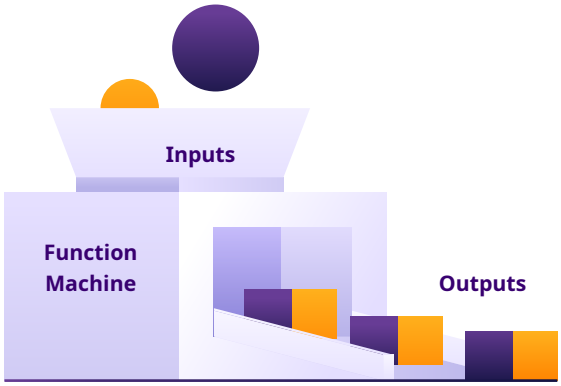
In summary, the digital signature, created with the sender's private key, serves as cryptographic proof of authenticity and ownership, allowing Bitcoin's decentralized network to validate and record

9.1.2 Hashing Explanation

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

What Is a function?

A function is like a machine that takes some information and turns it into something new. The information you give the function is called the input. The new information the function creates is called 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 is a function that takes the ingredients as the input and generates the tossed salad as the output.

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

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

What Is a One-Way Function?

A one-way function uses a set of instructions to process 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.

Chapter #9

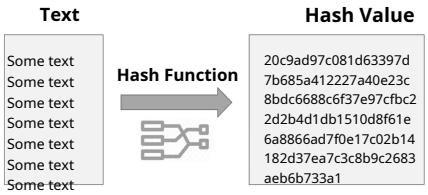
Primul Meu Bitcoin

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

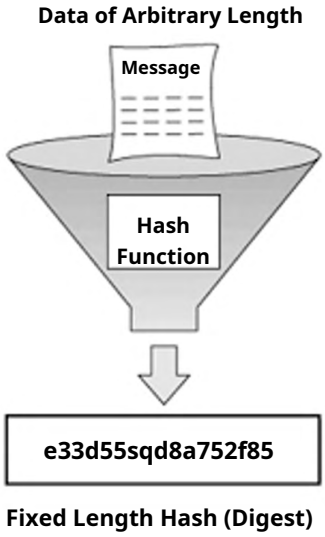


How Hashing Is Used in Bitcoin Transactions

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

The Role of Hashing in Providing Security

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



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

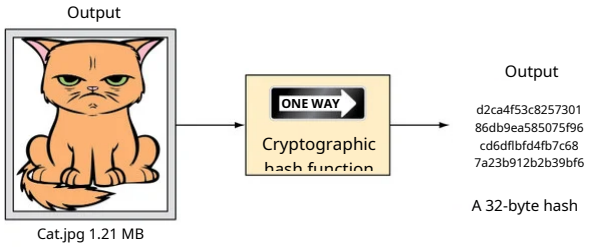
A hash function is like a secret code machine. It takes in a message and turns it into a code.

An Introduction to the Technical Side of Bitcoin

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.

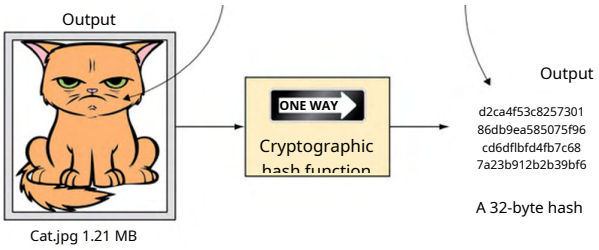
Instantly generate a SHA256 hash of any string or input value. Hash functions are used as one-way methods.

Activity - Generate SHA 256 Hash →



Missing whisker! Now she's got a reason to be grumpy.

Completely different than the previous hash.



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

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

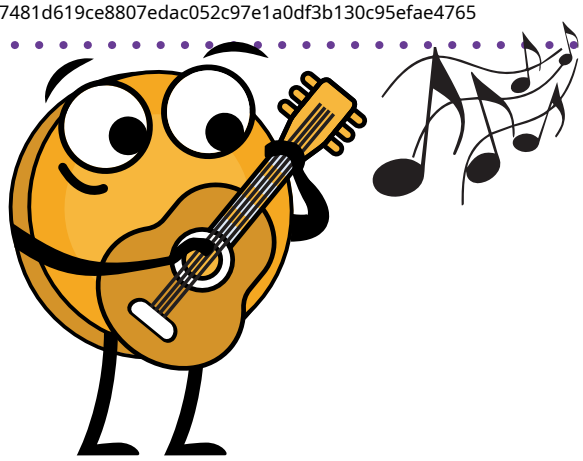
- Notice that a small change in the second input changes the output completely when compared to the first one.
- The third input is a huge file yet the output is still the same fixed length as the other two.

SHA256 hash of the string hello world
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

SHA256 hash of the string hello world.
7ddb227315f423250fc67f3be69c544628dffe41752af91c50ae0a9c49faeb87

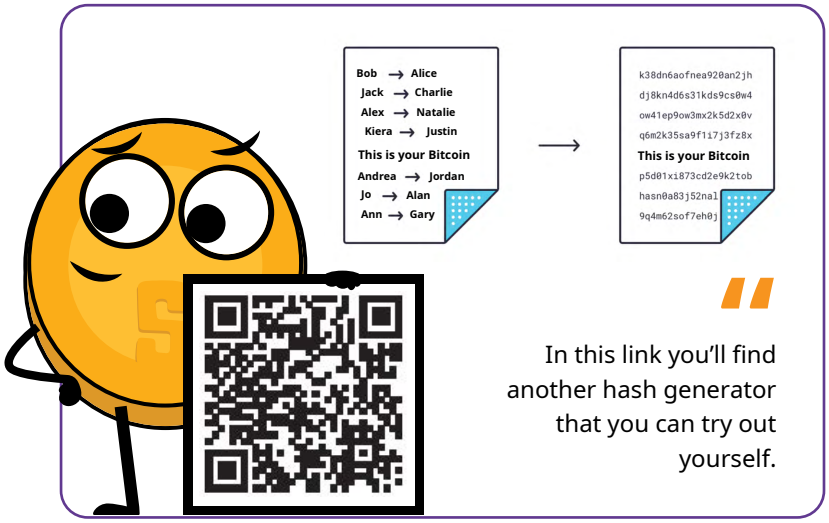
SHA256 hash of the downloadable iso file Ubuntu 18.10
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

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 a bitcoin transaction.

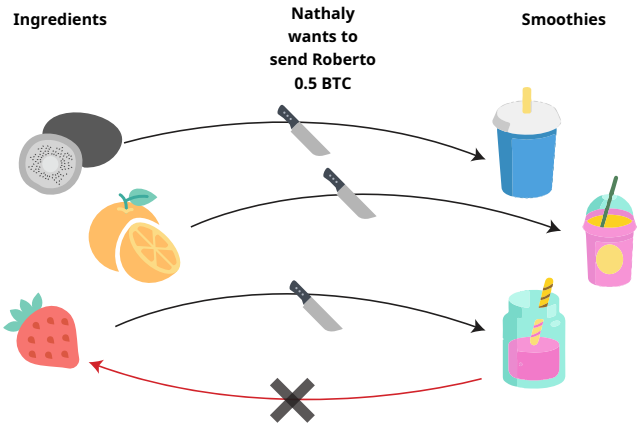
The process of encoding the public key through hashing is used to improve the security of information by converting it into a fixed-length, unreadable format. Bitcoin uses the SHA-256 and Ripemd-160 algorithms to produce public addresses. The resulting output serves as a unique identifier for the public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



In this link you'll find another hash generator that you can try 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.

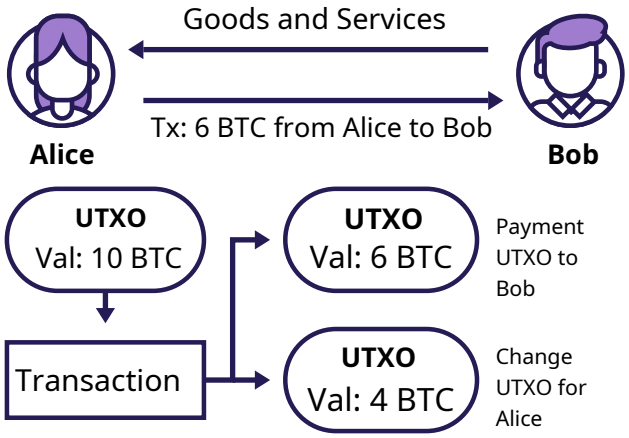
9.2 The UTXO Model

UTXO - Unspent Transaction Output

An Introduction to the Technical Side of Bitcoin

What Are UTXOs?

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



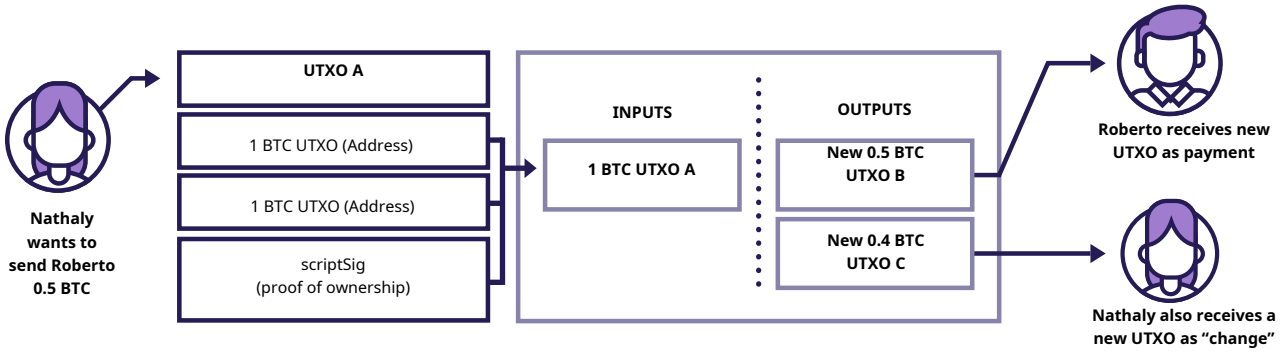
You can think of UTXOs as different sizes and pieces of bitcoin or differently denominated bills in your wallet. When you spend a UTXO, it is recreated into a new UTXO for the receiver, and whatever is left over is sent back to you in a different, new UTXO known as the "change UTXO." This is much like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

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

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

> It is important to note that you should not make others aware of your UTXOs because when someone knows them, they can track your bitcoin transactions in the network and will ultimately know how much money you own.

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



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

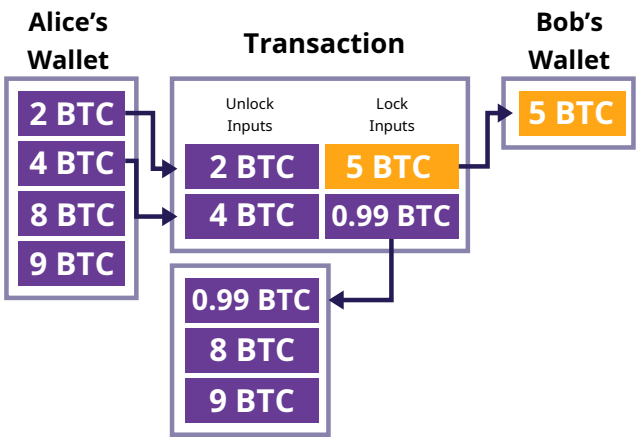
Chapter #9

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

An example to illustrate how this works: if you want to send two bitcoins but you only have a UTXO worth five bitcoins, the difference of three bitcoins is sent back to you as "change". This change is a new UTXO for you, and you can spend that new UTXO in a future transaction.

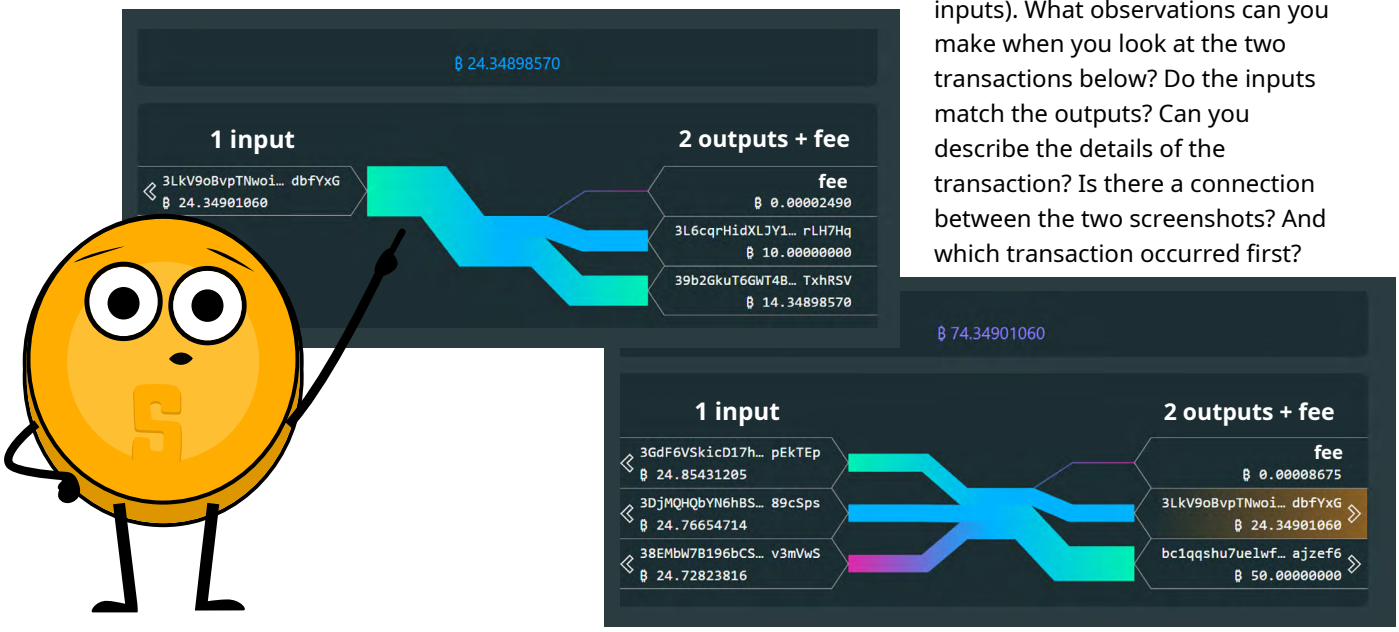
Another example:

1. Alice wants to send Bob five bitcoins.
2. She combines six bitcoins from two of her UTXOs
3. From these UTXOs, she sends five bitcoins toBob, gets 0.99 bitcoins as change back toherself, pays a 0.01 bitcoin transaction fee.
4. After confirmation, the transaction is added to Bitcoin's ledger, updating all the nodes that have a copy of the ledger.



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

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



9.3 A Closer Look at Bitcoin Nodes and Miners

In this section, we'll take a more detailed look at two very important parts (and participants) of the Bitcoin network that were first introduced in Chapter 6. We'll look at:

4 **Bitcoin Nodes:**

Gatekeepers of validation whose main job is to keep a copy of Bitcoin's ledger, making sure that all transactions are valid, and everyone follows the same rules.

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

2 **Bitcoin Miners:**

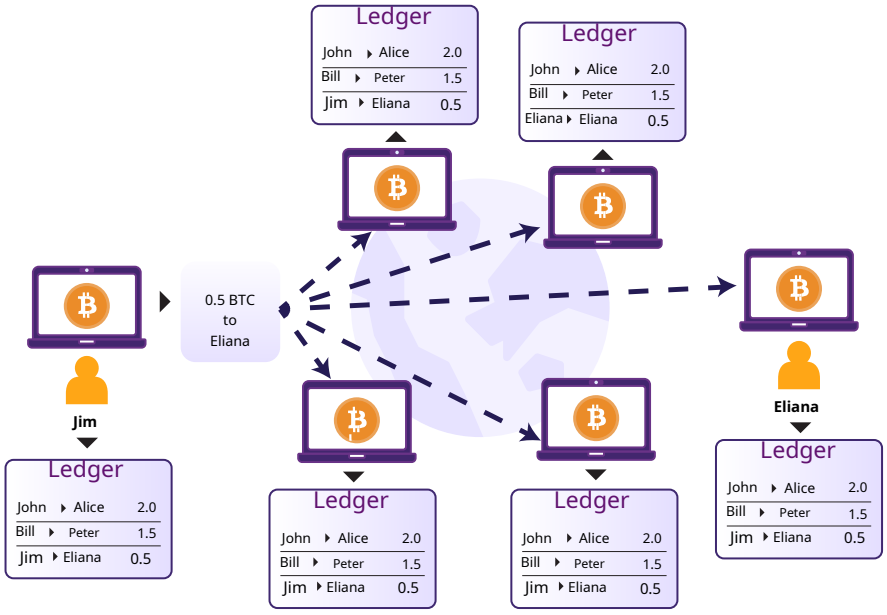
Architects of security that use powerful computers and electricity to check and confirm transactions, making sure everything is secure. This work helps make the ledger, or blockchain, resistant to any bad actors trying to mess things up.

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

9.3.1 What Is a Bitcoin Node and How Do I Set One Up?

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

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



Let's imagine a Bitcoin node as a digital traffic cop with some essential tasks:

1. **Gatekeepers of Validation:**

   A Bitcoin node keeps a digital copy of the blockchain, which is like a shared ledger of all bitcoin transactions. Many nodes around the world hold this same record.

2. **Communication Hub:**

   Nodes connect with each other, creating a vast communication network. They share information, especially transactions waiting to be added to the blockchain, stored in a digital waiting room called “mempool."

3. **Quality Checker:**

   Every addition to the blockchain undergoes scrutiny. Nodes ensure that transactions are valid, rejecting any that don't follow the rules of the Bitcoin network.

4. **Blockchain Informant:**

   Other software, like wallets, can ask a node for information about the blockchain, such as bitcoin balances. Nodes serve as information hubs.

5. **New Node Welcomer:**

   When a new node wants to join, existing nodes generously provide a copy of the blockchain. The new node independently checks the validity of each transaction, emphasizing a trustless system.

Activity:

Watch a video on Bitcoin Nodes

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

Resource:

Bitcoin Core Software

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

9.3.2. What Is a Bitcoin Miner and How Does Mining Work?

> The purpose of mining is not the creation of new bitcoin; that’s the incentive system. Mining is the mechanism by which Bitcoin’s security is decentralized.
>
> **My First Bitcoin**

An Introduction to the Technical Side of Bitcoin

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

Miners are in a race to add the next block to the blockchain. The sought-after prize is a "valid block hash," cleverly hidden among billions of others, and only a specific key assigned by the network can unlock it. Picture a massive haystack filled with millions of keys, each representing a unique block hash. The network has chosen one specific key to unlock a valuable reward. Miners rummage through the haystack, testing each key in the lock, but only one lucky miner will discover the perfect match.

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

Miners earn rewards for their efforts in two ways:

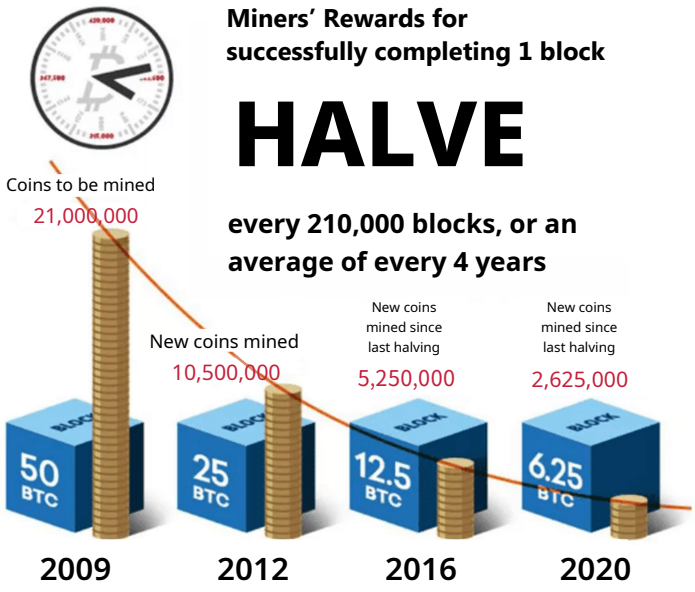
1. Block rewards
2. Transaction fees

Block rewards are new bitcoins 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.

Bitcoin Halvings

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

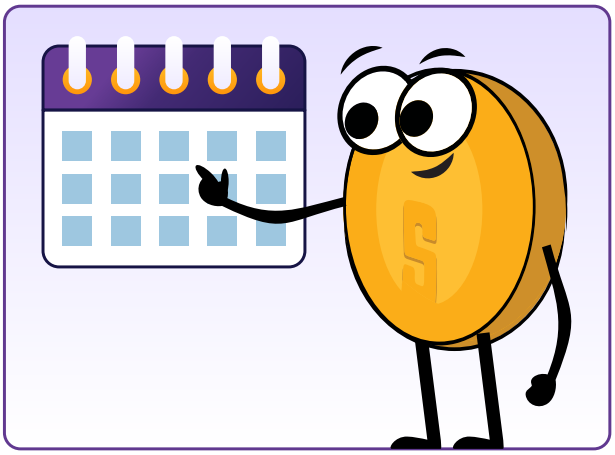
Satoshi Nakamoto cleverly designed a block reward system to distribute new bitcoins without a central authority. In Bitcoin's early days, miners got a sweet 50 bitcoin reward for each block they mined, motivating them to invest in powerful equipment and electricity for their mining operations.



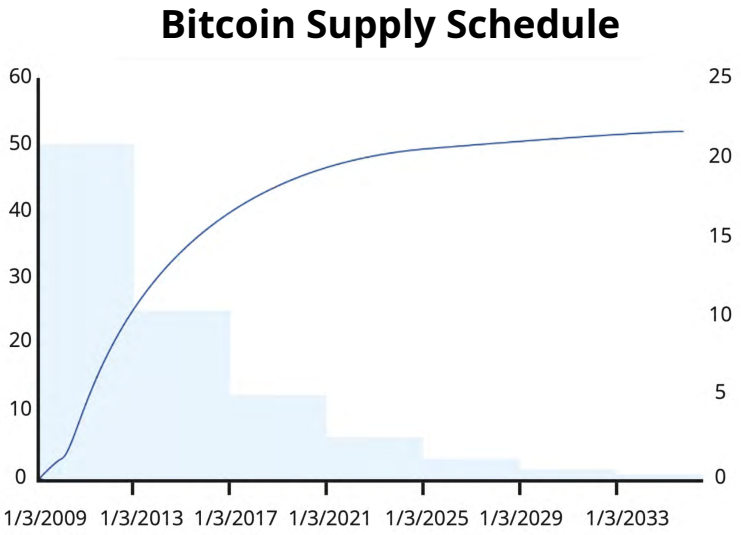
To keep the network stable and manage new bitcoin supply, the block reward is halved about every 210,000 blocks. This event, called "the halving," decreases the number of new bitcoins entering circulation and continues to motivate miners to protect the network and uphold its decentralization. Historically,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

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

During each halving event, miners receive smaller 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 bitcoins predictable and transparent.



The Bitcoin supply scheduleis the predetermined and public plan for the release of new bitcoins into circulation, designed to maintainBitcoin's scarcity over time.



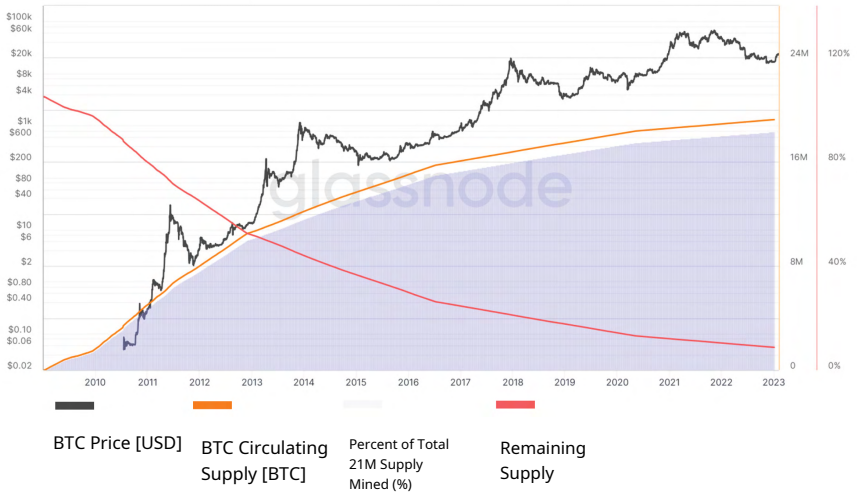
The following table outlines the details of upcoming halving events for Bitcoin, including the expected date of the next halving event, the block number at which the halving event will happen, the block rewards (per mined block) during that halving event, and the percentage of the total supply that will be mined.

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 %

An Introduction to the Technical Side of Bitcoin

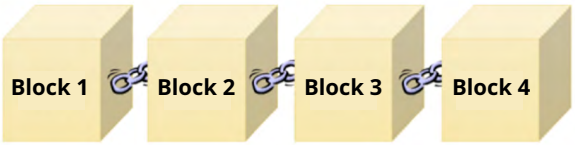
As more bitcoins are mined, the circulating supply and the percentage of the total supply that has been mined will keep increasing until the total supply of 21,000,000 is reached. The reduced supply, combined with rising demand, can boost Bitcoin's price (relative to the dollars). This benefits early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

Bitcoin: Percent of 21M Supply Mined

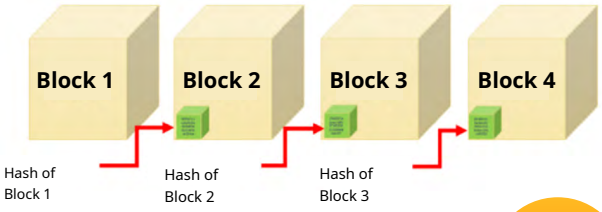


What Is a Valid Block Hash in Bitcoin?

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



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 dadata 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 fingerprint of the message.

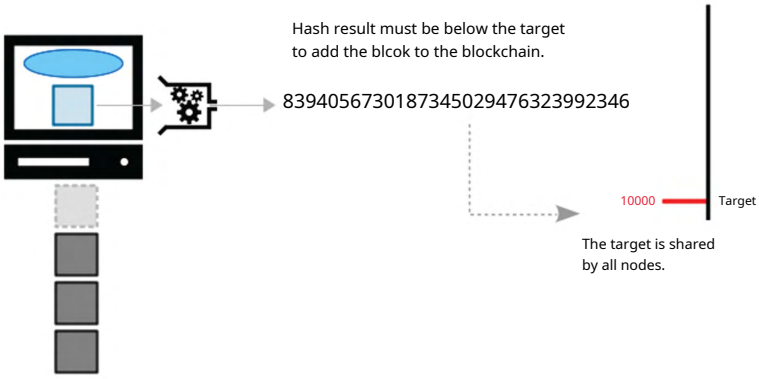


Satoshi Nakamoto, the creator of Bitcoin, mined the initial block, which held a total of 50 bitcoins.

The Race to Mine a Block

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

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



Let's say the target number set by the Bitcoin network is 1,000. The miners would have to use their computational power and energy to search for a block hash (a specific number) that is lower than 1,000. The first miner to find a block hash lower than 1,000 gets to add the new block to the blockchain and is rewarded with bitcoins.

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

For example, consider two different hashes:

- **Hash 1:** 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Difficulty level: 1
- **Hash 1:** 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Difficulty level: 2

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

> 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 they are paid a reward in bitcoins, plus transaction fees, for their effort. Proof-of-Work (PoW) is the method the Bitcoin network uses

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

In summary, the miner's tasks consist of:

1. **Bundling Transactions into Blocks:**

   While nodes verify newly created transactions that are waiting in the "Mempool," miners select a subset of these to include in their candidate block.

2. **Proof-of-Work:**

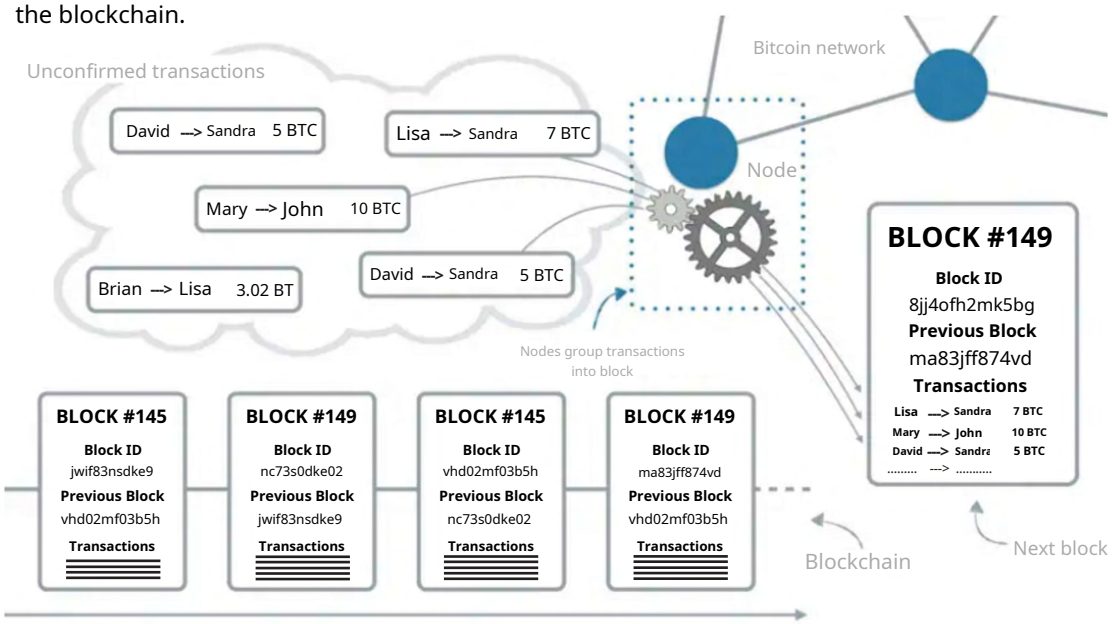
   Miners race with each other to find the valid block hash.

3. **Broadcast Valid Blocks:**

   After finding the valid blockhash, they propagate the new block to the network.

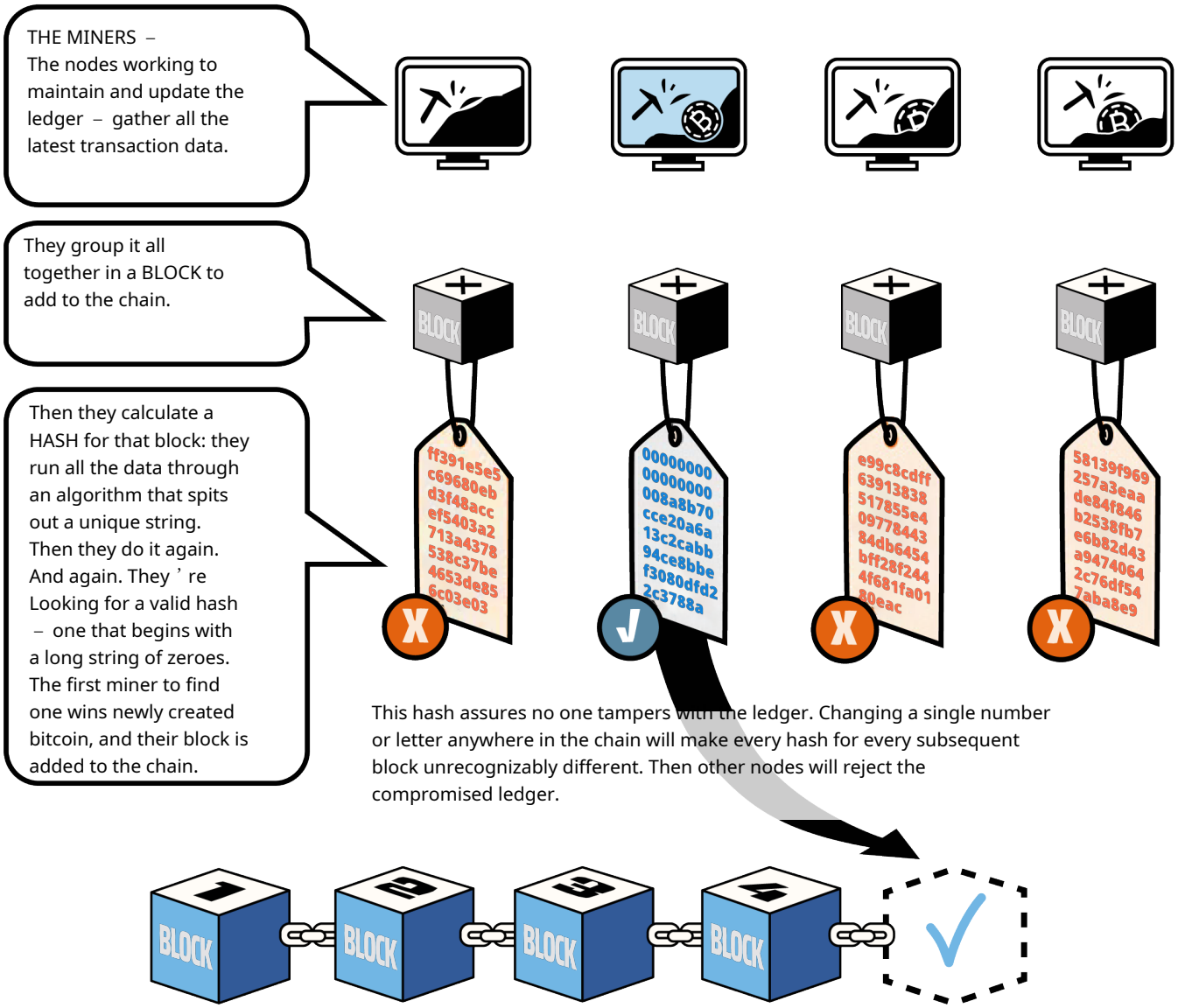
4. **Earn Rewards:**

   Lastly, they receive newly created bitcoins and transaction fees for successfully adding the block to the blockchain.



Multiple miners can work 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 set of transactions considered for addition to the blockchain that has

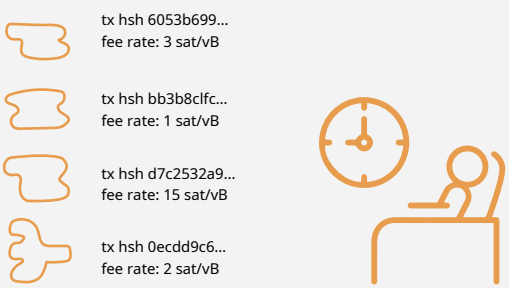


9.4 What Is the Mempool?

The "mempool" or memory pool is like a waiting room for transactions in the Bitcoin network. When you make a transaction, it is first broadcasted to the Mempool before it is verified, selected, and added to the blockchain.

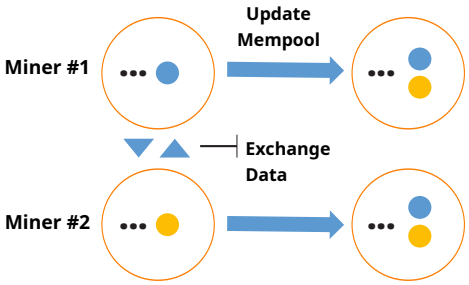
Imagine you are waiting in line at a restaurant. Your name is added to a list of people waiting for a table. When a table becomes available, the host calls your name and seats you. Similarly, a bitcoin transaction is added to the mempool when it is made and is confirmed and added to the blockchain when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

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



When a node first 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:

Relay unconfirmed transactions.

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 Are Transactions Verified and Added to the Mempool?

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

1. **Low Transaction Fees:**

   Transactions with low fees 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.

2. **Malformed Transaction:**

   If a transaction is malformed, it may be rejected by the network.

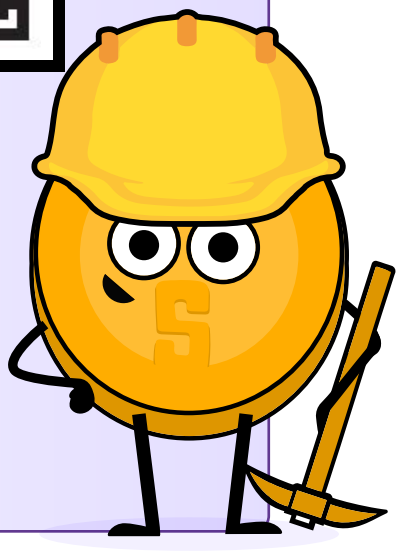
To avoid having transactions rejected, it's recommended to include a fee that is high enough to ensure the transaction is processed in a timely manner and to double — check that all the data in the transaction is correct before sending it.

Activity: Mempool

1. Scan the following QR code:

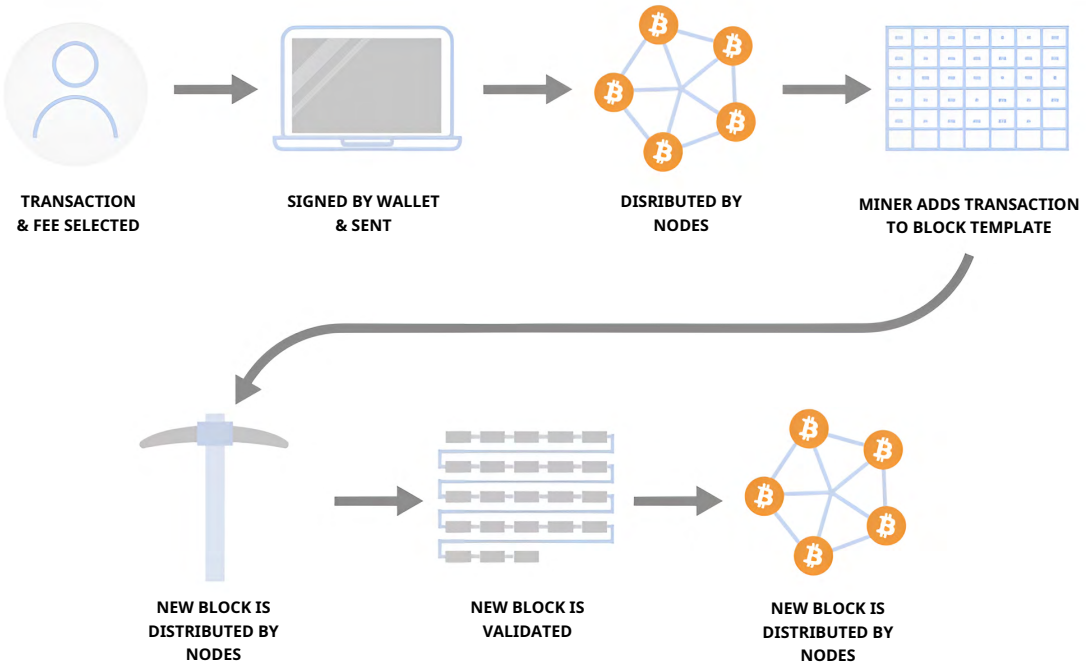
2. Review the various elements displayed on the page, including the latest blocks, confirmed transactions, number of transactions, memory usage, and approximate value of the entire block. Answer the questions:

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



An Introduction to the Technical Side of Bitcoin

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



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

4. The nodes on the network receive the transaction and verify its validity according to the consensus rules (like checking if Adam's signature is valid and if he has sufficient funds to make the transaction).
5. The transaction is marked valid, and the nodes propagate it to other nodes on the network, adding it to the Mempool.
6. Since Adam picked a high enough transaction fee, almost all miners include his transaction in their blocks.

7. Proof-of-Work: Miners race and try to mine their block by finding the valid block hash. One of the miners finds the hash and broadcasts their block to the network.
8. The nodes receive the newly mined block and verify its validity. This includes validating all transactions within the block and ensuring that the Proof-of-Work requirement is met.
9. The majority of nodes agree that the block is valid and add it to the blockchain. Gerardo receives the confirmed bitcoins at his receiving address.
10. As additional blocks are added to the blockchain in the subsequent hour, the number of confirmations for the transaction grows. As the number of confirmations for the transaction increases, Gerardo gains greater confidence in its success and irreversible nature.

In summary, the sender signs the transaction with their private key, the nodes verify the transaction UTXOs, and the miners add the verified transaction to the blockchain. The receiver can then access the bitcoins 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.

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

Chapter #10

Why Bitcoin?

10.0 Introduction

Activity: What Could a Bitcoin Future Look Like?

10.1 What Are Central Bank Digital Currencies (CBDCs) and

Who Controls Them?

10.2 The Philosophy of Bitcoin

Activity: Class Discussion — Do You Have the Right to

Control Your Own Money?

10.3 The Benefits of Bitcoin

10.4 An Empowered Future

Activity: Class Discussion — How Did Your Perspective Change?

Caietul elevului

Limba Română | 2025

Why Bitcoin?

10.0 Introduction

> Bitcoin is more than a currency; it's a revolution restoring power to the people, offering a taste of peace and freedom in a world hungry for empowerment.
>
> **My First Bitcoin**

In this concluding chapter, we'll summarize the lessons learned throughout our journey, ask and discuss a few important questions, and explore the future of Bitcoin.

Bitcoin is not just a technology; it's a type of network that powers a new form of money whose supply cannot be changed by any single party. Humanity has never had a form of money with a fixed supply and no centralized control. If widely adopted, Bitcoin is a tool that will unlock a movement for positive change that can transform the lives of people all over the world. It represents a peaceful revolution toward collective freedom and equity, opening up new opportunities for humanity by creating a shared, global monetary system.

As a decentralized global system, 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.

Activity: Watch the Video

The possibilities for positive change are immense, which is why we invite you to watch this video to learn more.

Next, we'll look at another form of digital currency called a Central Bank Digital Currency (CBDC) and evaluate how is similar and different to Bitcoin.

10.1 What are Central Bank Digital Currencies (CBDCs) and Who Controls Them?

Central Bank Digital Currencies, or CBDCs, are digital versions of regular fiat money. CBDCs follow the same rules as regular fiat money, where a central authority, like the government, can create more supply thereby reducing people's purchasing power. However, CBDCs also grant governments new and potent tools to control how that money is used by people around the world.

According to the Human Rights Foundation (HRF) research, 119 out of 193 governments worldwide are looking into,

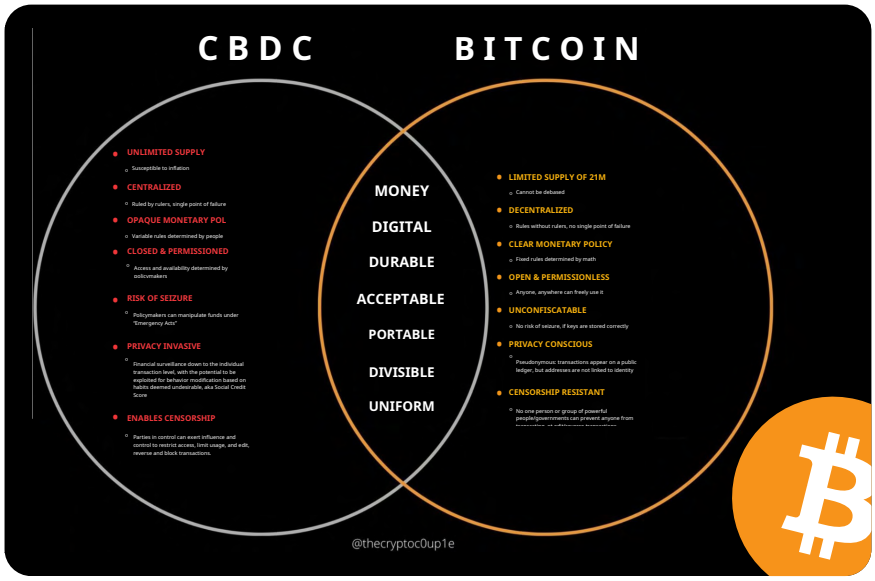
You can check if your country is trying CBDCs on the Human Rights Foundation's CBDC tracker at

https://cbdctracker.hrf.org/home or https://cbdctracker.org/

So, what makes CBDCs different from regular fiat money besides being digital? It's crucial to understand that, unlike regular fiat money in the form of paper or coins, CBDCs let the government digitally watch and control every transaction globally. This means the government can stop certain transactions or even freeze your whole account if they don't like you or how you're using your money.

For example, imagine you want to send money to a family member in a country that needs help but your local government rejects your transaction because they don't agree with that country's leaders. Or picture going to the store to buy something you like but you can't because you expressed your opinion on social media.

CBDCs give governments unlimited power to control how money is used around the world, limiting individuals' ability to spend money based on their own choices. Some even argue that CBDCs would enable powerful governments to centrally enforce tyrannical policies on a global scale at the flick of a switch, without the need for human enforcement agents.



Both CBDCs and Bitcoin are digital, but beyond this commonality, they represent very different forms of money with distinct philosophies, leading to varied outcomes for humanity.

10.2 The Philosophy of Bitcoin

In Chapters 6 and 9, we discovered that individuals who run a node help keep Bitcoin's rules safe. This is a big deal because, for the first time ever, people like us can be part of a team that ensures the rules of our monetary system are protected. These rules include the fact that there's only a limited amount of money, and no one single party can change these rules. It's a unique opportunity for regular people to help keep our money secure and reliable.

Bitcoin's philosophy is about empowerment, freedom, financial independence, critical thinking, and the concept that we should all have a say in the rules of the system we choose for ourselves. Unlike the fiat system controlled by powerful central parties, Bitcoin works on a network where no single party has all the control. This means, unlike with other types of money like CBDCs, no one can take your property from you or stop you from spending your money the way you want.

In the fiat world, having more wealth directly translates to having more influence and control. Contrastingly, Bitcoin operates in a way that's all about power to the people. It's a team effort where everyone, no matter how much money they have, plays a crucial role in the system. Imagine it as a collective force, where your financial size doesn't automatically mean you control everything. Bitcoin is built on unchangeable rules, and, in this harmony, it's as if humanity itself is in control of the system. It's not a few big-shots calling the shots; it's all of us working together, as a resilient community, guiding the course of Bitcoin without any single authority telling it what to do.

While in the fiat system the powerful dictate the rules, in the Bitcoin ecosystem, it's the collective strength of individuals that sustains the network. No single entity, regardless of wealth, can dictate the path of the Bitcoin ecosystem. It's an inversion of the traditional power dynamic, where the system's resilience lies not in the hands of the few but in the collective power of every participant.

The main idea is to create a safe, clear, and fair system where everyone can access global money equally.

Activity: Class Discussion — Do You Have the Right to Control Your Own Money?

1. Is money a human necessity and a human right? And why?
2. If you can’t spend your money how you want, send it to who you want, or take your money with you to a new country, is it really yours? And why?
3. Why did barter stop being used? What is the problem with the double coincidence of wants?
4. What historical event was the most impactful for you? Why is it important to understand the Nixon shock and its relevance for everyone today?
5. How is money with a fixed supply different from traditional fiat currencies?

6. When was Bitcoin created, by whom, for what purpose, and how does this purpose define the concept of a decentralized system?
7. What is the difference between a custodial and a non-custodial wallet? What was your favorite wallet?
8. What do you understand about the Lightning Network? What type of transactions would you use it for?
9. Why does running your own node support the network?
10. How does having control over your own money empower you in your daily life and future planning?
11. In what ways can financial freedom enhance your ability to contribute positively to your community or society?

10.3 The Benefits of Bitcoin

”Hyperbitcoinization” is a theoretical future where Bitcoin becomes the dominant global monetary system. This would mean that Bitcoin would be used by everyone, everywhere, and for everything — from buying coffee to paying bills and even buying property.

The growing interest in Bitcoin among individuals, businesses, countries, and governments highlights the potential impact of its widespread adoption on the economy and society. Here are some of the benefits of a hyperbitcoinized world:

1. **A Self-Sovereign Future:**

   A self-sovereign future is one where individuals worldwide have full control over their own digital identity and assets. This could lead to greater financial inclusion, freedom, privacy, and security, and thereby contribute to heightened human flourishing, abundance, and overall happiness.

2. **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.

3. **Changes in Monetary Policy:**

   If Bitcoin were to become widely adopted, it could take away government's ability to control the money supply through traditional monetary policy tools. Mass adoption of Bitcoin would potentially increase people’s purchasing power and encourage society to move toward low-time preference activities.

4. **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. Currently, powerful entities have the ability to move trillions of dollars around the world without clear visibility into where these funds go or how they are utilized. By providing an open and verifiable record of financial transactions, Bitcoin could ensure that the movement of capital becomes more accountable and accessible to the public.

5 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. The Lightning Network offers fast and inexpensive 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.

1 Abundant Energy:

When there's a lot of affordable energy, societies do well, and many industries and communities can meet the increasing need for power in homes, businesses, and new technologies. Bitcoin mining incentivizes miners to use surplus energy that would usually go to waste from sustainable energy sources like solar, wind, and hydroelectric power. Bitcoin miners use this surplus energy to create new bitcoins through mining activities, secure the network, and offer excess energy they create back to the energy grid society uses when it is needed.

10.4 An Empowered Future

Bitcoin is money.

Money helps people communicate which activities, goods, and services are most important within society. As we have seen in this course, when money is controlled by centralized authorities, it will be manipulated.

One of the mistakes humanity keeps repeating throughout history is manipulating money, which then negatively affects individuals, families, businesses, governments, and ultimately global human prosperity.

By taking control of money out of the hands of centralized parties and instead using money with a fixed supply that no single party can change, we create a different world — one where we don't have to trust that people will do the right thing but rather one in which people is unable to do the wrong thing.

This is a fundamentally different world.
And you, dear student, can be a part of creating this world. By using Bitcoin, running your own node, and helping your fellow humans learn more about the future of money, you are voting for a different world.

Activity: Final Class Discussion — How Did Your Perspective Change?

Please answer the five questions below:

Why do we need money?

What is money?

Why Bitcoin?

Who controls money?

What gives money its “value”?

Chapter #10

Write down the questions posed by students that were selected during Chapter 1 and answer them.

1. **Go back to the first activity in Chapter 1 and compare your new answers to your old answers.**
2. **Compare and discuss the original answers and questions. Did something change?**
3. **Ask yourself this final question: What is my next step? And how can I use this new knowledge to empower myself?**

If you're ready to take the next step, check out the additional resources in the following section, where we have selected the best resources for further learning and success.

Additional Resources

1. Why Use Bitcoin?

a "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.

b "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.

c "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.

2. What Is Bitcoin?

a "How Bitcoin Works under the Hood" by CuriousInventor:

https://www.youtube.com/watch?v=Lx9zgZCMqXE This video provides a detailed explanation of the technical aspects of Bitcoin and how it works.

b "What Is Bitcoin" by Greg Walker:

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.

c "Intro to Bitcoin Austrian Thought" (1 hour):

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.

3. Further Learning:

a "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.

b "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.

c "Bitcoin Babies"

https://learning.chaincode.com/#FOSS: Online courses and a residency program which enables students to learn the skillsnecessary to work on Bitcoin protocol development.

d BTC Sessions

A Bitcoin-only education YouTube channel with useful tutorials and guides: https://www.youtube.com/@BTCSessions

4. Courses:

a Summer of Bitcoin

https://www.summerofbitcoin.org/: A global, online summer internship program focused on introducing university students to Bitcoin open-source development and design.

b Chaincode Labs

https://learning.chaincode.com/#FOSS: Online courses and a residency program which enables students to learn the skillsnecessary to work on Bitcoin protocol development.

c Saylor Academy

Free education across multiple disciplines: https://www.saylor.org/

5. Important Authors

- a Alex Gladstein: Check Your Financial Privilege
- b Alex Swan: Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications
- c Amanda Cavaleri: Bitcoin and the AmericanbDream: The New Monetary Technology Transcending Our Political Divide
- d Anita Posch: Learn Bitcoin: Become Financially Sovereign
- e Eric Yakes: The 7th Property: Bitcoin and the Monetary Revolution
- f Jeff Booth: The Price of Tomorrow: Why Deflation is the Key to an Abundant Future
- g Jeff Booth: The Price of Tomorrow: Why Deflation is the Key to an Abundant Future
- h Nik Bhatia: Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies
- i Robert Breedlove: Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money
- j Lyn Alden: Broken Money

6. Cited Authors

a Curious Inventor: https://www.youtube.com/@CuriousInventor

b Anil Patel: Twitter: @anilsaidso

7. Other Resources:

1. **Bitcoin.org:** The official website of the Bitcoin protocol.
2. **Bitcointalk.org:**
   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 Bitcoinenthusiasts and experts.
3. **Bitcoincore.org:**
   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.
4. **Bitcoinwiki.org:**
   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.
5. **Bitcoinmagazine.com:**
   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.
6. **Bitcoin.Design:**
   An open-source repository of bitcoin-related design files for illustrations, websites, templates, and icons.
7. **Simple X:** https://nostr.com
   Social media where you actually own your data.
8. **Simple X:** https://simplex.chat/
   A private, decentralized application protocol.
9. **Set up a Bitcoin Node:** Raspberry Pi DIY by Keith Mukai:
   https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?t ab=readme-ov-file
10. **How to select a Bitcoin wallet:** https://bitcoin.org/en/choose-your-wallet
    Use your newly gained knowledge to select the right wallet for you.
11. **BitcoinIcons.com:** https://bitcoinicons.com/ -
    A collection of free Bitcoin icons.
12. **Bitcoin For Local Business:** https://bitcoinforlocalbusiness.com/
    A set of fliers to help you share the value of Bitcoin with your favorite local businesses.
13. **Mempool.Space:** https://mempool.space/
    An open source Mempool project which also features Lightning Network data and graphs.
14. **Yzer:** https://yzer.io/
    An open-source repository of bitcoin-related design files for illustrations, websites, templates, and icons.

Chapter Key Concepts

Chapter 1:

Course Introduction:

Explore the course objectives and expectations for the Bitcoin Diploma.

Reflective Activity — Defining Money:

Engage in a reflective exercise by providing five answers to key questions about money.

Class Discussion — Why We Need Money:

- Participate in a class-wide discussion exploring the fundamental necessity of money.
- Share and compare individual perspectives on the importance of money.
- Lay the groundwork for understanding the role of money in economic systems.

Chapter 2:

Understanding Money:

- Explore the fundamental definition and concept of money.
- Discuss the diverse perspectives within the class to grasp the multifaceted nature of money.

Functions, Properties, and Types:

- Delve into the functions, properties, and types of money.
- Recognize the importance of these aspects in defining and utilizing money..

Psychology of Money:

- Understand the psychological aspects of money, including scarcity, time preference, and tradeoffs
- Engage in the "Time Preference" activity to relate psychological elements to real-life scenarios

Chapter 3:

Introduction to Money's History and Evolution:

Explore the history and evolution of money. Understand how ancient forms of trade led to the development of the currency we use today.

Digital Currency Revolution:

- Discover the current pinnacle of money's evolution — digital currency.
- Understand how it exists only in electronic form, enabling instantaneous, low-cost transactions globally.
- Learn about the significant role Bitcoin played in solving early challenges of digital currencies, making them ready for worldwide use.

Evolution of Currency:

Explore the transition from ancient forms like shells and beads to the emergence of coinage and paper money. Follow the journey from paper to plastic, unraveling the evolution of currency throughout history.

Barter Game Activity:

Engage in a hands-on barter game experience to grasp the challenges of direct exchange and appreciate the need for a more efficient system.

Chapter 4:

Fiat Money Origins:

Explore the origins of fiat money through a brief historical overview, understanding how it became a dominant form of currency.

Fractional Reserve Banking Activity:

Engage in the Fractional Reserve Banking activity to gain insights into how this system operates, highlighting its reliance on debt and the implications for the broader economy.

The Fiat System:

Grasp the fundamental aspects of the fiat system, including its nature as a monetary system by decree, the role of fractional reserve banking, and the key players controlling this system.

Chapter 5:

Decreasing Purchasing Power:

Understand the concept of monetary inflation and its impact on purchasing power. Engage in the Effects of Inflation: An Auction Activity to experience the effects firsthand.

The Fiat System's Consequences Activity:

Participate in the Consequences of the Fiat System activity, shedding light on the broader repercussions of the current monetary
framework.

Central Bank Digital Currencies (CBDCs):

Explore the evolving landscape of Central Bank Digital Currencies (CBDCs) and their potential impact on the future of money.

Global Debt Burden and Social Inequality:

Explore the dual impacts of the global debt burden and social inequality. Recognize the individual and societal consequences, emphasizing the loss of purchasing power and the widening wealth gap.

The Cypherpunks and Decentralization:

Learn the Cypherpunks' story and their motivation for seeking a decentralized currency. Differentiate between centralized and decentralized systems, gaining insights from a brief history of digital currencies.

Chapter 6:

Satoshi Nakamoto and Bitcoin's Creation:

Explore the mysterious figure of Satoshi Nakamoto and the origin story of Bitcoin, understanding the initial motivations behind its development.

Class Activity — Consensus Building:

Engage in the Consensus Building in a Peer-to-Peer Network activity to gain practical insights into how consensus is achieved within the Bitcoin network.

Embracing Personal Responsibility:

Emphasize the concept of personal responsibility in the context of Bitcoin, encouraging an understanding of individual roles and accountability within the decentralized ecosystem.

How Bitcoin Works:

A look into the mechanics of Bitcoin, including the Nakamoto Consensus Mechanism. Identify the key players in the Bitcoin network, such as miners, nodes, users, developers, and projects, and grasp the collaborative dynamics between them.

Bitcoin as Sound Digital Money:

Examine Bitcoin's role as sound digital money, discussing its evolution, functions, and properties, and participate in a class discussion on whether Bitcoin qualifies as sound money.

Chapter Key Concepts

Chapter 7:

Peer-to-Peer Transactions:

Engage in decentralized transactions to experience the core principles of Bitcoin exchanges.

Setting Up a Bitcoin Wallet:

Learn the essential steps to download, create keys, and back up a Bitcoin wallet for secure transactions.

Saving and DYOR:

Understand saving in Bitcoin as a store of value and the importance of independent research for informed decision-making.

Bitcoin Wallet Types:

Differentiate between open source, closed source, custodial, and noncustodial wallets, understanding the role of keys in security.

Acquiring Bitcoin:

Explore methods like peer-to-peer transactions and exchanges, discussing privacy concerns related to KYC processes.

Chapter 8:

Introduction to Lightning Network:

Recognize the evolution of Bitcoin through technologies like the Lightning Network, enhancing its capabilities.

Setting Up a Lightning Wallet:

Learn the essential steps to set up a Bitcoin Lightning wallet, facilitating faster and more scalable transactions.

Hands-On Activity:

Engage in a practical Lightning wallet relay race, promoting a dynamic understanding of Lightning Network transactions.

Lightning Wallet Types:

Differentiate between open source, closed source, custodial, and noncustodial Lightning wallets for varied user preferences.

Lightning Transactions:

Explore the process of sending and receiving Lightning transactions, emphasizing the speed and efficiency of the Lightning Network.

Chapter 9:

The Bitcoin Ledger:

Understand the concept of a decentralized ledger facilitated by nodes and miners, ensuring transparency and security.

The UTXO Model:

Grasp the Unspent Transaction Output model as a fundamental aspect of Bitcoin's transaction process.

Public and Private Keys:

Explore the significance of cryptographic security in Bitcoin transactions through public and private keys, along with an activity demonstrating SHA 256 hashing.

Bitcoin Nodes and Miners:

Look into the roles of nodes and miners in maintaining the Bitcoin network, covering aspects like issuance, scarcity, halving, and difficulty.

How Bitcoin Transactions Work:

Gain insight into the entire lifecycle of a Bitcoin transaction, involving the sender, receiver, nodes, miners, and the mempool, with a dedicated activity focused on the mempool.

Chapter 10:

Philosophical Underpinnings of Bitcoin:

Explore the foundational philosophy behind Bitcoin, understanding how it emerged as a response to economic challenges, with a focus on its impact on financial freedom and how it differs from traditional currencies.

Bitcoin's Future:

Delve into the potential trajectory and future developments of Bitcoin as a revolutionary digital currency.

Diploma Reflection:

- Summarize key takeaways from the Bitcoin Diploma, encouraging students to reflect on their journey and insights gained.
- Activities include watching a video on "why Bitcoin?" and revisiting Chapter 1's questions to assess personal growth in understanding.

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.

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.

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 bitcoins. 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.

Centralized System:

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 by which "miners" verify the authenticity of transactions with their computer hardware and software. It is recommended to wait for at least six 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.

Digital Asset

A digital representation of value that can be traded or used as a store of value, such as bitcoins.

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 send their bitcoins to two different recipients at the same time.

Dust Transaction:

A transaction that sends a very small amount of bitcoins that is too small to be economically viable.

Glossary

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 that is not compatible with the previous version (i.e. 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 ofconsensus, 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.

Hash Rate:

A way to measure the processing power of the Bitcoin network.

Lightning Network:

A layer-2 payment protocol that enables faster and cheaper bitcoin transactions by using off-chain channels for smaller transactions.

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 bitcoins.

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.

Monetary and Fiscal Policy:

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, oftenused to represent art, collectibles, or other unique objects.

Nonce:

A random number added to a block header to create a hash that meets the difficulty target.

Orphan Block:

A block not included in the main chain of the blockchain due to being invalidated by a longer competing chain.

Glossary

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:

blockchain 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 to participate in the network.

Public Blockchain:

A blockchain open to anyone to participate in and verify transactions, making it decentralized.

Public Key:

A unique identifier used for receiving bitcoins 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:

Money's ability 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 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 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.

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 goods or services is determined by the interaction of the quantity of the goods or services supplied and the quantity 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:

small amount of bitcoins paid by the sender of a transaction, incentivizing 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.

Glossary

Transaction:

The transfer of bitcoins 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.

XBT and BTC:

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 bitcoins 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 bitcoins similar to a physical wallet that contains private key(s) that allow you to spend the bitcoins 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 that a blockchain project or cryptocurrency is trying to address and its solution.

XBT and BTC:

Abbreviations for bitcoin.

Independent because of you!

THANKS TO THE DONORS WHO CONTRIBUTED TO OUR GEYSER CAMPAIGN OR AT ADOPTING BITCOIN 2024

Mi Primer Bitcoin

Alireza
Ratio Freedom
LOUIS HOLBROOK
Alvin Delgado
Mark Sierra
Roberto Magana
Hubertus
Michael Hong
ROGZY
Kyle Huber
Rain International
Timothy McMahon
Golaizeo-Shekecan
LeeBlc
ANDREAS KOHL
Rosi Collejas Morales
Arnold
Dale Cumbee
Mike Peterson
Pamela News
PIERRE BONHOMME
Rob G
Juan Mayen
Philipp Hartmann
@psah91
Jorrit
Tim & Noelle Australia
Bitcoin Berlin
Mayra Grice
FREE MADEIRA
CARCAHO
NACHO
Bitcoin
Describe
Maziccia
Fife Family
Gerardo
Luis Verduzco
Guido
Stelios
Maximilian Madrid
Madison Madrid
tetakta
HENRIQUE ALBUQUERQUE
(FROM FREE MADEIRA)
lightsats
@LaCasaDeSatoshi
Matt
@CodingInLondon
Dr. Mathias Linkerhand
@Mathias_UMF596
Arel Edelkamp
OPI
the orange pill
Limburg3rt
K1
Stephan Jaeckel
Edgar Hernandez
Vladimir Kristić
tweetious
Lindy Frit
Jiria for Bitcoin!
LUIS SATOSHI
SHULTON CITY
B&E
Adrián Treviño
Estefany Fagioli
clusk
Sergio Benedetti
Jurjen de Vries
Ben de Waal
Nelson Imo
Jeremy Almond
Roger Hong
Rick Lions
JAPHY RIDER
Brad & Angelica Long
Jeff Hephner
Daniel "DJ" Jones
Jonathan Yagoobian
Andrés Posada
Regina Chicas
Rubiano
Will Ramirez
-SJEC-
Samantha de Wool
(@SamHodlGirl)
Mario from Bitcoinstuff.com
ERIC SUMMERS
@ericscalibur
Diana d Morius
Hurley
Jason Howard
Jose Rodriguez
Christian Ehrenmann
Emilio Rivas
Bart Gaik
Christian Blaze
KENT HALLIBURTON
Legalitika
Bula
Rob Wallace
Guillermo Hunung
ADVENTURES IN PERSUING FREEDOM
Chicas

Thank you!

English Version | 2025