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

Cuprins

Capitolul #1 - De ce avem nevoie de bani?

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

Capitolul #2 - Ce sunt banii?

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

Capitolul #3 - Istoria banilor

3.0 Introducere 21

Activitate: Jocul Trocului 21

3.1 Evoluția de la troc la moneda modernă 23

3.1.1 Problemele formelor timpurii de bani 23

3.1.2 Dezvoltarea monedelor și a banilor de hârtie 24

3.1.3 Tranziția de la monedă sănătoasă la monedă fără acoperire 25

3.1.4 De la hârtie la plastic 27

3.2 Moneda digitală 31

Capitolul #4: Ce sunt banii fiat și cine îi controlează?

4.0 Introducere 31

4.1 Scurtă istorie a banilor fiat 31

4.2 Sistemul Fiat 34

4.2.1 Un sistem monetar prin decret 34

4.2.2 Rezerve fracționare: Un sistem alimentat de datorii 35
Activitate: Rezerve fracționare 38
4.2.3 Cine controlează sistemul fiat și cum beneficiază? 39
4.3 Monedele digitale ale băncilor centrale: Viitorul banilor fiat 41

Capitolul #5: Cum Problemele Duc la Soluții

5.0 Introducere în Problemă 45
5.1 Scăderea Puterii de Cumpărare 45
5.1.1 Inflația Monetară și Efectul asupra Puterii de Cumpărare 45
Activitate: Efectele Inflației - O Activitate de Licitație 46
5.2 Povara Datoriei Globale și Inegalitatea Socială 47
5.2.1 Impactul asupra Individului - Pierderea Puterii de Cumpărare 47
5.2.2 Impactul asupra Societății - Creșterea Inegalității Averii 52
Activitate: Consecințele Sistemului Fiat 53
5.2.3 Povara Datoriei Globale 55
5.3 Cypherpunks și Căutarea unei Monede Descentralizate 55
5.3.1 Cypherpunks 56
5.3.2 Sisteme Centralizate vs Sisteme Descentralizate 57
5.3.3 Scurtă Istorie a Monedelor Digitale 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

Este esențial să ai o înțelegere solidă a bazelor banilor, a istoriei lor și a sistemului financiar actual înainte de a studia Bitcoin. Înțelegerea acestor concepte oferă o fundație puternică pentru a înțelege natura unică și disruptivă a Bitcoin. Prin învățarea despre evoluția banilor, vei putea înțelege mai bine potențialul și limitările sistemului financiar actual și modul în care Bitcoin își propune să le abordeze. Fără această fundație, poate fi dificil să apreciezi pe deplin semnificația și impactul potențial al Bitcoin. Ai încredere în procesul de învățare și rămâi concentrat, deoarece recompensa unei înțelegeri mai profunde și a unei aprecieri a acestui domeniu de vârf va merita cu adevărat.

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?

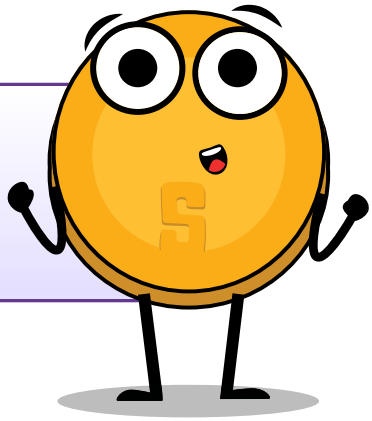
1.0 Introducere

> 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

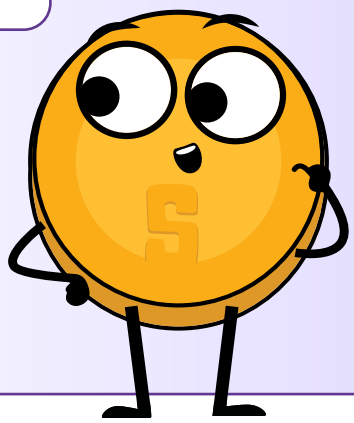
> Banii sunt o garanție că putem avea ce ne dorim în viitor. Chiar dacă nu avem nevoie de nimic acum, ei asigură posibilitatea de a satisface o nouă dorință când apare.
>
> **Aristotel**

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.

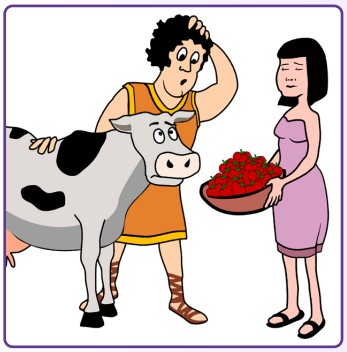
Tranzacția este un schimb sau transfer de bunuri și servicii. Este o modalitate de a schimba valoare între două sau mai multe părți.

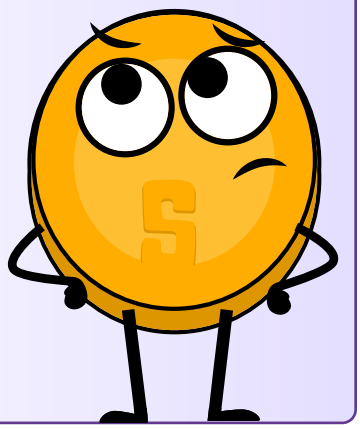
Există multe tipuri de tranzacții, de la schimburi simple (cum ar fi cumpărarea unui sandviș la o cafenea) la tranzacții financiare complexe (cum ar fi cumpărarea unei case sau investiția în acțiuni sau obligațiuni). Tranzacțiile pot fi realizate față în față, la telefon, online sau prin alte mijloace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

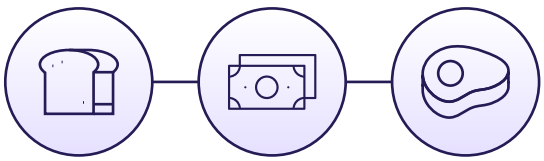
1 Depozit de valoare

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.

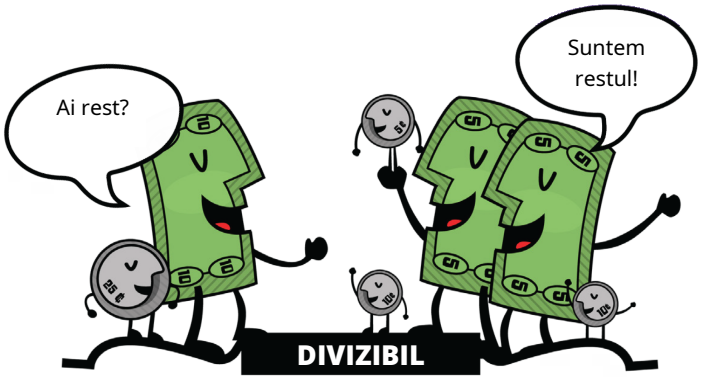
Exercițiu în clasă: Ce funcție a banilor este exemplificată aici?

- 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

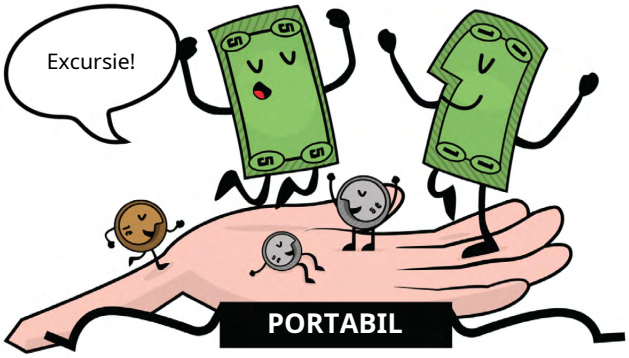
De-a lungul timpului, oamenii au realizat că banii trebuie să aibă anumite calități pentru a fi eficienți ca mijloc de schimb. Aceste caracteristici includ durabilitate, divizibilitate, portabilitate, acceptabilitate, raritate și fungibilitate.

- 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.

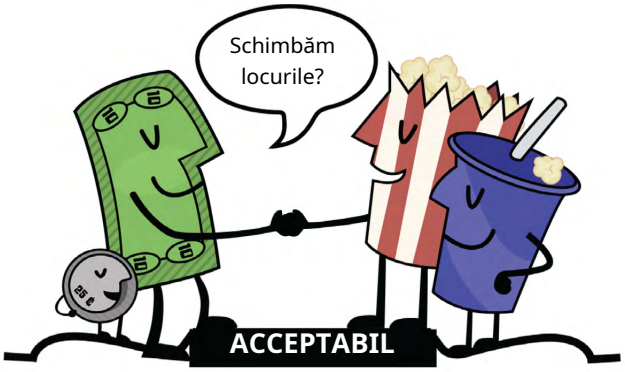


Ce sunt banii?

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.

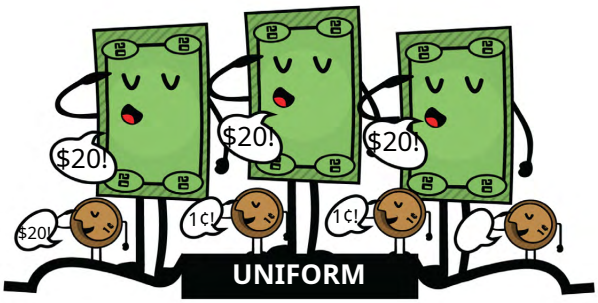


Acceptabilitate se referă la acceptarea pe scară largă a banilor ca formă de plată, astfel încât oamenii să-l poată folosi cu încredere pentru a cumpăra și vinde bunuri și servicii. Dolarul american este larg acceptat ca formă de plată, fiind o bună reprezentare a acceptabilității banilor.



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?

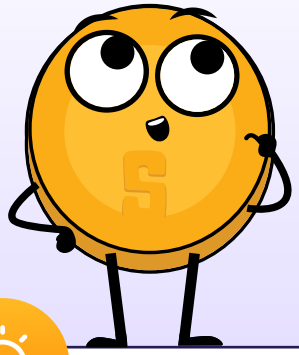
2.4 Tipuri de bani

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

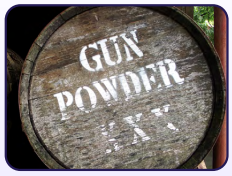
Banii fizici includ:

- 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

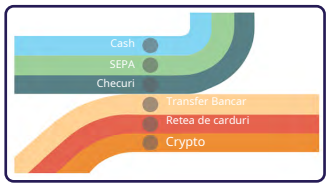
Moneda reprezentativă, precum acest certificat de argint, putea fi răscumpărată în argint.

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

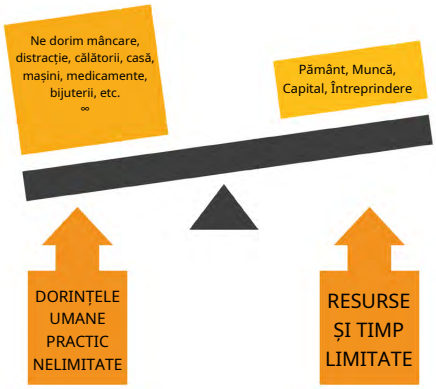
Imaginează-ți că ești blocat în deșert și ai doar o sticlă de apă rămasă. Ești însetat și disperat după o gură de apă, dar știi că vei avea nevoie de apă ca să supraviețuiești până găsești mai multă. Acesta este un exemplu clasic de raritate – ai doar o cantitate limitată dintr-o resursă (apă) și trebuie 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.

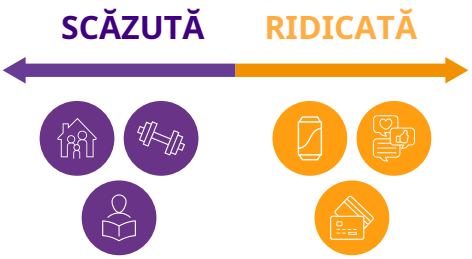
Există două tipuri de raritate: creată de om și naturală.



- 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.

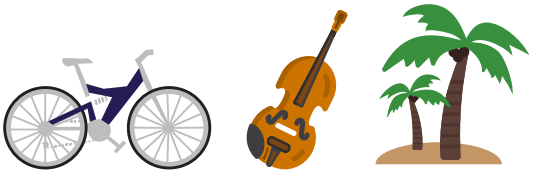
Ce sunt banii?

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

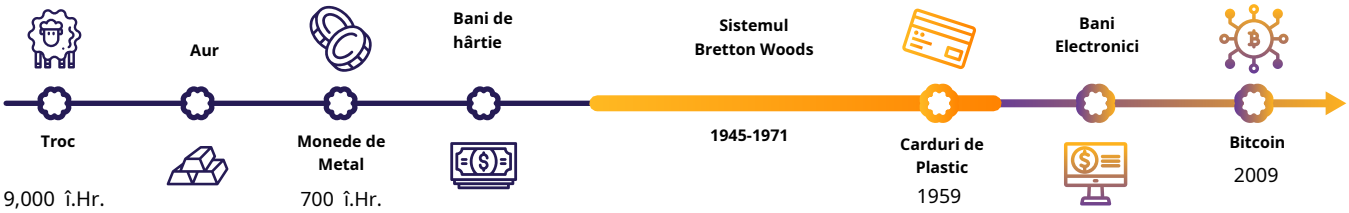
Caietul elevului

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)?

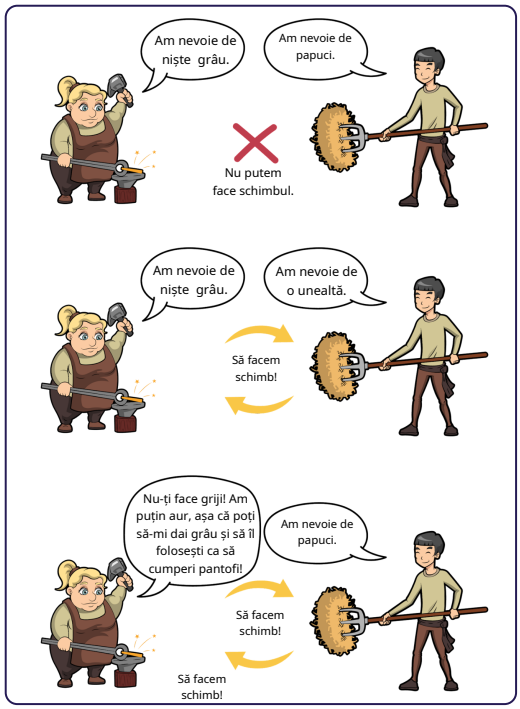
3.1 Evoluția de la troc la moneda modernă

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.

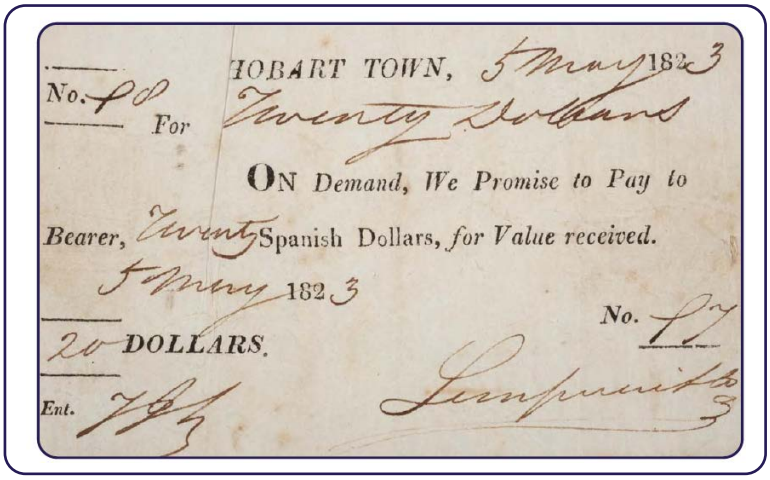
Acesta este al doilea episod intitulat „Nu doar tăiței", din seria „Istoria banilor de hârtie".

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.

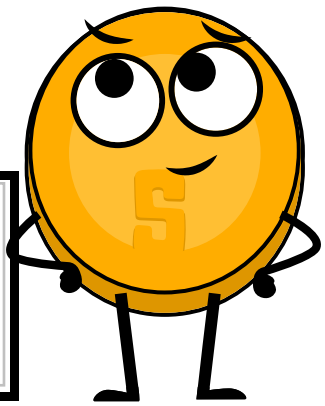
Pentru a rezolva aceste probleme, comunitatea începe să folosească chitanțe de hârtie ca formă de bani.

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.

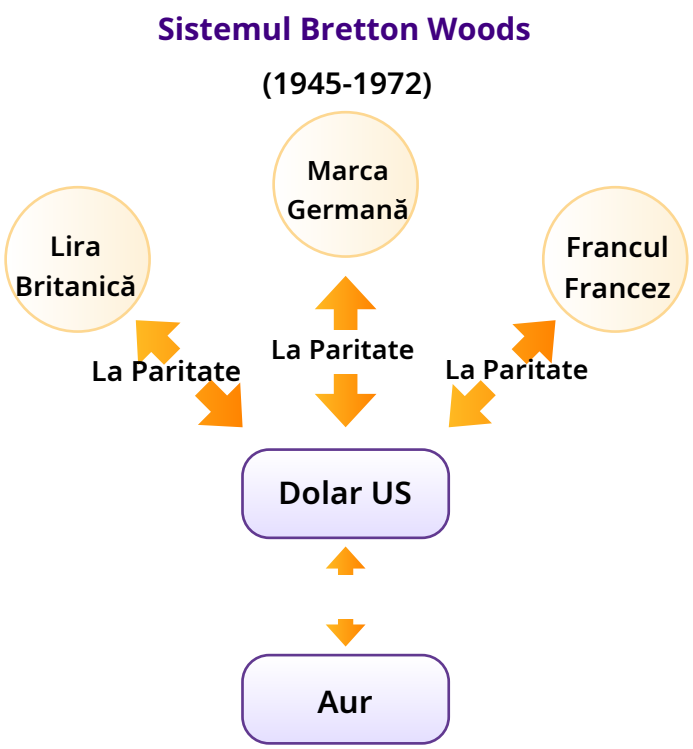
Ce se întâmplă când încerci cu adevărat să pui în practică doctrina banilor de hârtie? Află în episodul al patrulea din seria „Istoria banilor de hârtie”.



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:

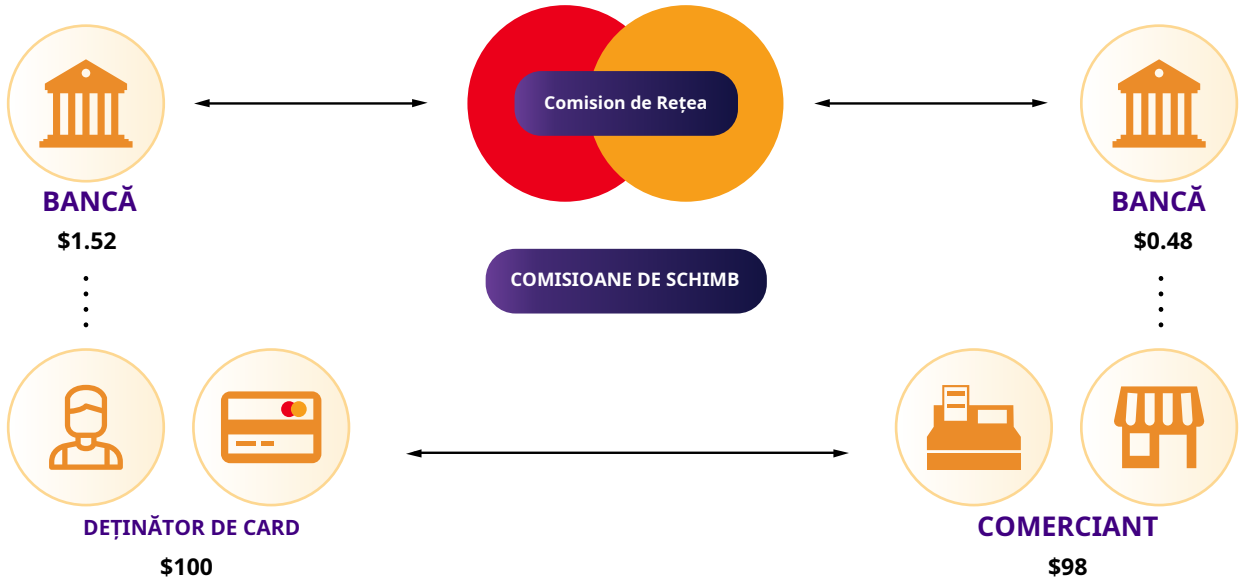
- Abuzului de centralizare
- Creșterii prețurilor
- Stagnării salariilor reale
- Slăbirii monedelor
- Nevoii de a cheltui mai mult pt. mai puține lucruri

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?

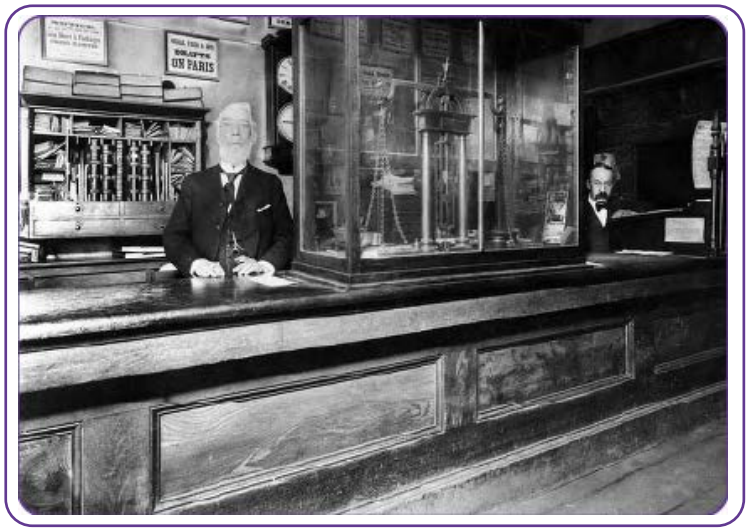
Pentru a răspunde la această întrebare, trebuie să ne concentrăm atenția asupra dolarului american, moneda de rezervă actuală a lumii, care joacă un rol dominant în lumea de azi. Fiecare țară, direct sau indirect, simte impactul deciziilor luate cu privire la dolarul american. Pentru a înțelege cu adevărat 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

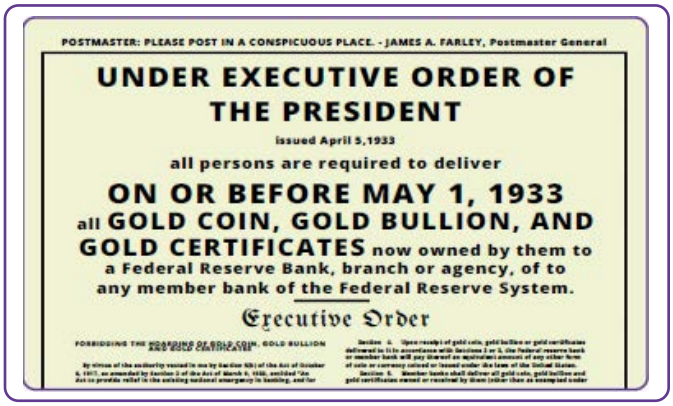
certificate de hârtie direct legate de cantitatea exactă de aur sau argint depozitată. Această legătură directă între certificatele de hârtie și banii marfă tangibili a marcat începutul a ceea ce recunoaștem astăzi ca bănci.



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.

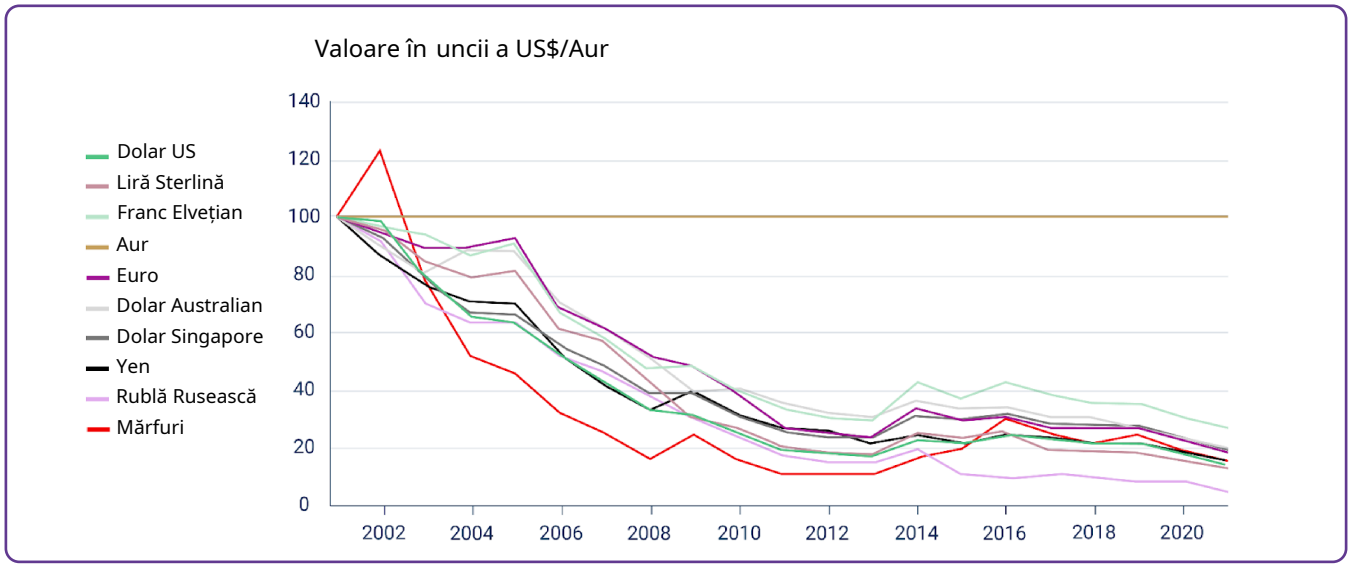
Executive Order

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.

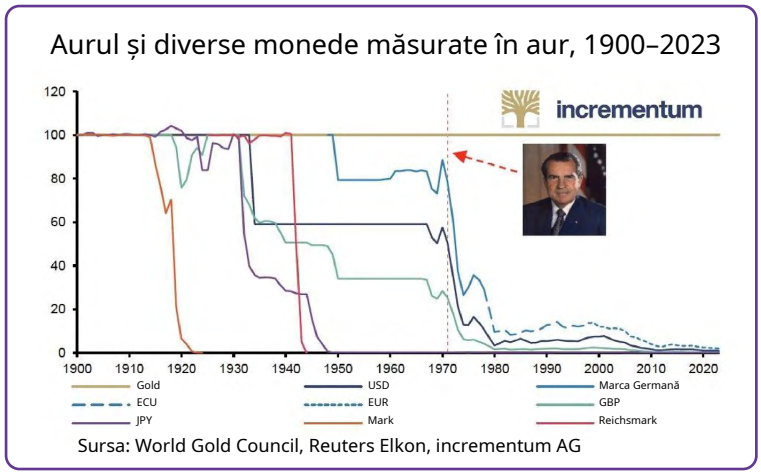
Ce sunt banii fiat și cine îi controlează?

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.

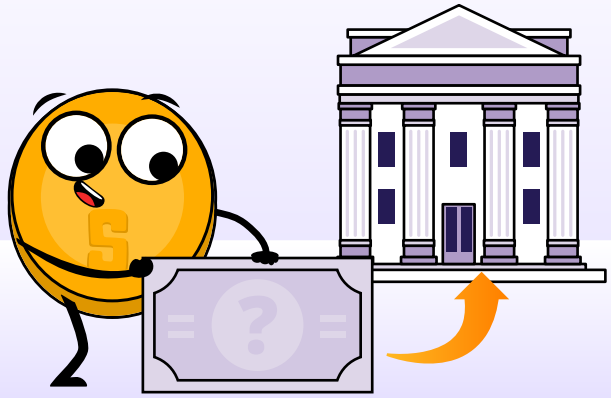
În lumea creditării cu rezervă fracționară, povestea este similară. Băncile împrumută mai mulți bani decât au de fapt, iar pentru o vreme toată lumea se bucură de beneficii. Circulă mai mulți bani și pare că există destui pentru toți. Dar, dacă prea mulți oameni încearcă să-și retragă banii în același 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)

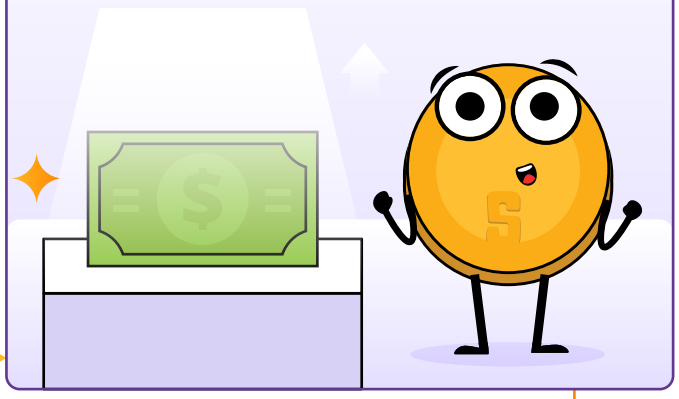


- Expansiunea masei monetare (moneda nou creată intră în sistem și mărește masa monetară)
- Supra-investiție (clienții folosesc creditele pentru a investi pe piețe, creând o creștere a cererii)
- Inflația prețurilor (prețurile cresc ca urmare a noii cereri)
- Lipsa cererii noi

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)

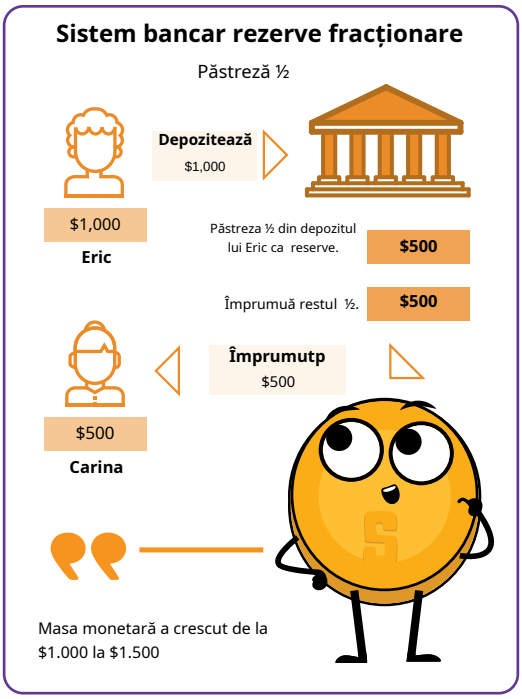
Activitate: Rezervă fracționară

Avem nevoie de următorii voluntari:

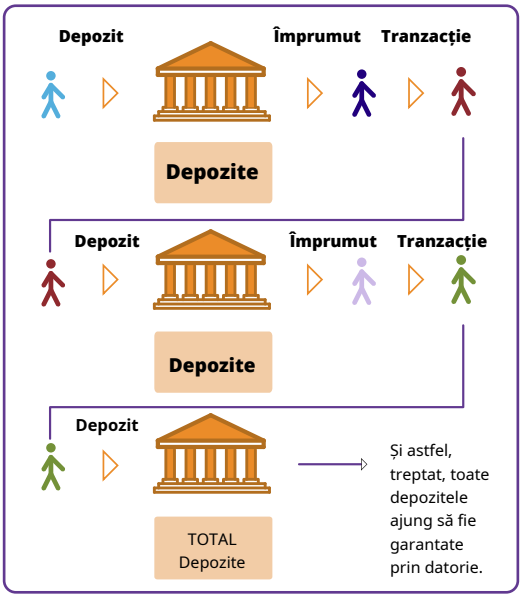
A = Depunător (Albastru deschis)
B = Casier bancar (Bancă)
C = Debitor nr. 1 (Albastru închis)
D = Proprietar de imobil/Depunător (Roșu)
E = Debitor nr. 2 (Mov deschis)
F = Proprietar galerie de artă (Verde)

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?

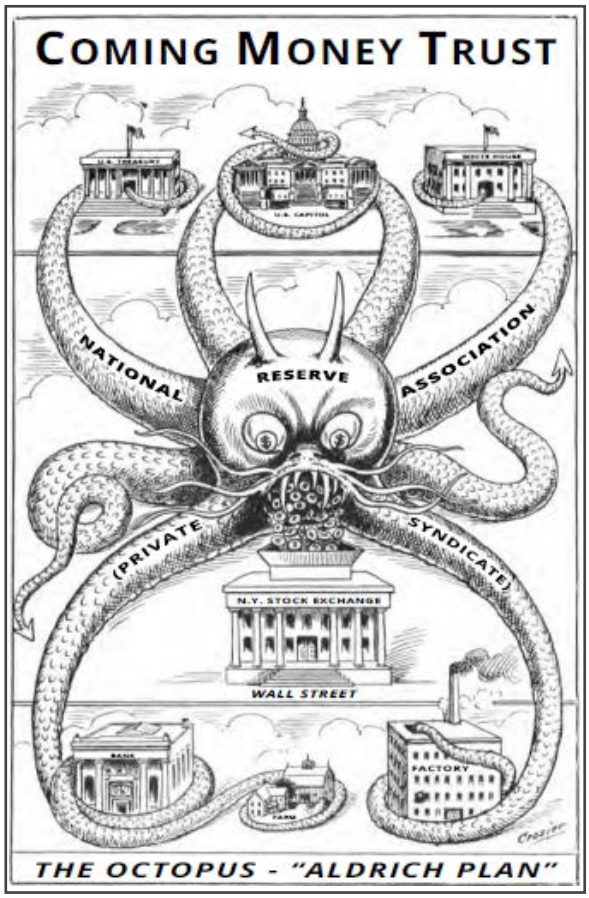
Este important de menționat că din 2020, Federal Reserve (Banca Centrală a SUA) a redus raportul de rezervă la zero procente pentru a stimula economia.

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.

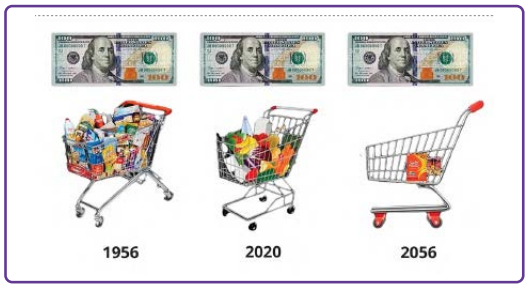
Un registru este o evidență detaliată a tuturor tranzacțiilor tale monetare. Fie că este vorba de bani câștigați sau cheltuiți, un registru te ajută să le urmărești pe toate.

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.

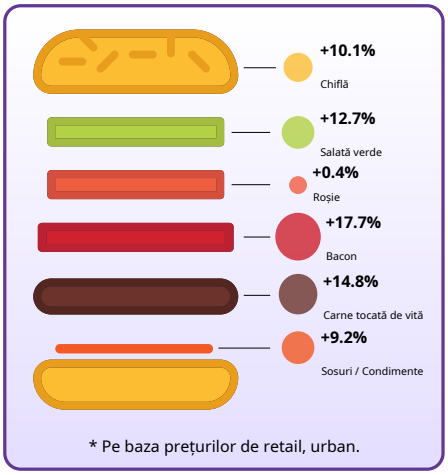
După douăsprezece luni, Ștefan ia prânzul cu bunicul său, căruia îi împărtășește detaliile bugetului său pentru 2024. Ștefan observă că bugetul său nu mai ajunge la fel de mult ca înainte și că costul vieții a crescut semnificativ în ultimul an. În timp ce Ștefan se întreabă cum este posibil acest lucru,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



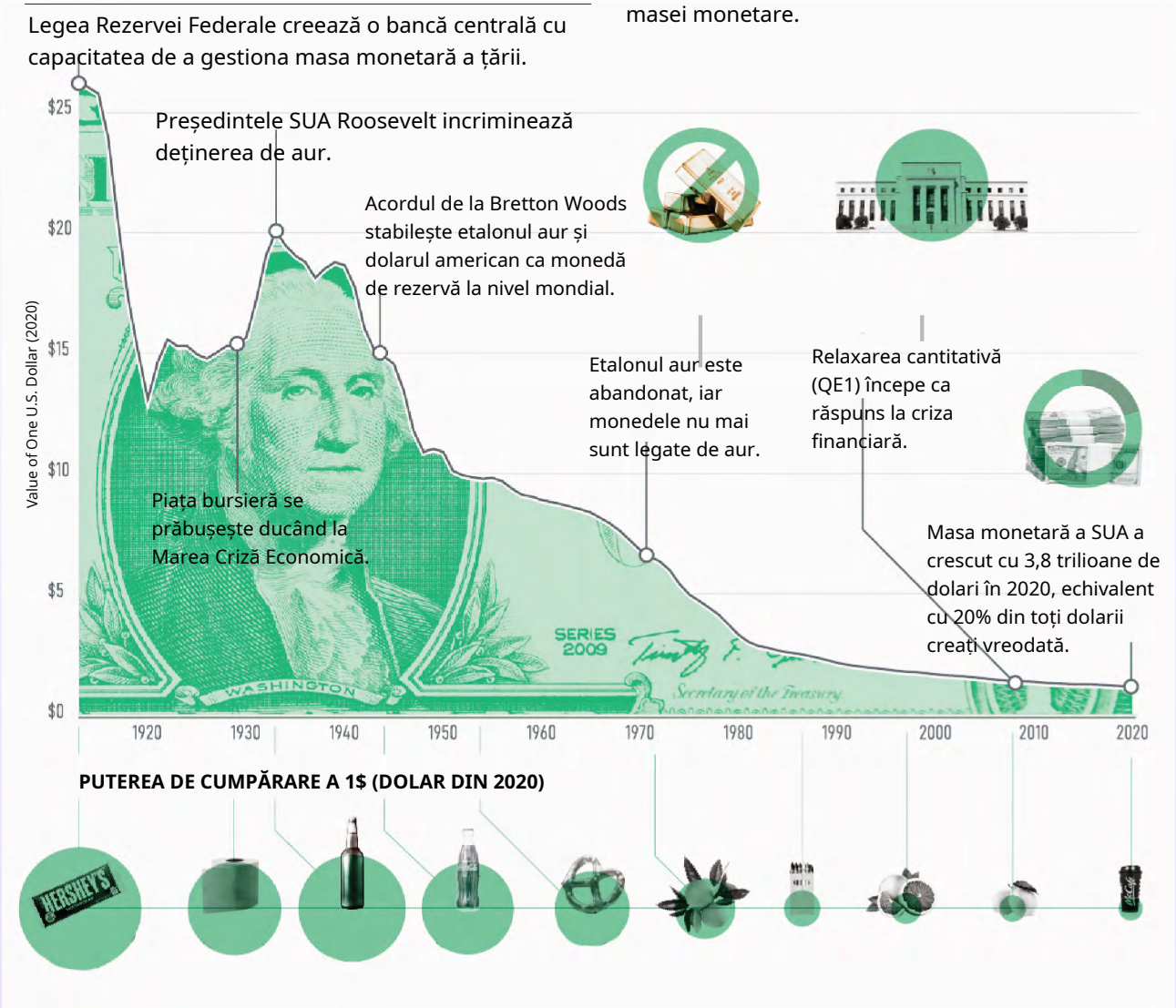
Această diferență semnificativă de preț evidențiază schimbarea puterii de cumpărare în timp și modul în care aceasta s-a modificat de-a lungul anilor din cauza inflației.

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.

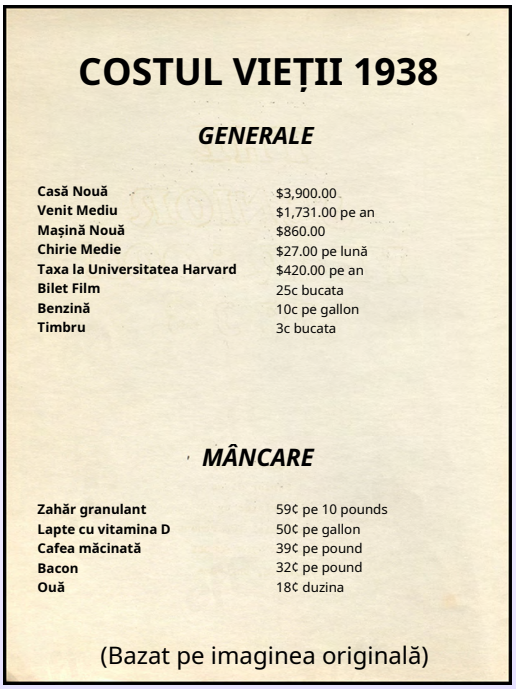
Tabelul următor arată costurile lui Ștefan în primul și al doilea an, precum și procentul de creștere a prețului.

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

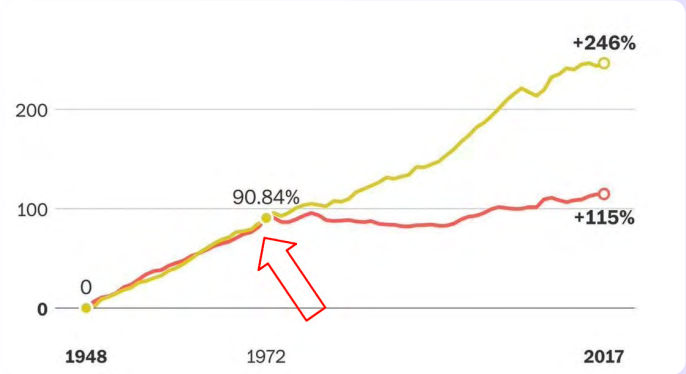
Zahăr granulant	59¢ pe 10 pounds
Lapte cu vitamina D	50¢ pe gallon
Cafea măcinată	39¢ pe pound
Bacon	32¢ pe pound
Ouă	18¢ duzina

(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



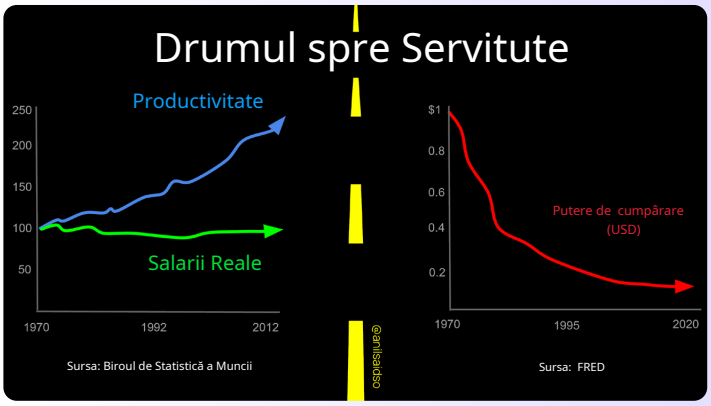
NOTĂ: Compensația include salariile și beneficiile pentru lucrătorii din producție și cei nesupervizori.

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?

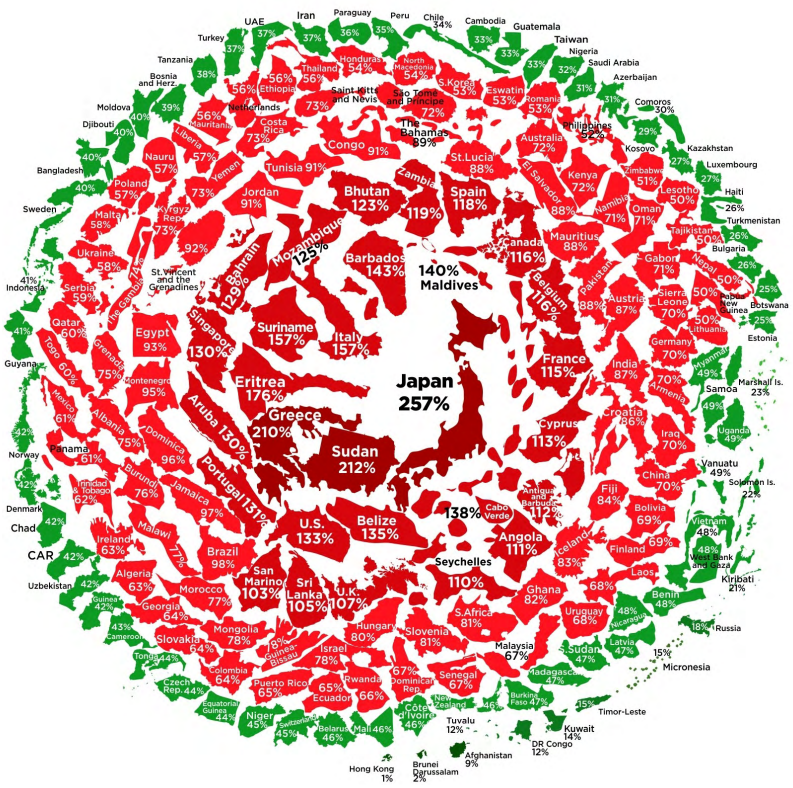
a. Exemple personale: sesiune interactivă

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 (%)

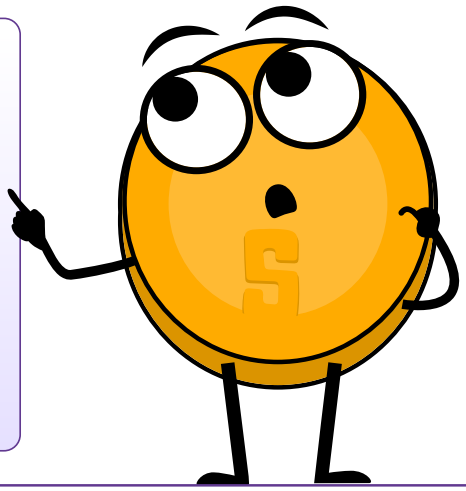
- 200% sau mai mult
- 100% — 199.9%
- 50% — 99.9%
- 20% — 49.9%
- 10% — 19.9%
- Mai puțin de 10%

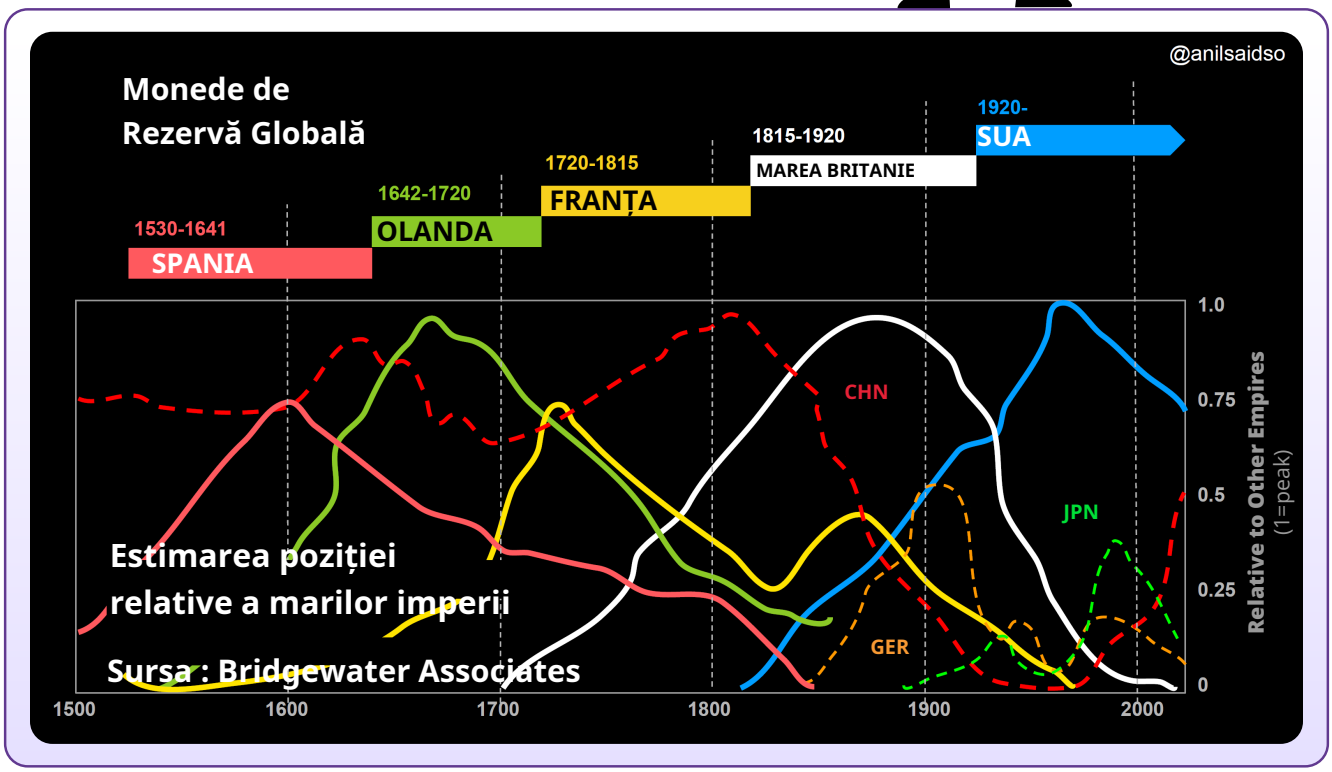
Deci, ce înseamnă acest lucru pentru indivizii și societățile care deja trebuie să facă față consecințelor sistemului fiat? Spirala datoriei în care sunt prinși este ca un bulgăre de zăpadă care se rostogolește la vale—devine tot mai mare și nu știm cum să o oprim.

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.

În ciuda numeroaselor încercări ale Cypherpunks de-a lungul deceniilor de a crea o monedă digitală liberă de controlul unui grup sau guvern, eforturile lor s-au lovit de provocări practice și nu au reușit să se materializeze complet în lumea reală. Cypherpunks au concluzionat că nu este atât de ușor să construiești o formă digitală de bani care să fie sigură, scalabilă și cu potențial de adopție largă.

Totuși, povestea se schimbă când un individ, învățând din lecțiile Cypherpunks, a ridicat conceptul de monedă digitală descentralizată la un nou nivel. În capitolele următoare, vom explora cum contribuția acestei persoane, bazându-se pe 40 de ani de muncă anterioară, a dus în cele din urmă la crearea unui sistem funcțional.

Capitolul #6

O Introducere în Bitcoin

6.0 Satoshi Nakamoto și Crearea Bitcoin

6.1 Cum funcționează Bitcoin?

6.1.1 Mecanismul de Consens Nakamoto

6.1.2 Actorii Jocului

Activitate: Consensul într-o rețea peer-to-peer

6.2 Bitcoin ca Bani Digitali sănătoși

6.2.1 Introducere

6.2.2 Caracteristicile Bitcoin

Activitate: Discuție în clasă - Este Bitcoin bani sănătoși?

6.2.3 Asumarea Responsabilității Personale

Caietul elevului

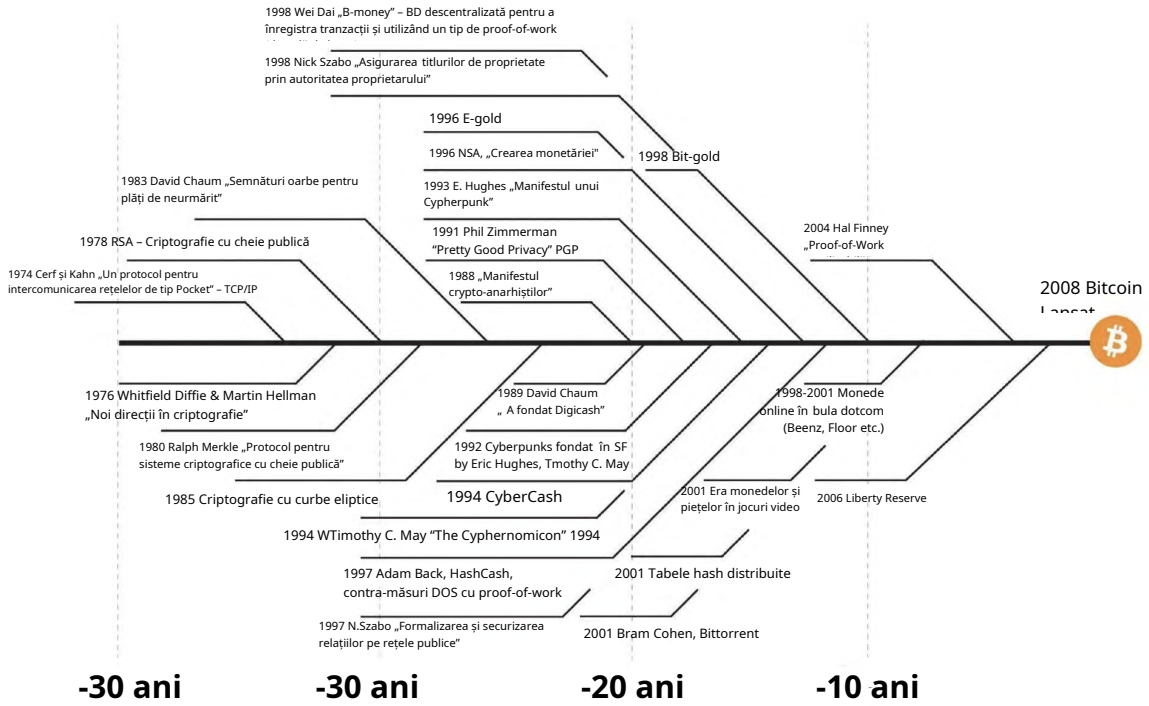
Limba Română | 2025

O Introducere în Bitcoin

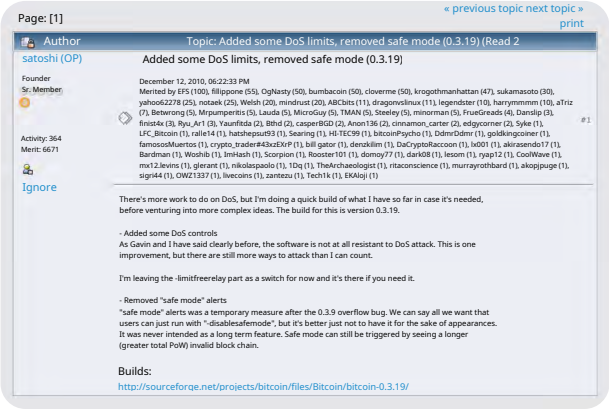
6.0 Satoshi Nakamoto și Crearea Bitcoin

> Mulți oameni resping automat moneda electronică ca fiind o cauză pierdută din cauza tuturor companiilor care au eșuat din anii 1990. Sper că este evident că doar natura controlată centralizat a acelor sisteme le-a condamnat. Cred că este prima dată când încercăm un sistem descentralizat, care nu se bazează pe încredere.
>
> **Satoshi Nakamoto**

Preistoria Bitcoin — Este rezultatul a 40 de ani de cercetare, dezvoltare și cerere.



Așa cum ai citit în capitolul precedent, mai mulți cypherpunks au încercat să creeze un sistem monetar alternativ. Acest capitol continuă povestea unuia dintre ei: o minte vizionară cu numele „Satoshi Nakamoto." Această persoană anonimă (bărbat, femeie sau grup), cu mult înainte de Bitcoin, a făcut parte din entuziaști ai criptografiei precum informaticieni și hackeri, implicându-se în discuții pentru a găsi soluții practice de înlocuire a sistemului fiat.

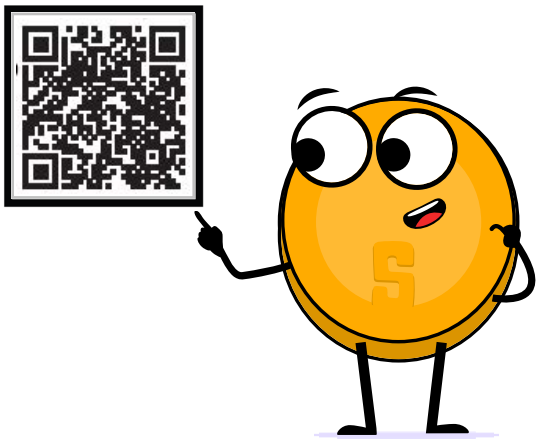


Capitolul #6

Primul Meu Bitcoin

În octombrie 2008, Nakamoto a prezentat un document revoluționar intitulat „Bitcoin: Un Sistem de Numerar Electronic Peer-to-Peer” pe o listă de discuții despre criptografie. Acest document a pus bazele unui protocol descentralizat peer-to-peer (de-la-egal-la-egal), conceput pentru a facilita tranzacții online sigure fără intermediari.

Viziunea lui Nakamoto era clară: să creeze o versiune pur peer-to-peer a banilor electronici, liberă de controlul guvernelor puternice și al instituțiilor financiare.



Pe 3 ianuarie 2009, Nakamoto a minat primul bloc Bitcoin, cunoscut sub numele de „blocul geneză”. Acesta a marcat lansarea oficială a rețelei Bitcoin, un nou sistem monetar construit pe încredere și securitate printr-un registru descentralizat. În lunile și anii ce au urmat, tot mai mulți entuziaști au început să se alăture și să contribuie la idee.

Blocul Geneză Bitcoin

Versiunea Hexa

```
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._¬....
```

În 2011, după ce rețeaua Bitcoin a dovedit că poate funcționa cu succes fără creatorul său influent, Nakamoto a trimis un email unui dezvoltator Bitcoin, anunțând că se retrage din scena Bitcoin și că lasă viitorul acesteia în „mâini bune” care îi împărtășesc viziunea.

Deși identitatea lui Nakamoto rămâne un mister până în ziua de azi, scopul său pentru crearea Bitcoin nu a fost niciodată un mister. În esență, Nakamoto a creat Bitcoin pentru a lua puterea de la câțiva și a o da celor mulți, creând o alternativă sub forma unui sistem monetar descentralizat, open-source, transparent, separând banii de stat. Crearea Bitcoin a fost răspunsul lui Nakamoto la criza financiară din 2008, care a afectat oamenii obișnuiți din întreaga lume, îmbogățind din nou clasa elitistă. Bitcoin a fost răspunsul lui Nakamoto la corupția și fragilitatea sistemului fiat. Nakamoto a pus bazele unei noi revoluții și s-a retras, fără să revendice merite.

O Introducere în Bitcoin

În anii ce au urmat, Bitcoin a început să crească rapid și a devenit un simbol al speranței, al împuternicirii și al rezilienței, provocând sistemul fiat și oferind o modalitate sigură, rezistentă la cenzură, de tranzacții financiare. Bitcoin este un protocol open-source, ceea ce înseamnă că nimeni nu are puterea să-l dețină sau să-l controleze. Designul său este public și deschis oricui dorește să participe.

Astăzi, visul lui Nakamoto pentru un sistem financiar fără granițe, transparent și sigur continuă să trăiască, alimentând revoluția globală a libertății pe care o vedem astăzi. În fiecare zi, oameni obișnuiți renunță la sistemul fiat și intră în lumea Bitcoin. Hub-uri Bitcoin—numite economii circulare Bitcoin—au fost lansate de entuziaști ai libertății în regiuni din întreaga lume. Chiar și țări întregi care caută o cale alternativă, precum El Salvador, încep să adopte Bitcoin în moduri proprii.

6.1 Cum funcționează Bitcoin?

6.1.1 Mecanismul de Consens Nakamoto

Deci, cum funcționează Bitcoin? Bitcoin are multe caracteristici, iar labirintul este foarte complex. Din fericire, dacă intri pentru prima dată în lumea Bitcoin, nu trebuie să înțelegi perfect cum funcționează pentru a începe să-l folosești.

La fel se întâmplă și cu internetul. Majoritatea oamenilor nu știu cum funcționează protocolul TCP/IP, totuși trimit emailuri, mesaje și postează conținut pe rețelele sociale zilnic. La fel și cu condusul unei mașini—majoritatea nu știu exact cum funcționează o mașină, dar știu să o conducă.

Totuși, Bitcoin nu este încă adoptat pe scară largă. Este încă o tehnologie destul de nouă, așa cum era internetul în anii '90. Din acest motiv, poate fi util să înțelegi elementele de bază ale Bitcoin într-un mod simplu, mai puțin tehnic.

Capitolul #6

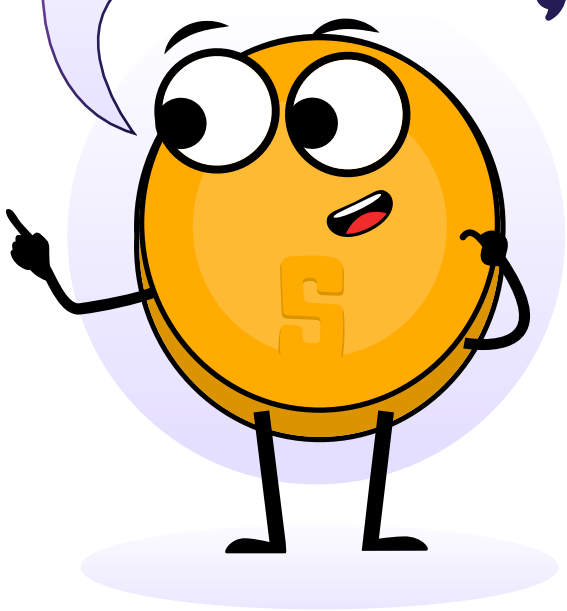
Primul Meu Bitcoin

Ideea cheie din spatele modului în care funcționează Bitcoin poate fi condensată într-o singură propoziție: Bitcoin este un acord între oameni online. Poți să te gândești la asta ca la un joc de societate cu prietenii. La un joc precum Monopoly, ești de acord cu ceilalți jucători asupra unor reguli specifice. Una dintre regulile Monopoly este că doar „bancnotele Monopoly" speciale sunt acceptate. Dacă James (unul dintre jucători) încalcă regulile folosind hârtie igienică pentru a cumpăra o casă în loc de bancnote Monopoly, ceilalți jucători îi vor spune lui James că trișează și pur și simplu vor înceta să joace cu el. Pe scurt, pentru a juca, ai ajuns la un consens asupra unui set de reguli cu ceilalți și nu te abați de la ele, altfel vei fi respins.

Așa funcționează, în esență, Bitcoin. Bitcoin este o rețea de oameni care sunt de acord cu același set de reguli. Aceste reguli sunt legate matematic, scrise în cod informatic și acceptate direct de toți cei care rulează software-ul Bitcoin. Regulile Bitcoin se aplică tuturor participanților în mod egal, ceea ce înseamnă că toți trebuie să respecte regulile jocului sau nu pot participa, deoarece rețeaua îi va respinge.

De exemplu, una dintre regulile Bitcoin este: „Nu vor exista niciodată mai mult de 21 de milioane de bitcoin." Dacă cineva ar vrea să creeze un milion de bitcoin suplimentari pentru sine, nu i-ar folosi la nimic, deoarece ar fi identificat și respins automat de toți ceilalți. Acesta este motivul pentru care Bitcoin este atât de robust.

> Știai că, din 2009, Bitcoin a rezistat la zeci de mii de încercări de hacking, manipulare sau modificare? Bitcoin a demonstrat că nimeni nu îl poate opri, controla sau manipula.



Nu contează cine ești sau de unde vii; dacă intri în lumea Bitcoin, trebuie să joci după același set de reguli ca oricine altcineva.

Acest lucru se aplică și tuturor persoanelor și entităților cu multă putere și influență în lumea fiat. În lumea Bitcoin, nu există loc pentru trișare sau sabotaj— toți sunt tratați egal și nimeni nu poate schimba asta.

6.1.2 Actorii jocului

Pentru a înțelege mai bine descentralizarea Bitcoin, trebuie să analizăm mai profund diferitele roluri din cadrul rețelei. În lumea Bitcoin, diverși participanți joacă roluri distincte, dar armonioase, contribuind la funcționarea fără probleme a rețelei.

1. Minerii: Arhitecții securității

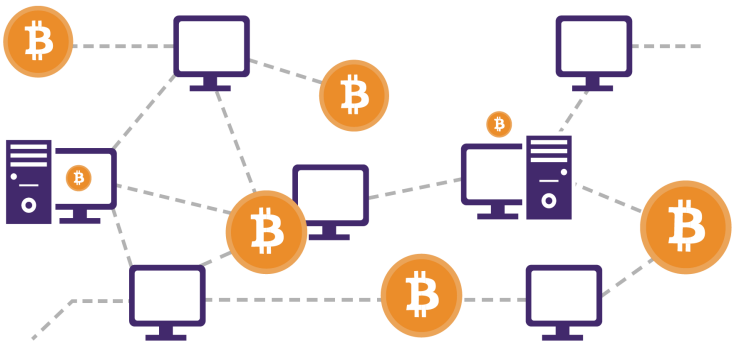
Minerii sunt coloana vertebrală a Bitcoin. Aceștia sunt persoane sau grupuri care lucrează în spatele scenei pentru a menține și securiza rețeaua printr-un mecanism numit Proof-of-Work (PoW). Acești jucători sunt dotați cu computere speciale cu putere de calcul ridicată. Ei pun hardware-ul la dispoziția rețelei Bitcoin, concurând între ei pentru a găsi numere criptografice complexe, a verifica tranzacțiile și a adăuga noi blocuri de informații despre tranzacții în registrul descentralizat al Bitcoin (așa-numitul blockchain). Angajamentul lor asigură imuabilitatea registrului și protejează împotriva atacurilor malițioase.

Natura descentralizată a mineritului permite oricui are resurse de calcul suficiente să participe. Datorită muncii lor, minerii care rezolvă cel mai rapid puzzle-ul sunt recompensați cu bitcoin.

Minerii Bitcoin sunt distribuiți în întreaga lume, protejând rețeaua împotriva centralizării și asigurând că securitatea Bitcoin rămâne robustă și distribuită.

2. Noduri: Gardienii validării

Nodurile Bitcoin sunt oameni obișnuiți care trăiesc pe tot globul. Acești participanți sunt gardienii rețelei Bitcoin, rulând software-ul Bitcoin pe calculatoarele lor mici, unde mențin o copie a întregului registru. Nodurile validează tranzacțiile și se asigură că toți participanții respectă regulile de consens.



Prin distribuirea responsabilității validării pe o rețea de noduri, Bitcoin rămâne rezistent la atacuri și își menține natura trustless. Nodurile joacă un rol crucial în menținerea integrității registrului, contribuind la ethosul descentralizării Bitcoin.

3. Utilizatori: Participanți împuterniciți

Utilizatorii—sufletul rețelei Bitcoin—sunt indivizi care efectuează tranzacții. Poți să te gândești la utilizatori ca la oameni obișnuiți care își trăiesc viața, dar care și-au luat puterea în propriile mâini integrând Bitcoin. De exemplu, unii utilizatori își economisesc banii în bitcoin, iar alții, precum cetățenii din El Salvador, îl folosesc ca monedă pentru a cumpăra alimente și a primi salariul în bitcoin.

Bitcoin îi împuternicește pe utilizatori prin eliminarea intermediarilor, permițând tranzacții directe peer-to-peer. Aceasta înseamnă că utilizatorii au control total asupra banilor lor, oferind control asupra fondurilor și tranzacțiilor.

4. Dezvoltatori și proiecte: Arhitecții inovației

Sistemul monetar al viitorului nu se construiește singur, nici nu este adoptat global într-un mod etic fără efort. Aici intervin dezvoltatorii și proiectele Bitcoin.

Dezvoltatorii folosesc expertiza lor tehnică pentru a îmbunătăți și inova protocolul Bitcoin. Acești indivizi contribuie cu cod, propun îmbunătățiri și rezolvă vulnerabilități, asigurând evoluția rețelei în fața tuturor tipurilor de provocări. Natura open-source a Bitcoin invită la colaborare, permițând dezvoltatorilor din întreaga lume să contribuie la creșterea sa.

Frumusețea acestei dezvoltări descentralizate previne monopolizarea controlului asupra protocolului de către o singură entitate. Acest lucru se întâmplă printr-un proces bazat pe consens. Dezvoltatorii propun idei și schimbări, iar doar cele mai bune idei, aliniate cu viziunea generală pentru o lume mai bună, primesc sprijinul comunității, favorizând o evoluție transparentă și democratică a Bitcoin până când va fi pregătit pentru 8 miliarde de oameni.

Proiectele Bitcoin implică grupuri diverse, de la organizații non-profit cu misiune clară și corporații, la grupuri și indivizi care creează conținut valoros. Acești oameni lucrează împreună pentru un scop specific sau o direcție în cadrul marii misiuni Bitcoin către libertatea colectivă.

Proiectele Bitcoin joacă un rol crucial în modelarea și promovarea adopției Bitcoin, lucrând pentru un viitor care prioritizează împuternicirea și libertatea rasei umane.

Simfonia

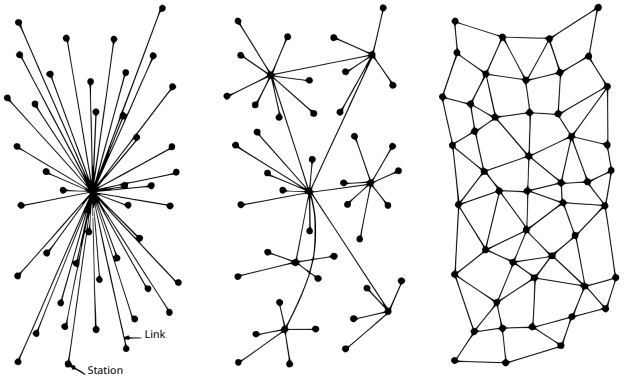
Descentralizarea Bitcoin poate fi gândită ca o orchestră muzicală, un act de echilibru în care toți muzicienii creează împreună cea mai frumoasă muzică. Nu există un șef în rețeaua Bitcoin; în schimb, minerii, nodurile, utilizatorii, dezvoltatorii și proiectele își îndeplinesc rolurile cu autonomie și colaborare.

Registrul descentralizat, menținut de noduri, garantează transparența, în timp ce mecanismul proof-of-work oferă securitate și descurajează centralizarea mineritului. Utilizatorii experimentează suveranitate financiară și împuternicire, liberi de controlul sistemului fiat. Dezvoltatorii, ghidați de consens, asigură adaptarea protocolului la nevoile în evoluție ale umanității. Proiectele Bitcoin, în moduri unice, contribuie la misiunea mai largă a libertății colective.

O Introducere în Bitcoin

Așa cum se poate vedea, fiecare participant joacă un rol vital în modelarea adopției Bitcoin și împuternicirea umanității. Fiecare participant din această orchestră descentralizată contribuie la reziliența și longevitatea Bitcoin, creând un ecosistem in care încrederea nu este necesară (trustless) și fără granițe.

Pe scurt, simfonia descentralizării în Bitcoin răsună ca un testament al viziunii lui Satoshi Nakamoto și al pasiunii imense a unei comunități globale care caută libertate și împuternicire.



CENTRALIZAT (A) | DESCENTRALIZAT (B) | DISTRIBUTED (C)

Exercițiu în clasă — Construirea consensului într-o rețea peer-to-peer

Obiective

Să înțelegem cum se ajunge la consens într-un grup și pentru a afla despre criptografie și stratul de consens al Bitcoin.

Materiale

Mesaj cu instrucțiuni criptate și necriptate pentru acțiuni („atacă” sau „nu ataca”).

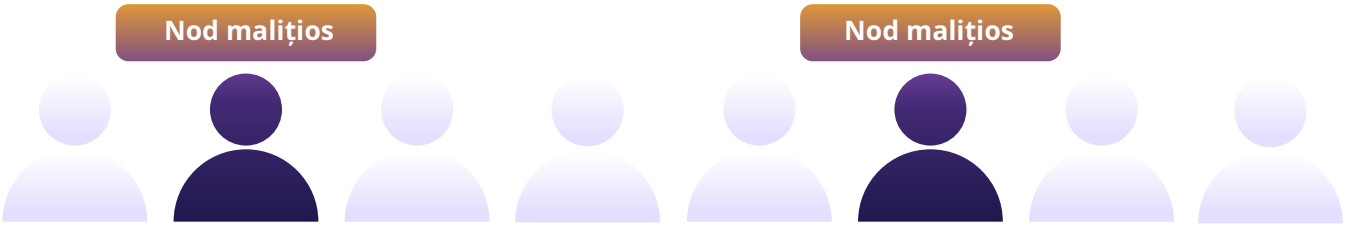
Pregătirea pentru activitate

Profesorul va selecta un grup de trei sau patru elevi înainte de oră pentru a fi noduri malițioase în activitatea următoare. Profesorul va atribui acestor noduri malițioase un puzzle criptografic ca temă pentru acasă în ora precedentă.

Pașii exercițiului:

1. Profesorul va selecta un „inițiator” care va primi un mesaj pe o bucată de hârtie ce spune „ATACĂ” și o serie de numere: „4-16-14-21-1-21-21-1-3-11-” către un student din grup.

2. Elevii vor forma un cerc în spațiul desemnat, asigurându-se că studenții selectați ca noduri malițioase sunt separați pentru a crește eficiența lecției.



3. După ce grupul a format cercul, inițiatorul va transmite nota persoanei din dreapta cercului.

4. După ce toți au citit mesajul, inițiatorul va da semnalul grupului spunând „acum”, iar grupul va reacționa simultan la mesaj. Dacă mesajul spune „ATACĂ”, toți participanții vor face un pas înainte.

5. După reacția inițială, unii studenți (cei care au primit mesajul criptat și l-au interpretat corect) vor rămâne pe loc, iar restul vor urma instrucțiunea originală, dezvăluind lipsa de consens.

Concluzie:

Discută de ce nu s-a ajuns la consens, introducând conceptul de Problema Generalilor Bizantini, cum se leagă de nevoia unui scop comun și discutând ulterior cum Bitcoin oferă o soluție la această problemă.

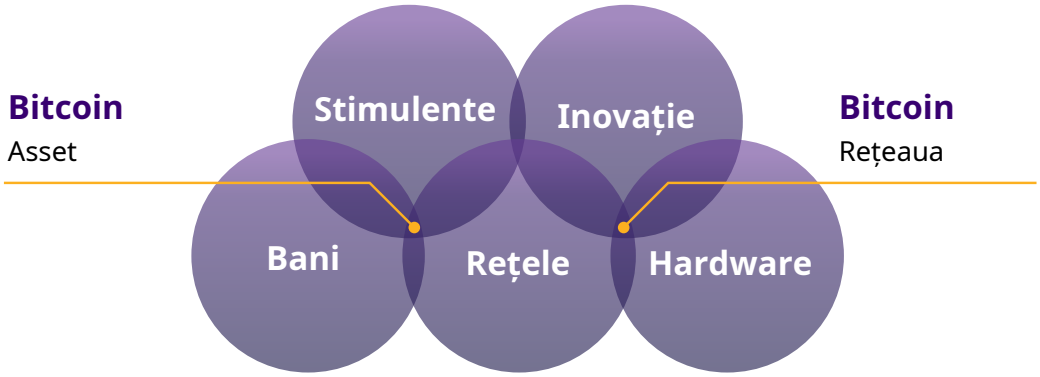
6.2 Bitcoin ca monedă digitală sănătoasă

6.2.1 Introduction

Introducere

Urmărește un videoclip de 1,5 minute, „Ce este Bitcoin?”

Pe scurt, Bitcoin este bani. Bitcoin nu este o investiție, ci mai degrabă o modalitate sigură și puternică de a economisi banii câștigați cu greu. Deținerea de bitcoin nu te va îmbogăți, deoarece nu îți va aduce un randament sub formă de mai mulți bitcoin. Valoarea sa, măsurată în raport cu o monedă fiat, crește, dar acest lucru se datorează doar adopției tot mai mari și devalorizării monedelor fiat.



Bitcoin este o nouă formă de bani; este „Internetul Banilor”, ceea ce înseamnă că oricine poate să se alăture și să înceapă să facă schimb de valoare cu alți utilizatori. Chiar și cele mai izolate și sărace comunități din lume au în sfârșit acces la un sistem monetar. La fel cum oricine are un telefon și o conexiune la internet poate folosi un motor de căutare, Bitcoin face posibil ca oricine are un telefon și internet să acceseze un nou sistem monetar global.

Plăți mai rapide și mai ieftine

Trimite bani în întreaga lume în câteva minute, cu taxe foarte mici.

Incluziune financiară

2,5 miliarde de persoane fără cont bancar pot accesa bani prin telefon sau calculator.

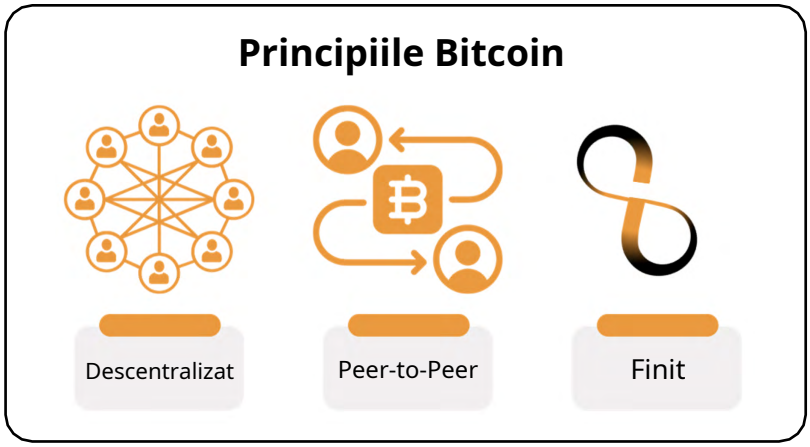
Confidențialitate

Tranzacțiile Bitcoin sunt publice, dar identitatea ta nu este.

Bitcoin este complet digital și fără granițe. Nu contează unde te afli, deoarece există pe computere și smartphone-uri din întreaga lume. Mulți utilizatori din întreaga lume rulează software-ul Bitcoin și o copie a registrului său.

Acest software și evidența tuturor tranzacțiilor au șanse foarte mici să dispară, deoarece există nenumărate copii. Pentru a-l opri, ar trebui să oprești întregul internet, pentru totdeauna, ceea ce este extrem de puțin probabil să se întâmple.

În cele din urmă, Bitcoin este rar, ceea ce înseamnă că numărul de unități bitcoin care pot exista este absolut limitat. Nimeni nu poate falsifica Bitcoin—nici măcar cele mai puternice guverne și instituții financiare.



6.2.2 Caracteristicile Bitcoin

Evoluția banilor sănătoși

Așa cum ai învățat în Capitolul 2, ciclul de viață al banilor sănătoși trece prin trei etape pentru a fi acceptat general de societate: de la a fi un depozit de valoare, la a deveni mijloc de schimb și, în final, unitate de cont.

Prima etapă a banilor, depozitul de valoare, este atunci când o monedă începe să câștige încredere ca activ stabil (sau în apreciere) în timp. Cei care recunosc acest lucru devreme caută să-și protejeze averea stocând-o sub această formă, mai ales în perioade de incertitudini geopolitice și macroeconomice.

Unele grupuri, precum instituțiile media, numesc Bitcoin „aur digital”. Acest lucru se datorează faptului că Bitcoin s-a impus ferm ca depozit de valoare în ultimul deceniu. În fiecare zi, tot mai mulți oameni văd Bitcoin ca o protecție împotriva inflației, așa cum a fost istoric aurul.

Următoarea etapă este atunci când încrederea în stabilitatea unei monede se consolidează. Atunci moneda devine mijloc de schimb, facilitând tranzacțiile din viața de zi cu zi. În această etapă, moneda începe să fie acceptată pe scară largă pentru schimbul de bunuri și servicii.

Bitcoin avansează progresiv spre a deveni mijloc de schimb. Odată cu acceptarea tot mai mare de către comercianți și dezvoltarea protocolului, tranzacțiile cu Bitcoin devin mai eficiente și mai frecvente în comerțul zilnic. Un exemplu este El Salvador, unde Bitcoin este recunoscut oficial ca mijloc legal de plată. În fiecare zi, tot mai mulți cetățeni și afaceri obișnuite folosesc Bitcoin ca mijloc de schimb.

În etapa finală, o monedă atinge statutul de unitate de cont, servind ca măsură comună pentru stabilirea prețurilor bunurilor și serviciilor. Aceasta este etapa în care devine standardul după care sunt măsurate toate celelalte valori.

Drumul spre a deveni unitate de cont este un proces mai lung (pe termen lung). Lumea măsoară în prezent bunurile și serviciile doar în monede fiat, iar din acest motiv, Bitcoin are nevoie de o adopție mai largă și integrare în diverse sisteme financiare. Totuși, fundația este deja pusă, deoarece afacerile și indivizii încep să ia în considerare și să denomineze valori în Bitcoin.

După cum poți vedea, Bitcoin este pe drumul cel bun în această evoluție a banilor sănătoși. Când Bitcoin va fi complet integrat în sistemul financiar global, ar putea deveni o unitate de cont standard, remodelând întregul sistem monetar global.

Proprietăți ale banilor

Așa cum ai învățat în Capitolul 2, de-a lungul timpului, omenirea a descoperit că banii sănătoși trebuie să aibă anumite proprietăți pentru a fi eficienți. Aceste proprietăți sunt durabilitatea, divizibilitatea, portabilitatea, acceptabilitatea, raritatea și fungibilitatea.

Să vedem dacă Bitcoin trece testul.

Durabilitate: Bitcoin este pur digital și, prin urmare, complet durabil.

Divizibilitate:

Spre comparație, moneda fiat USD poate fi divizată până la cent (.01). Bitcoin poate fi divizat în ceea ce se numește un satoshi sau sat (.00000001). Și datorită caracterului digital al Bitcoin, poate fi chiar mai divizat în viitor dacă omenirea va avea nevoie. Bitcoin este în prezent cel mai divizibil activ monetar din lume.

Portabilitate:

În aprilie 2020, 1,1 miliarde de dolari au fost transferați în doar câteva minute, iar costul a fost de doar 68 de cenți. Nicio altă metodă de plată nu poate muta atât de mulți bani la un cost atât de mic, atât de rapid și independent. Acesta este motivul pentru care Bitcoin este cea mai ușor de mutat formă de bani din lume.

Acceptabilitate:

Bitcoin este încă în stadiile incipiente de a deveni un mijloc de schimb, iar comparativ cu monedele fiat, acceptabilitatea este momentan scăzută.

Raritate:

Vor exista doar 21 de milioane de bitcoin. Prin cod, este imposibil ca această sumă să crească vreodată, ceea ce înseamnă că Bitcoin nu este doar rar, ci este cel mai rar activ monetar din lume.

Fungibilitate:

Fiecare unitate de bitcoin este identică cu oricare altă unitate și poate fi interschimbată și tranzacționată pe protocolul Bitcoin pe bază de tip similar, ceea ce îl face o monedă fungibilă.

Bitcoin vs. AUR vs. Dolar

Proprietăți ale banilor	Aur	Fiat	Bitcoin
Durabilitate	Moderată	Moderată	Ridicată
Portabilitate	Moderată	Ridicată	Ridicată
Divizibilitate	Moderată	Moderată	Ridicată
Fungibilitate	Ridicată	Ridicată	Ridicată
Raritate	Moderată	Scăzută	Ridicată
Verificabil	Moderată	Moderată	Ridicată
Istorie stabilită	Ridicată	Moderată	Scăzută
Rezistent la cenzură	Moderată	Moderată	Ridicată
Inteligent/Programabil	Scăzută	Moderată	Ridicată

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

Bitcoin este un tip de bani inteligenți, programabili, care nu pot fi confiscați și are toate calitățile care îl fac excelent pentru economisire și ușor de folosit pentru comercianții care doresc tranzacții rapide.

Deoarece este un registru digital transparent, Bitcoin poate fi extrem de eficient în detectarea fraudei și evaluarea riscurilor în serviciile sale. Are avantajele aurului, cum ar fi faptul că există o cantitate limitată, dar are și beneficiile monedelor fiat, deoarece poate fi divizat și transportat ușor. În plus, aduce funcții noi care se potrivesc bine în lumea noastră digitală.

Ce părere ai? Bitcoin nu este încă larg recunoscut și adoptat, dar este oare monedă sănătoasă?

Activitate: Discuție în clasă - Este Bitcoin monedă sănătoasă?

Acum că am discutat despre Bitcoin în detaliu, să ne uităm din nou la tabelul de comparație a banilor.

	Vaci	Țigări	Diamante	Euro	Bitcoin
Portabil					
Portabil					
Uniform					
Acceptabil					
Rar					
Divizibil					
Total					

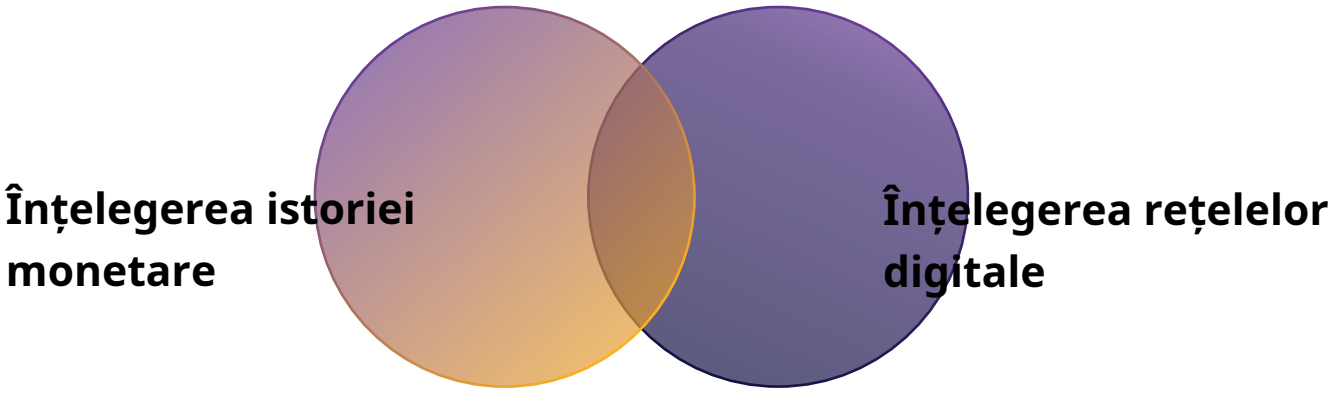
6.2.3 Asumarea Responsabilității Personale

> Rezultatul este un sistem distribuit fără un punct unic de eșec. Utilizatorii dețin cheile criptografice ale propriilor bani și tranzacționează direct între ei, cu ajutorul rețelei P2P pentru a verifica dubla cheltuire.
>
> **Andreas M. Antonopoulos**

O Introducere în Bitcoin

În lumea fiat, oamenii se bazează pe guverne, bănci și furnizori de plăți consacrați. Conducătorii acestor instituții (financiare) stabilesc regulile rețelei, iar participanții, în mare parte cetățeni obișnuiți, trebuie să se conformeze acestor reguli. Nu contează unde locuiești—există întotdeauna un set de proceduri standard care îți indică ce să faci și cum să faci. În timp, acest lucru a dus la un ciclu de dificultăți, în special pentru familiile care se confruntă cu provocările tot mai mari ale vieții de zi cu zi.

Din cauza acestui sistem, oamenii sunt obișnuiți să lase responsabilitatea pentru finanțele lor în mâinile altora. De exemplu, majoritatea oamenilor se bazează pe altcineva să îi ajute, mai ales când ceva nu merge bine (cum ar fi pierderea accesului la contul bancar).



„Bitcoin a câștigat deja”

După cum știi, sistemul monetar Bitcoin este foarte diferit. Bitcoin funcționează într-un mod specific, iar conducătorii au fost înlocuiți de un sistem autonom de reguli. Nu există dictator sau lider, ceea ce înseamnă că nimeni nu îți va dicta ce trebuie să faci. Dacă vrei libertatea și puterea nou dobândite oferite de Bitcoin, va trebui să înveți cum funcționează și să integrezi tehnologia într-un mod care să funcționeze personal pentru tine.

	Unitate	Finalizare	Emitere
$	Cent 0.01		
฿	Sat 0.00000001		

Cu Bitcoin, ai control total asupra fondurilor tale, dar acest control suplimentar vine cu o responsabilitate crescută. De exemplu, pierderea accesului la bitcoinul tău prin pierderea cheilor portofelului digital înseamnă că ți-ai pierdut economiile—permanent. Nu există un serviciu de asistență clienți la care să suni sau altcineva la care să apelezi când apare o problemă; trebuie să te ocupi singur de ea.

Din fericire, acest lucru nu se va întâmpla celor care decid să își asume pe deplin responsabilitatea pentru propria viață. Să folosești Bitcoin nu este complicat în mod inerent; este doar un concept nou. Orice disconfort apare pentru că este ceva necunoscut, dar dacă ești dispus să înveți cum să folosești Bitcoin și să îți asumi pe deplin responsabilitatea de a-ți proteja averea, Bitcoin devine un instrument care îți oferă putere—tu ești în control, iar nimeni nu îți poate confisca averea.

În concluzie, cheia constă în acțiune, înțelegerea modului de funcționare a Bitcoin și implementarea acestuia conform nevoilor și filosofiei tale de viață. În continuare, vom începe să folosim bitcoin prin configurarea unui portofel Bitcoin, trimiterea și primirea primelor tranzacții și revizuirea celor mai bune practici de securitate.

Capitolul #7

Cum folosim Bitcoin

7.0 Introducere

7.1 Achiziționarea și schimbul de Bitcoin

7.1.1 P2P: În persoana

7.1.2 P2P: Online

7.1.3 Exchange-uri Centralizate

7.2 Introducere în portofelele Bitcoin

7.2.1 Portofele auto-custodial vs custodial

7.2.2 Tipuri diferite de portofele Bitcoin

7.3.3 Open Source vs Closed Source

Activitate: Evaluarea portofelelor Bitcoin în clasă

7.3 Configurarea unui portofel Bitcoin pe mobil

Activitate: Configurarea unui portofel Bitcoin

7.4 Primirea și trimiterea tranzacțiilor

Activitate Tranzacții Bitcoin în acțiune

7.5 Economisirea în Bitcoin

7.6 Nu te încrede, verifică

Caietul elevului

Limba Română | 2025

Cum folosim Bitcoin

7.0 Introducere

> De ce ar avea cineva încredere în banii programatorilor și nu în banii băncii centrale? Programatorii ți-au adus internetul. Băncile ți-au adus marea depresie.
>
> **Andreas M. Antonopoulos**

Acum că avem o înțelegere mai bună despre ce este Bitcoin și scopul său, este timpul să învățăm cum să-l folosim practic. În acest capitol, te vom ghida pas cu pas prin procesul de achiziționare de bitcoins, vom explora diferitele tipuri de portofele disponibile, te vom ajuta să-ți configurezi propriul portofel Bitcoin și chiar vom exersa trimiterea și urmărirea unei tranzacții bitcoin pe rețea. E timpul să transformi înțelegerea în acțiune!

7.1 Achiziționarea și schimbul de Bitcoin

Există multe modalități de a achiziționa bitcoin. De exemplu, poți:

- Să fii plătit în bitcoin pentru munca ta și să plătești produsele și serviciile altor persoane cu bitcoin (mai multe despre asta în Capitolul 8)
- Să minezi bitcoin (mai multe despre asta în Capitolul 9)
- Să schimbi moneda fiat pentru bitcoin sau să schimbi bitcoin pentru moneda fiat, în persoană.
- Să schimbi moneda fiat pentru bitcoin sau să schimbi bitcoin pentru moneda fiat, online.

Mai jos, vom explora schimbul de monedă fiat în bitcoin și invers, atât prin tranzacții față în față, cât și prin metode online, deoarece acestea sunt cele mai des întâlnite opțiuni.

7.1.1 Peer-to-Peer: Față în Față

Implicarea în tranzacții peer-to-peer (P2P) pentru achiziționarea și vânzarea de bitcoin presupune schimbul direct al monedei fiat (sau a altor bunuri sau servicii) cu bitcoin cu o altă persoană, eliminând necesitatea implicării unei bănci sau a altei părți în tranzacție.

Ambele părți stabilesc de comun acord suma și rata de schimb. Cumpărătorul oferă numerarul, vânzătorul transferă bitcoin, iar tranzacția se încheie. Deși este mai ușor să faci schimburi P2P fizic, întâlnindu-te direct cu cealaltă persoană în lumea reală, poți face acest lucru și practic de oriunde, datorită internetului. În plus, schimbul de bitcoin în monedă fiat urmează un proces similar, dar invers.

7.1.2 Peer-to-Peer: Online

Intră pe platformele P2P, unde cumpărătorii și vânzătorii de Bitcoin se întâlnesc în spațiul cibernetic pentru a efectua tranzacții fără intermediari, direct pe internet.
Cu astfel de platforme, nu trebuie să ai încredere în nimeni cu informațiile sau banii tăi; poți întâlni alți parteneri și poți tranzacționa direct cu ei.

Pe majoritatea platformelor P2P, partenerii trebuie să depună o parte din fonduri în escrow (cont de garanție) pentru a se asigura că vor respecta partea lor din înțelegere. Escrow înseamnă să pui banii într-un loc sigur controlat de platformă până când ambele părți își îndeplinesc promisiunea. Este ca și cum un prieten de încredere îți păstrează lucrurile până când toată lumea își respectă cuvântul.

7.1.3 Exchange-uri Centralizate

Utilizarea exchange-urilor centralizate poate fi cea mai ușoară modalitate de a cumpăra și vinde bitcoin, dar implică și compromisuri semnificative. Exchange-urile centralizate sunt companii care permit clienților să cumpere și să vândă bitcoin direct prin intermediul lor. Totuși, această comoditate vine cu un cost.

CENTRALIZAT

Exchange-urile centralizate și compromisurile lor

Este important de menționat că atunci când cumperi bitcoin printr-un exchange centralizat, de obicei ți se cere să furnizezi informații personale și să-ți verifici identitatea. Acest lucru creează un risc de furt de identitate și expune informațiile tale personale unor amenințări. În plus, exchange-urile centralizate dețin bitcoinul pentru tine, ceea ce înseamnă că nu ai control asupra banilor tăi până când îi retragi.

Pe lângă aceste preocupări, exchange-urile centralizate pot folosi în mod necorespunzător fondurile utilizatorilor sau pot împrumuta mai mult bitcoin decât au în rezervă până când se prăbușesc. Da, exact ca băncile! Totuși, în lumea Bitcoin nu există o bancă centrală care să salveze băncile frauduloase prin tipărirea de monedă, deoarece nu poți tipări mai mult bitcoin!

7.2 O Introducere în Portofelele Bitcoin

Spre deosebire de banii fizici, monedele bitcoin nu sunt prezente efectiv într-un portofel Bitcoin. În schimb, ele există pe registrul distribuit pe care rețeaua Bitcoin îl verifică și îl securizează constant. Deci, cum poți deține bitcoin?
Deții bitcoin doar atunci când deții cheile private care îți permit să semnezi tranzacții și să transferi proprietatea bitcoinului tău către altcineva. Acesta este actul de a trimite bitcoin.

Având acest lucru în vedere, să analizăm două concepte pe care le descriem atunci când folosim termenul “ portofel”:

- O cheie privată principală (ca o parolă) din care poți genera chei publice pe care le poți împărtăși cu alții pentru a primi și trimite bitcoin.
- Interfața mobilă sau desktop prin care poți interacționa cu rețeaua Bitcoin pentru a verifica soldul tău de bitcoin, a trimite și primi tranzacții și a le transmite rețelei. Diferite tipuri de portofele, împreună cu beneficiile și compromisurile lor, vor fi descrise în secțiunea următoare.

7.2.2 Portofele auto-custodiale vs custodiale

Înainte de a detalia diferitele tipuri de portofele Bitcoin și caracteristicile lor, să facem o distincție importantă între portofelele auto-custodiale și cele custodiale, prezentată în tabelul de mai jos. Auto-custodial înseamnă că utilizatorul deține cheile private, ceea ce înseamnă că are cu adevărat posesia bitcoinului său, în timp ce în al doilea caz, o terță parte deține bitcoinul.

Tipul portofelului	Cine controlează monedele?	Beneficii	Riscuri
Portofele auto-custodiale	**Utilizatorul**	Control complet asupra fondurilor și tranzacțiilor, fără proces de aprobare sau blocare a contului, fără control corporativ sau guvernamental, protejat împotriva confiscării arbitrare, ca și cum ai păstra banii acasă.	Nu există recuperare dacă fraza de recuperare este pierdută, fară suport pentru clienți, toată responsabilitatea revine utilizatorului.
Portofele custodiale	**Parte terță furnizoare**	Recuperare ușoară dacă accesul este pierdut, suport pentru clienți mai facil	Fondurile sunt mereu conectate la internet, mai vulnerabile la hacking și breșe de securitate. Custodienii controlează și pot bloca conturile.

Primul Meu Bitcoin

Într-un portofel auto-custodial (numit și portofel non-custodial), doar tu ai cheile portofelului și ai control total asupra a ceea ce intră și iese. Pe de altă parte, într-un portofel custodial, altcineva deține cheia și poate accesa și gestiona conținutul portofelului în numele tău.

- Auto-custodia este ca și cum ai fi propria ta bancă. Tranzacțiile nu sunt supuse controlului sau autorității vreunui guvern sau companie, dar înseamnă și că tu porți întreaga responsabilitate pentru securitatea bitcoinului tău.
- Auto-custodia asigură că terții nu pot confisca bitcoinul tău fără consimțământul tău.
- Auto-custodia oferă liniște sufletească în perioade de incertitudine, știind că bitcoinuk tău este în siguranță.

Este important să alegi tipul potrivit de portofel pentru nevoile fiecăruia. Uneori, oamenilor li se pare dificil să distingă dacă instalează un portofel auto-custodial sau custodial. Acest tabel arată diferențele în procesul de instalare.

Tipul portofelului	Pasul 1: Alege un portofel	Pasul 2: Instalează portofelul	Pasul 3: Creează un portofel nou	Pasul 4: Asigură fraza de recuperare	Pasul 5: Folosește portofelul
Self Custodial Wallets	Alege un furnizor de portofel auto-custodial	Urmează instrucțiunile furnizorului	Generează fraze de recuperare și cel puțin o cheie privată	Păstrează fraza de recuperare într-un loc sigur	Începe să folosești portofelul pentru a primi și trimite bitcoin
Custodial Wallets	Alege un furnizor de portofel custodial	Urmează instrucțiunile furnizorului	Creează un cont la furnizorul portofelului	N/A (furnizorul deține cheia privată)	Începe să folosești portofelul pentru a primi și trimite bitcoin

NU AI CHEILE

NU AI MONEDEL

„Nu ai cheile, nu ai monedele” este o zicală populară printre deținătorii de bitcoin. Se referă la ideea că dacă nu ai control direct asupra cheilor private asociate portofelului tău Bitcoin, nu dețiu cu adevărat monedele.

Cine are acces la cheile tale private va dobândi proprietatea asupra bitcoinului tău. De aceea este extrem de important să le protejezi, ținându-le departe de ochii curioșilor! Vom vedea câteva metode de protecție mai târziu în carte.

În continuare, vom vorbi doar despre portofele auto-custodiale, unde utilizatorul deține cheile și are control complet asupra bitcoinului său.

Nu te îngrijora dacă pare complicat sau nu înțelegi totul—este o călătorie, iar pe măsură ce vei folosi Bitcoin, vei înțelege din ce în ce mai mult!

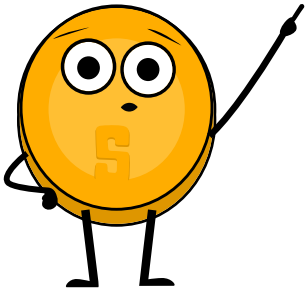
7.2.2 Portofele auto-custodiale vs custodiale

În funcție de locul unde este creată și stocată cheia ta privată, folosim denumiri diferite pentru a descrie portofelele Bitcoin. Dacă cheile sunt stocate pe smartphone-ul tău, îl numim „portofel mobil”. Dacă sunt stocate în siguranță pe un dispozitiv dedicat, îl numim „portofel hardware”. Dacă cheia este stocată doar pe hârtie, atunci se numește „portofel de hârtie”.

Denumirile diferite pe care le dăm portofelelor Bitcoin în funcție de structură:

Tip	Descriere	Avantaje	Dezavantaje	Exemplu Utilizator
Portofel Online	Un portofel accesat printr-un browser web.	Accesibil de pe orice dispozitiv cu conexiune la internet. Ușor de folosit.	Mai puțin sigur. Poate fi spart sau compromis.	Cineva care are nevoie să acceseze portofelul frecvent și nu are multe fonduri de stocat.
Portofel Mobil	Un portofel instalat pe un dispozitiv mobil.	Convenabil. Poate fi accesat de oriunde.	Poate fi pierdut dacă dispozitivul este rătăcit, furat sau spart.	Cineva care are nevoie să facă tranzacții din mers și nu are multe fonduri de stocat.
Portofel Desktop	Un portofel instalat pe un computer desktop.	Mai sigur decât portofelele online. Poate fi folosit offline.	Poate fi spart dacă computerul este infectat cu malware.	Cineva care dorește să stocheze o cantitate mare de bitcoin și se simte confortabil să folosească un computer desktop.
Portofel Hardware	Un dispozitiv fizic care stochează bitcoin offline.	Foarte sigur. Poate fi folosit offline.	Fondurile pot fi pierdute definitiv dacă dispozitivul este pierdut sau furat.	Cineva care dorește să stocheze o cantitate mare de bitcoin și este dispus să plătească pentru securitatea suplimentară oferită de un portofel hardware.
Portofel de hârtie	O înregistrare fizică a cheilor private și publice ale unui portofel bitcoin.	Very secure. Can be used offline.	Foarte sigur. Poate fi folosit offline.	Cineva care dorește să stocheze o cantitate mare de bitcoin și este dispus să ia măsuri suplimentare pentru a asigura securitatea.

Deoarece cheile pot fi mutate de pe un dispozitiv pe altul, „statutul” portofelului Bitcoin nu este definitiv. De exemplu, dacă generez cheile portofelului Bitcoin pe un computer și ulterior le încarc pe telefon, „portofelul desktop” devine „portofel mobil”.



Când vine vorba de stocarea bitcoinului tău, nu este vorba doar despre cine are controlul asupra lor - există multe alte riscuri de luat în considerare. De aceea este important să găsești o soluție de stocare care să fie atât sigură, cât și convenabilă.

Când analizezi compromisurile diferitelor tipuri de portofele, vei descoperi că nu există un portofel ideal care să satisfacă toate nevoile.

Când alegi un portofel Bitcoin, există câteva lucruri pe care ar trebui să le iei în considerare:

- **Securitate:** Asigură-te că portofelul are măsuri de securitate solide, cum ar fi autentificarea în doi pași și politici stricte pentru parole.
- **Privacy:** Verifică dacă portofelul îți permite să rămâi anonim sau dacă solicită informații personale pentru crearea unui cont.
- **Simplitate:** Alege un portofel care este ușor de folosit și de navigat, mai ales dacă ești nou în lumea Bitcoin.
- **Compatibilitate:** Asigură-te că portofelul este compatibil cu dispozitivul și sistemul tău de operare.
- **Taxe:** Compară taxele percepute de diferite portofele pentru a te asigura că obții cea mai bună ofertă.
- **Reputație:** Cercetează reputația portofelului și a echipei din spate pentru a te asigura că este de încredere.
- **Control:** Unele portofele îți oferă mai mult control asupra cheilor private, ceea ce poate fi un avantaj de securita

Gândește-te dacă vrei un portofel care îți oferă control total sau unul care este mai ușor de folosit, dar poate are mai puțin control.

7.2.3 Open-Source vs Closed-Source

Un alt factor important de luat în considerare atunci când alegi un portofel Bitcoin este să știi dacă aplicația sau software-ul este open-source.

Codul open-source este foarte important deoarece permite comunității să revizuiască codul și să continue dezvoltarea proiectului chiars dacă echipa ar înceta să lucreze la el.

Așa cum codul Bitcoin este complet deschis pentru ca oricine să îl poată revizui, folosi și modifica, la fel ar trebui să fie și codul portofelului pe care îl folosești pentru a stoca bitcoin.

Activitate: Discuție în clasă și evaluarea portofelelor Bitcoin pe bitcoin.org

Accesează următorul site web:
https://bitcoin.org/en/choose-your-wallet
și folosește noile cunoștințe despre portofelele Bitcoin pentru a selecta cel mai bun portofel pe baza criteriilor discutate astăzi.

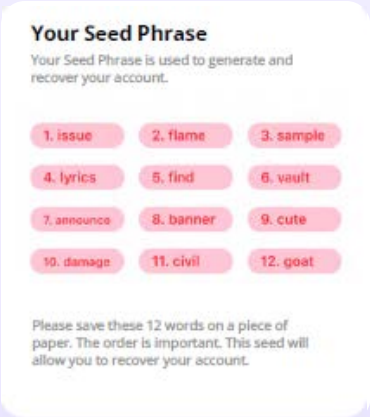
7.3 Configurarea unui portofel Bitcoin pe mobil

Acum că avem o înțelegere mai bună a portofelelor Bitcoin și a diferențelor dintre ele, vom vedea cum să folosim unul în practică. Pentru acest exemplu, vom crea un portofel mobil direct pe smartphone-ul nostru.

Activitate: Configurarea unui portofel Bitcoin

Dacă elevii nu au telefoane mobile, profesorul va oferi fiecărui elev un telefon împrumut. Există două opțiuni pentru această activitate.

Exercițiu în clasă: Opțiunea 1 - Descarcă un portofel nou.



Cum să creezi și să folosești un portofel Bitcoin:

1. Caută aplicația în App Store (iOS) sau Google Play Store (Android).

2. Deschide aplicația și salvează fraza de recuperare din 12 sau 24 de cuvinte (uneori numită seed phrase). Asigură-te că o notezi și o păstrezi într-un loc sigur! Această frază de recuperare îți permite să recuperezi accesul complet la fondurile tale dacă este necesar.

Amintește-ți că dacă pierzi sau uiți această secvență de cuvinte, nu vei putea accesa bitcoinul dacă pierzi accesul la portofel.

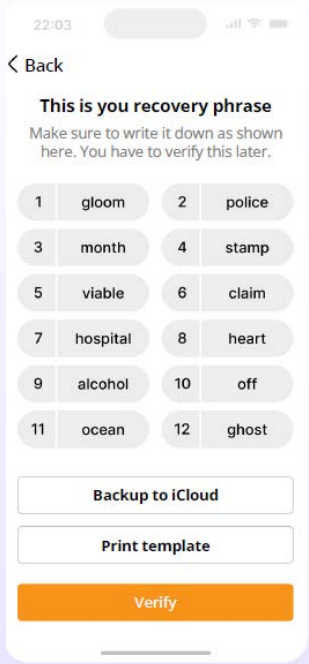
3. Trebuie să confirmi că ai salvat cu adevărat fraza de recuperare sau seed phrase. Pentru aceasta, trebuie să introduci, în aceeași ordine, cuvintele din fraza ta.

4. Ca măsură suplimentară de securitate, unele portofele îți permit să alegi o parolă. Cheia ta privată și prima adresă Bitcoin sunt create automat de portofelul tău.

Gândește-te la adresa ta publică ca la adresa de email – vrei să o împărtășești cu alții pentru ca ei să îți poată trimite bitcoin— sau, în cazul unei adrese de email, un email.

Gândește-te la adresa ta privată ca la parola de la email – nu ai vrea să o împărtășești cu nimeni deoarece le-ar oferi acces la emailul tău.

5. Folosește adresa „receive” pentru a primi bitcoin. Transferă bitcoin în portofelul tău. Cu un portofel auto-custodial, nu poți cumpăra întotdeauna bitcoin direct cu fiat, așa că poate fi nevoie să îi cumperi și să îi transferi dintr-un exchange.



Exercițiu în clasă: Opțiunea 2 - Restaurare portofel (timp limitat).

Descarcă un portofel Bitcoin și adaugă câțiva satoshi pentru fiecare elev.

Oferă fiecărui elev o frază seed pentru a recupera un portofel.

Ghidează elevii pas cu pas:

1. Când pornești portofelul pentru prima dată, vei vedea trei metode de creare a portofelului, apasă [Import]. Vei vedea un ecran de introducere, apasă [Restore].
2. Introdu fraza de recuperare din 12/18/24 cuvinte, unul câte unul, în ordinea corectă.
3. Apasă [Restore]. când ai terminat.
4. Vei vedea un mesaj "Import Successful" când portofelul a fost importat cu succes.

7.4 Primirea și trimiterea tranzacțiilor

O tranzacție bitcoin este un transfer de proprietate de bitcoin existent către un nou proprietar. Totuși, în loc să transfere monede reale, toate nodurile din rețea își actualizează copia locală a registrului public pentru a reflecta schimbarea de proprietate.

Când se trimite o tranzacție bitcoin, expeditorul semnează un mesaj pe care doar el îl poate semna cu cheia sa privată, semnalând rețelei că proprietatea monedelor bitcoin se transferă către adresa destinatarului.

Monedele bitcoin vor fi acum legate de o adresă de la care doar noul proprietar poate trimite, oferindu-i acestuia dreptul de proprietate asupra lor.

REGISTRU

Deținător cont	Valoare
Sebi	2.50
Adam	3.00
Mihai	6.00
Gicu	1.50
Robert	2.00
Ileana	1.75
Daniel	5.25

Mesaj de solicitare a tranzacției Bitcoin

Jim sends 0.50 BTC to Eliana

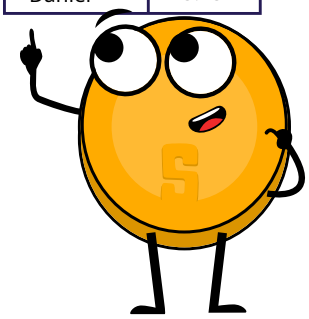
Jim ▶ **Eliana 0.50 BTC**

REGISTRU

Deținător cont	Valoare
Sebi	2.50
Adam	3.00
Mihai	6.00
Gicu	1.00
Robert	2.00
Ileana	2.25
Daniel	5.25

Noile tranzacții bitcoin sunt inițiate din portofele din întreaga lume, dar nu există un procesator central de plăți. În schimb, minerii din întreaga lume concurează pentru a înregistra tranzacțiile în registru.

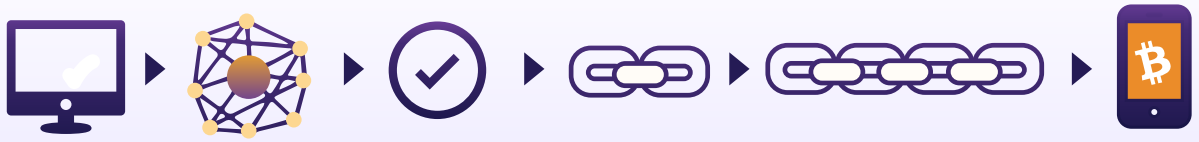
Să presupunem că Gicu îi datorează Ilenei 0,5 BTC și este gata să îi returneze suma. Ambii au portofele digitale.



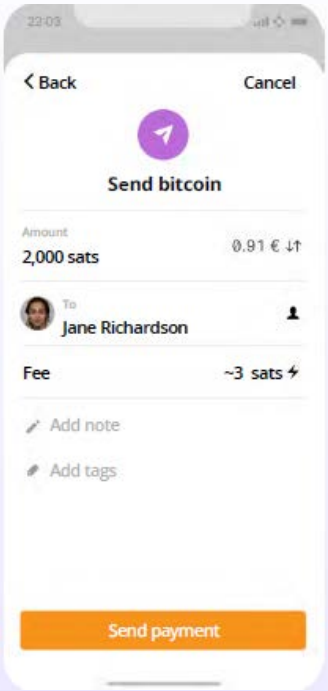
- Ileana îi transmite adresa lui Gicu.
- Gicu folosește software-ul portofelului său pentru a crea tranzacția, care include adresa Ilenei, suma de transferat (0,5 BTC) și un comision pentru miner.
- După semnarea tranzacției, aceasta este transmisă rețelei unde este verificată de noduri. Nodurile verifică validitatea tranzacției și se asigură că Gicu are suficiente fonduri. Dacă nu are, tranzacția este respinsă imediat.
- Odată ce tranzacția este verificată, este adăugată în blockchain de către mineri, iar fondurile sunt transferate către adresa Ilenei.
- Ileana poate apoi folosi cheia sa privată pentru a accesa fondurile transferate în portofelul ei.

Este important de menționat că, odată ce tranzacția este finalizată, aceasta nu poate fi anulată.

Cum funcționează o tranzacție Bitcoin



Cineva solicită o tranzacție → Tranzacția este transmisă către computerele P2P (noduri) → Minerii verifică tranzacția → Tranzacțiile sunt combinate pentru a forma un bloc de date → Un nou bloc este adăugat la blockchain-ul existent → Tranzacția este finalizată



Primirea tranzacțiilor Bitcoin:

Pentru a primi bitcoin, va trebui să îi furnizați expeditorului adresa portofelului dvs. Bitcoin. Aceasta este un șir unic de litere și cifre care reprezintă portofelul dvs. și este folosit pentru a-l identifica în rețeaua Bitcoin. Puteți găsi adresa portofelului dvs. conectându-vă la portofelul Bitcoin și căutând opțiunea „Primește” sau „Depune” bitcoin.

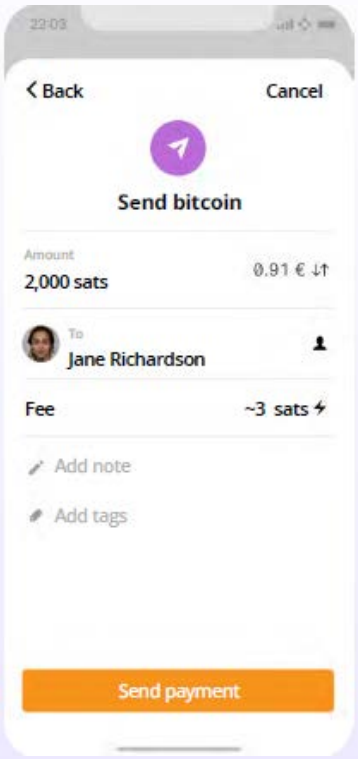
Puteți apoi să shear-uiți adresa Bitcoin cu expeditorul în unul dintre următoarele moduri:

1. Faceti copy-paste la adresa: Puteți copia adresa selectând-o și apăsând „Copy” pe tastatură, apoi „Paste” într-un e-mail sau mesaj către expeditor.
2. Share-uiți un link către portofelul Bitcoin: Unele portofele Bitcoin vă permit să creați un link către portofelul dvs. pe care îl puteți trimite expeditorului. Acesta poate apoi să acceseze linkul pentru a vă trimite bitcoin.
3. Generați un cod QR: Dacă expeditorul are un smartphone cu o aplicație de portofel Bitcoin, poate scana codul QR pentru a obține adresa dvs. Bitcoin.

Cum folosim Bitcoin

Odată ce expeditorul are adresa ta Bitcoin, îți poate trimite bitcoin introducând adresa ta și suma pe care dorește să ți-o trimită, apoi inițiază tranzacția. Bitcoinul va fi transmis către portofelul tău și vor fi vizibili odată ce tranzacția este confirmată de Rețeaua Bitcoin. Acest lucru durează de obicei câteva minute.

În continuare, vom analiza trimiterea tranzacțiilor bitcoin.



Trimiterea tranzacțiilor Bitcoin:

Pentru a trimite bitcoin, vei avea nevoie de câteva lucruri: un portofel Bitcoin, adresa Bitcoin a destinatarului și suma de bitcoin pe care dorești să o trimiți.

1. Deschide portofelul tău Bitcoin. Un cod SMS va fi trimis către numărul tău de telefon și va trebui să îl introduci în caseta de dialog. Alternativ, dacă ai activat Google 2FA, va trebui să introduci codul de șase cifre din aplicația Google Authenticator.
2. Navighează la funcția „Trimite” sau „Retrage” și copiază adresa destinatarului.
3. Introdu adresa Bitcoin a destinatarului lipind-o în câmpul „Către”.
4. Introdu suma de bitcoin pe care dorești să o trimiți în câmpul „Sumă”.
5. Verifică cu atenție adresa destinatarului și suma de trimis.
6. Înainte de a apăsa „Confirmă și Trimite”, îți recomandăm să verifici detaliile tranzacției încă o dată pentru a te asigura că trimiți suma corectă de bitcoin către adresa corectă a portofelului.
7. Confirmă tranzacția și așteaptă ca rețeaua să confirme tranzacția.

Acum știi cum să evaluezi, să selectezi și să configurezi un portofel Bitcoin auto-custodial. Trimiterea de bitcoin dintr-un portofel în altul pe rețeaua Bitcoin se numește trimiterea unei tranzacții „on-chain”. Acest lucru se datorează faptului că tranzacția are loc pe blockchain-ul principal al rețelei Bitcoin. Tranzacțiile on-chain sunt cea mai sigură modalitate de a tranzacționa cu bitcoin; totuși, tranzacțiile sunt mai scumpe și mai lente decât alte opțiuni, așa cum vom discuta în Capitolul 8.

Activitate: Tranzacții Bitcoin în Acțiune

Obiectiv Să înțelegi conceptele de bază și mecanica unei tranzacții bitcoin peer-to-peer.

Înainte de a începe, iată un scurt rezumat al actorilor cheie într-o tranzacție bitcoin:

- Expeditorii și destinatarii sunt părțile care doresc să tranzacționeze între ele.
- Nodurile validează tranzacțiile și stochează o copie completă a blockchain-ului. Nodurile light permit oamenilor să valideze tranzacții folosind mai puțină stocare și resurse computaționale.
- Minerii sunt responsabili pentru adăugarea de noi tranzacții în blockchain.

Înțelege-ți rolul.
Ți-a fost atribuit unul dintre următoarele: expeditor, destinatar, nod sau miner.

- Expeditorii vor fi responsabili pentru crearea și transmiterea tranzacțiilor.
- Destinatarii vor fi responsabili pentru primirea și verificarea tranzacțiilor.
- Nodurile vor fi responsabile pentru validarea tranzacțiilor.
- Minerii vor fi responsabili pentru adăugarea tranzacțiilor în blockchain.

Atât nodurile cât și destinatarii trebuie să verifice tranzacțiile

1. **Ca expeditor** Creează o tranzacție.

?

2. **Ca destinatar:** Ești responsabil pentru verificarea tranzacțiilor. Urmează acești pași:
   - Verifică biletul cu tranzacția pentru a te asigura că numărul corect de monede și numele sau inițialele destinatarului sunt scrise.
   - Numără monedele primite și compară-le cu numărul de monede scris pe notă.
   - Dacă monedele corespund, bifează caseta de aprobare. Dacă monedele nu corespund sau ai dubii, respinge tranzacția.

Monede trimise	Expeditor	Semnătura Expeditorului	Destinatar	Data și Ora	Aprobarea Destinatarului

3. **Monede trimise** Verifică și validează tranzacțiile. Ești responsabil pentru verificarea validității tranzacției.
   - Verifică dacă adresa expeditorului și adresa destinatarului sunt valide.
   - Verifică dacă expeditorul are suficiente fonduri pentru a finaliza tranzacția și că tranzacția nu cheltuiește dublu monedele.

Monede trimise	Expeditor	Semnătura Expeditorului	Destinatar	Data și Ora	Aprobarea Nodului

Cum folosim Bitcoin

4 **Ca miner:** Ești responsabil pentru adăugarea tranzacțiilor în blockchain. Urmează acești pași:

- Verifică tranzacțiile care au fost aprobate de destinatari și validate de noduri.
- Aruncă zarurile și compară numerele cu celălalt miner. Minerul cu numărul mai mic va adăuga tranzacția în blockchain.
- Pentru timpul, energia și efortul tău, vei câștiga un punct. La finalul activității, minerul cu cele mai multe puncte câștigă.

**Odată ce o tranzacție este adăugată în blockchain, nu poate fi schimbată sau anulată.

5 **Ține evidența soldului de monede:** Pe parcursul activității, ține evidența soldului de monede numărând monedele din portofelul digital.

Monede trimise	Expeditor	Semnătura Expeditorului	Destinatar	Data și Ora	Aprobarea

6 **Discută conceptele învățate cu clasa ta.**

7.5 Economisirea în Bitcoin

Bitcoin este o modalitate de a-ți proteja banii împotriva inflației și de a-i feri de controlul altora, dacă o faci corect. Economisirea în bitcoin oferă un mijloc de a stoca, acumula și construi avere în timp. După cum ai înțeles până acum, tipul de bani pe care alegi să îi economisești este una dintre cele mai importante decizii pe care le poți lua.

O alegere înțeleaptă îți permite să construiești un viitor mai bun pentru tine și familia ta.

Liniște sufletească: Dacă este stocat corect, Bitcoin este singura formă de proprietate pe care nimeni nu ți-o poate lua.

7.6 Nu te încrede, verifică

Orice ai face cu Bitcoin, amintește-ți acest lucru: „Nu te încrede, verifică.” Nu există lideri în Bitcoin. Nu ar trebui niciodată să urmezi orbește afirmațiile cuiva. Mai degrabă, ar trebui să pui mereu la îndoială ceea ce ți se spune și să verifici singur. Urmând această mantră, te vei proteja de pierderea bitcoinului tău. Aceste sfaturi se aplica de asemenea „următorului Bitcoin”, cât și pentru orice „oportunităților de investiții” sau promisiunilor de „profituri rapide și ușoare”.

Pe scurt, capitolul 7 ți-a oferit abilități importante pentru a folosi Bitcoin în viața de zi cu zi. Ai învățat cum să obții și să schimbi bitcoin în diferite moduri și cum să îi păstrezi în siguranță folosind diverse portofele.

Configurând portofelul Bitcoin pe mobil și realizând tranzacții cu alții, ai acum experiență practică pentru a folosi Bitcoin cu încredere zi de zi. Înțelegând Bitcoin ca modalitate de economisire și urmând ideea DYOR – „D Your Own Research”, ești acum în controlul banilor tăi.

În capitolul următor vom explora Lightning Network. Vom vedea cum această tehnologie inovatoare schimbă modul în care oamenii din întreaga lume accesează și folosesc banii. De la tranzacții zilnice la aplicații mai avansate, vei învăța cum Lightning Network oferă acces la servicii financiare pentru persoane, comunități și afaceri.

Capitolul #8

Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

8.0 Introducere

Activitate: Urmărește „Bitcoin Lightning Network Explained: Actually Works”

8.1 Rețeaua Lightning

8.2 Diferite Tipuri de Portofele Lightning

8.2.1 Portofele Auto-Custodial vs Custodial

8.2.2 Open Source vs Closed Source

8.3 Configurarea unui Portofel Bitcoin Lightning

8.4 Trimiterea și Primirea Tranzacțiilor Lightning

Activitate: Cursa de Ștafetă cu Portofel Lightning

8.5 Cumpărarea de Cafea și Alimente cu Bitcoin

8.5.1 Online: Plugin-uri de Plată - Ecommerce

8.5.2 În Persoană: Găsește un Comerciant în Zona Ta

8.5.3 Instrumente Tranziționale: Carduri Cadou și de Plată

8.5.4 Economii Circulare și Bitcoin ca Mediu de Schimb

Caietul elevului

Limba Română | 2025

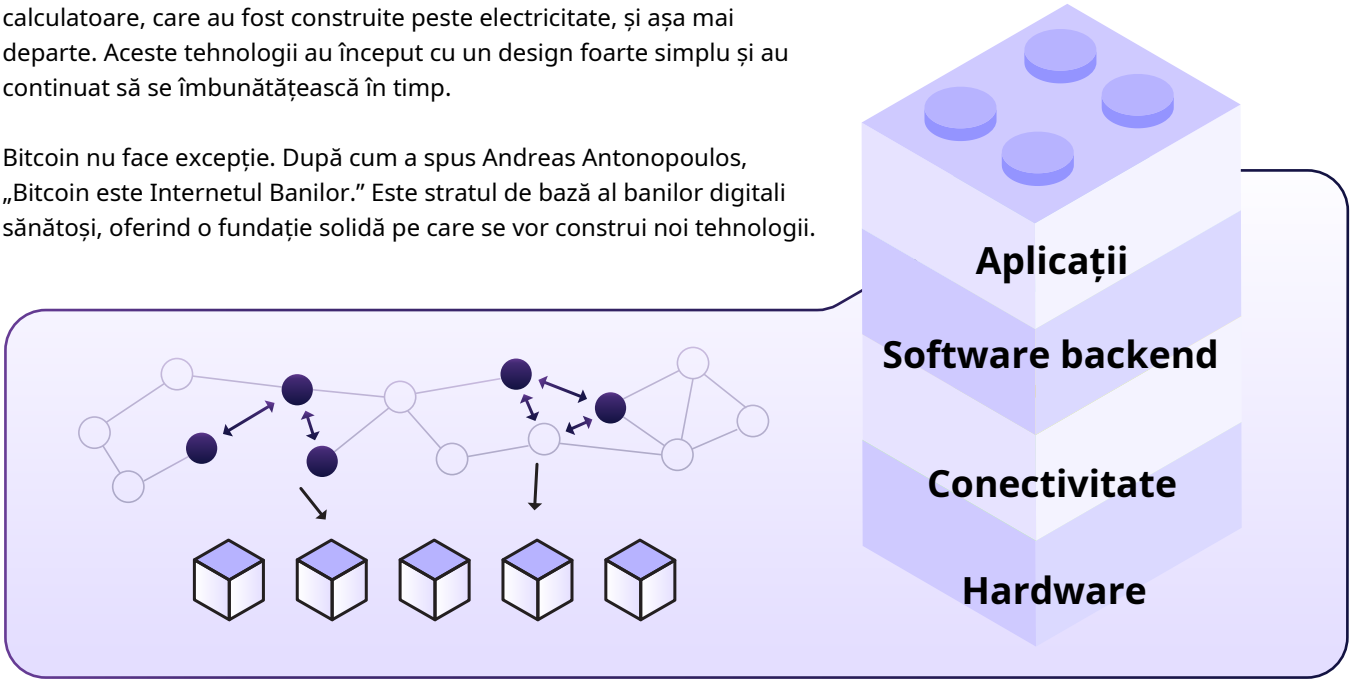
Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

8.0 Introducere

> Construim rețeaua Visa pentru bitcoin. Dar ceea ce cred că este deosebit, este că spre deosebire de Visa, oricine poate construi folosindu-se de ea.
>
> **My First Bitcoin**

Tehnologiile cresc și se extind de obicei în straturi (layers), ca o stivă. Gândește-te la site-ul tău preferat, email sau rețele sociale: acestea au fost construite peste protocolul de internet, care a fost construit peste calculatoare, care au fost construite peste electricitate, și așa mai departe. Aceste tehnologii au început cu un design foarte simplu și au continuat să se îmbunătățească în timp.

Bitcoin nu face excepție. După cum a spus Andreas Antonopoulos, „Bitcoin este Internetul Banilor." Este stratul de bază al banilor digitali sănătoși, oferind o fundație solidă pe care se vor construi noi tehnologii.



Unul dintre aceste straturi (layere) se numește Lightning Network. Acesta este ca o autostradă super-rapidă pentru Bitcoin, ajutând oamenii să trimită și să primească bitcoin rapid și cu comisioane foarte mici. Permite utilizatorilor să facă tranzacții instantanee și cu valori mici peste rețeaua obișnuită Bitcoin. Astfel, cumpărarea unei cafele sau plata unui prieten devine simplă și rapidă!

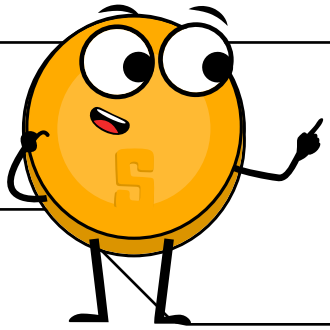
Amintește-ți: Un satoshi este ca cea mai mică diviziune a bitcoin. La fel cum un dolar poate fi împărțit în cenți, un bitcoin poate fi împărțit în unități mai mici numite satoshi. Un bitcoin este egal cu 100 de milioane de satoshi, ceea ce face ca satoshi să fie cele mai mici părți de valoare din sistemul Bitcoin. În acest capitol, când vorbim despre trimiterea de bitcoin prin Lightning Network, vom spune „trimiterea de sats", care sunt doar părți mai mici ale unui 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

Capitolul #8

Primul Meu Bitcoin

Urmărește acest videoclip despre Lightning



8.1 Rețeaua Lightning

Așa cum am văzut, Rețeaua Lightning servește ca un sistem de plată care facilitează tranzacții rapide și ieftine cu bitcoin. Funcționează prin creearea unui portofel comun unde ambele părți dețin niște bitcoin. Ei pot efectua numeroase tranzacții între ei fără a fi nevoie să înregistreze fiecare tranzacție pe registrul principal. Soldul final este apoi înregistrat pe registru după ce tranzacțiile sunt finalizate.

Rețeaua Lightning este un sistem de plată care permite utilizatorilor să trimită și să primească plăți rapid și ieftin folosind bitcoin. Funcționează prin configurarea unui portofel comun unde ambele persoane își stochează partea lor de bitcoin și apoi pot face tranzacții nelimitate între ei fără a atinge blockchain-ul principal. La final, soldul final este înregistrat pe blockchain.

Imaginează-ți o zi petrecută lucrând într-o cafenea. Anticipând că vei sta toată ziua, deschizi o notă de plată și plătești în avans, în loc să plătești de fiecare dată când comanzi ceva. Când ești gata să pleci la sfârșitul zilei, tu și proprietarul verificați nota pentru a achita suma finală. Dacă ai plătit mai mult decât ai consumat, primești banii înapoi.

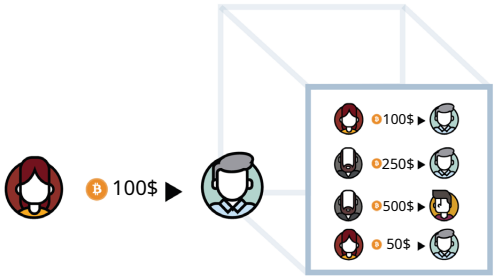
Acum, imaginează-ți mii de oameni făcând același lucru simultan și permițând altora să folosească notele lor pentru a se conecta cu mai mulți oameni. Aceasta este Rețeaua Lightning!

Cu Lightning, poți face plăți către oricine din rețea, nu doar către persoana cu care ai o notă directă. Plata ta poate naviga prin rețea până ajunge la destinație, chiar dacă nu ai un canal deschis cu destinatarul.

Să vedem diferența dintre tranzacțiile on-chain (tipul discutat în Capitolul 7) și tranzacțiile off-chain (Rețeaua Lightning):

Tranzacții On-Chain:

Acestea sunt tranzacții care au loc direct pe blockchain-ul Bitcoin. Confirmarea durează aproximativ 10 minute, iar comisioanele depind de dimensiunea tranzacției în bytes. Sunt mai sigure, dar mai lente.

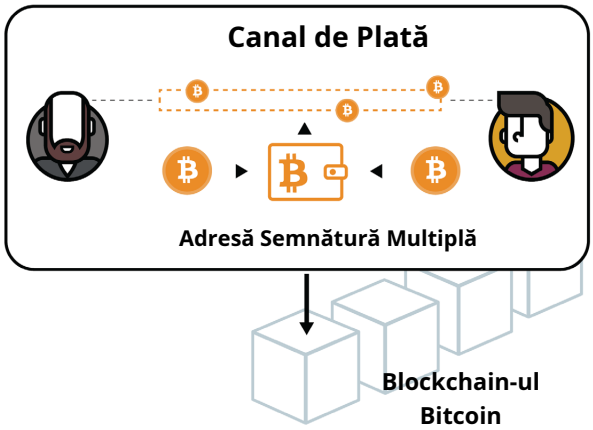


Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

Tranzacții Off-chain (Rețeaua Lightning):

Aceste tranzacții au loc pe o rețea separată construită peste blockchain-ul Bitcoin. Sunt finalizate mai rapid și cu comisioane mai mici.

Sunt folosite frecvent acolo unde reglementările și legile susțin adoptarea lor și unde caracteristici precum viteza și costul tranzacțiilor sunt mai importante. Comparativ cu tranzacțiile on-chain, sunt mai puțin sigure.



Rețea de Plăți	Rețeaua Bitcoin	Rețeaua Lightning
Definiție	O rețea digitală descentralizată care folosește criptografia pentru a securiza tranzacțiile financiare.	Un protocol de plată de tip Layer 2 care funcționează peste blockchain-ul Bitcoin, permițând tranzacții mai rapide și mai ieftine.
Avantaje	Descentralizată și sigură. Fără rambursări sau fraude. Poate fi folosită anonim. Acceptare globală.	Tranzacții mai rapide și mai ieftine. Scalabilitate crescută. Tranzacțiile off-chain nu aglomerează blockchain-ul.
Dezavantaje	Timp de tranzacție lent. Comisioane mari pentru anumite tipuri de tranzacții. Complex pentru începători.	Necesită încredere în operatorii de canal. Încă experimentală și nu este adoptată pe scară largă. Necesită tranzacție on-chain pentru deschiderea și închiderea canalelor.

8.2 Diferite tipuri de portofele Lightning

Un portofel Lightning este puțin diferit față de un portofel Bitcoin, deși îndeplinește aceeași funcție: primirea și trimiterea de bitcoin. Diferența este că un portofel Lightning îți permite să trimiți bitcoin pe Lightning Network, care este un al doilea strat deasupra rețelei Bitcoin.

Așa cum am văzut în capitolul precedent cu portofelele Bitcoin, portofelele Lightning au caracteristici diferite care trebuie luate în considerare înainte de a alege unul.

8.2.1 Portofele auto-custodial vs custodial

Portofelele Lightning pot fi împărțite în categorii foarte specifice, dar pentru simplitate, le vom împărți în două: auto-custodial și custodial.

La fel ca portofelele Bitcoin, un portofel Lightning auto-custodial este acela în care tu controlezi cheile portofelului, în timp ce un portofel Lightning custodial este acela în care altcineva controlează cheile.

Când folosești un portofel custodial, ți se oferă doar acces la portofel, dar depinzi de altcineva pentru permisiunea de a-ți folosi banii; renunți la proprietatea banilor pentru comoditate.

Acest lucru poate fi acceptabil pentru sume mici, deși este recomandat să folosești un portofel auto-custodial odată ce ai înțeles tehnologia.

În cele ce urmează, vom vorbi doar despre portofele Lightning auto-custodial.

8.2.2 Open Source vs Closed Source

La fel ca portofelele Bitcoin din capitolul precedent, portofelele Lightning pot fi open-source sau closed source. Folosește întotdeauna portofele open-source, deoarece acestea sunt complet deschise pentru revizuire și verificate de comunitate.

O aplicație open-source înseamnă, de asemenea, că oricine poate contribui la îmbunătățirea software-ului, ceea ce o face o alegere mai bună pentru utilizatori.

8.3 Configurarea unui portofel Bitcoin Lightning

Configurarea unui portofel Bitcoin Lightning auto-custodial este la fel ca configurarea unui portofel Bitcoin on-chain auto-custodial.

Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

Exercițiu în clasă Opțiunea 1. Descarcă un nou portofel Lightning auto-custodial

How to Create and Use a Bitcoin Lightning Wallet

1. Caută aplicația în App Store (iOS) sau Google Play Store (Android).

2. Deschide aplicația și salveaza fraza ta de recuperare de 12 sau 24 de cuvinte (uneori numită seed phrase). Asigură-te că o notezi și o păstrezi într-un loc sigur! Această frază de recuperare îți permite să recuperezi accesul complet la fondurile tale dacă este necesar.

Amintește-ți că dacă pierzi sau uiți această secvență de cuvinte, nu vei putea accesa monedele bitcoin dacă pierzi accesul la portofel.

3. Trebuie apoi să confirmi că ai salvat cu adevărat fraza de recuperare sau seed phrase. Pentru a face acest lucru, trebuie să introduci, în aceeași ordine, cuvintele din fraza ta seed.

4. Ca măsură suplimentară de securitate, unele portofele îți permit să alegi o parolă. Cheia ta privată și prima adresă Bitcoin sunt create automat de portofelul tău.

5. Generează o cerere de plata Lightning (invoice/factură), o adresă sau un cod QR pentru a primi bitcoin. Transferă bitcoin în portofelul tău. Cu un portofel auto-custodial, nu poți cumpăra întotdeauna bitcoin direct cu fiat, așa că poate fi nevoie să îi achiziționezi și să îi transferi dintr-un exchange mai întâi.

Fraza ta seed Fraza ta seed este folosită pentru a genera și recupera contul tău.

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

Te rugăm să salvezi aceste 12 cuvinte pe o bucată de hârtie. Ordinea este importantă. Această frază seed îți va permite să recuperezi contul.

*Notă: dacă folosești un portofel custodial, nu va trebui să urmezi unii dintre pașii din secțiunea 8.3. Utilizarea unui portofel custodial implică riscuri, deoarece nu vei avea control asupra cheii tale private, ceea ce înseamnă că nu vei avea control asupra banilor păstrați în portofel.

Acum că am configurat portofelul Bitcoin Lightning, să vedem cum primim și trimitem tranzacții Lightning și cum sunt diferite de tranzacțiile on-chain pe care le-am trimis în Capitolul 7.

8.4 Trimiterea și primirea tranzacțiilor Lightning

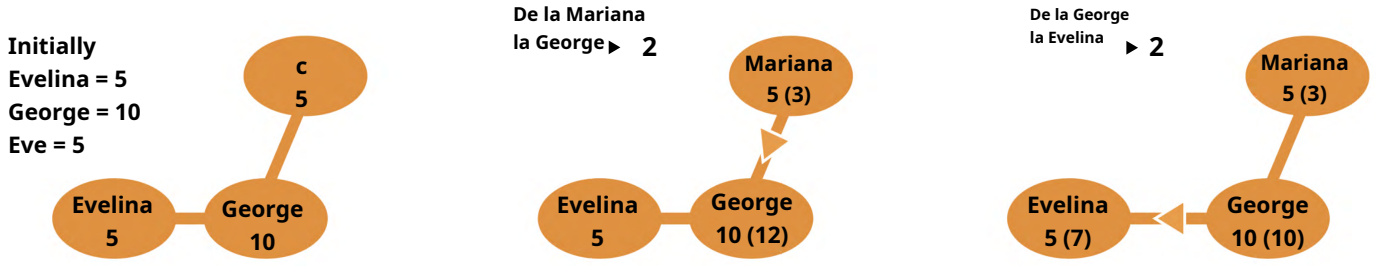
Cu un portofel Lightning, folosirea Bitcoin este rapidă, ieftină și privată, făcând tranzacțiile între două persoane foarte ușoare. Poți trimite și primi rapid bitcoin pentru lucruri de zi cu zi, cum ar fi cumpărarea unei cafele sau cumpărăturile.

Să vedem câteva exemple ale rețelei Lightning în acțiune.

Exemplul 1:

Mai jos, atât Mariana cât și Evelina au câte 5 unități de monedă. Mariana dorește să trimită 2 dintre unitățile sale către Evelina, așa că trimite 2 unități către George. George transmite apoi cele 2 unități către Evelina, care acum are 7 unități. Mariana are acum 3 unități. Și asta e tot! Tranzacția este finalizată.

Ideea principală aici este că Mariana și Evelina nu trebuie să treacă printr-o bancă sau alt intermediar pentru a realiza tranzacția.



George acționează ca intermediar sau „terță parte de încredere" în acest scenariu, unde Mariana și Evelina nu au încredere direct una în cealaltă. George primește cele 2 unități de la Mariana și apoi le transmite Evei, finalizând astfel tranzacția. Folosind pe George ca intermediar, Mariana și Evelina pot finaliza tranzacția fără a avea nevoie de o bancă sau altă instituție centralizată, ceea ce poate face tranzacția mai rapidă, mai ieftină și mai sigură. George este un element cheie în acest proces de tranzacție peer-to-peer.

Ca operator de nod în tranzacția din rețeaua Lightning, George beneficiază în mai multe moduri:

1. **Comisioane de tranzacție**

   George câștigă un mic comision pentru fiecare tranzacție care trece prin nodul său, ceea ce îl compensează pentru timpul și efortul depus în menținerea și operarea nodului.

2. **Participarea la rețea**

   Prin operarea unui nod Lightning, George participă la rețea și ajută la creșterea descentralizării, securității și stabilității acesteia. Acest lucru poate crește reputația și credibilitatea lui George ca operator de nod de încredere, făcându-l un intermediar mai atractiv pentru tranzacții viitoare.

2 Creșterea rețelei

Pe măsură ce rețeaua Lightning crește și tot mai mulți oameni o folosesc, numărul de tranzacții care trec prin nodul lui George va crește probabil, ceea ce poate duce la venituri mai mari din comisioanele de tranzacție.

4 Securitate sporită a rețelei

Rolul lui George ca intermediar ajută la creșterea securității rețelei prin adăugarea unui strat suplimentar de protecție între Mariana și Evelina. Acest lucru poate crește încrederea utilizatorilor în rețea, făcând-o mai atractivă pentru utilizatorii noi și ajutând la creșterea acesteia. În general, a fi operator de nod în rețeaua Lightning îi poate oferi lui George o sursă constantă de venit, precum și oportunitatea de a contribui la dezvoltarea și creșterea rețelei.

Tranzacțiile on-chain sunt mai lente, dar mai sigure, în timp ce cele off-chain (Lightning Network) sunt mai rapide, dar mai puțin sigure. Ar trebui să iei în considerare compromisurile între securitate și viteză, în funcție de nevoile tale.

Exemplul 2:

Mina are o mare pasiune pentru McDonald's; merge acolo pentru micul dejun, prânz și cină în fiecare zi! Dar, având atât de multe opțiuni de plată disponibile, nu este sigură care este cea mai bună alegere. Din fericire, a învățat câte ceva despre Bitcoin și Lightning Network. După ce a comparat tabelele de mai jos, Mina nu mai are nicio îndoială că metoda de plată Lightning este cea mai bună alegere.

Lightning Network vs Sistemul Bancar Tradițional

Beneficii	Lightning	Sistem Bancar Tradițional
Viteză	Rapid	Lent
Transparență	Transparent	Opac
Securitate	Sigur	Vulnerabil
Comisioane de tranzacție	Scăzute	Ridicate
Incluziune financiară	Ridicată	Limitată

Beneficii	Lightning	Sistem Bancar Tradițional
Scalabilitate	Ridicată	Scăzută
Confidențialitate	Ridicată	Moderată
Interoperabilitate	Ridicată	Scăzută
Conformitate legală	Moderată	Ridicată
Eficiență a costurilor	Ridicată	Moderată

Visa, Inc.

În medie, 1.700 de tranzacții pe secundă.

Capacitate de 65.000 de tranzacții pe secundă.

Bitcoin On-Chain

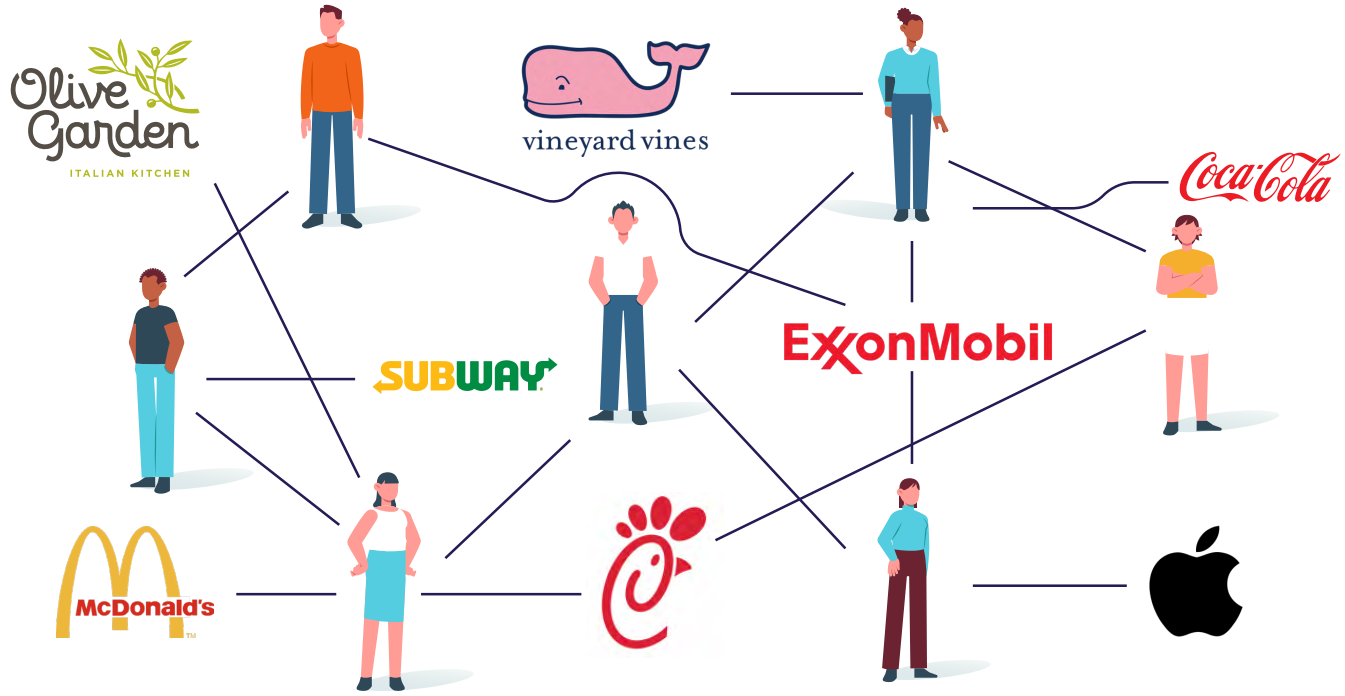
Capacitate de 7 tranzacții pe secundă.

Bitcoin Lightning Network

Milioane de tranzacții pe secundă.

Mina apreciază de asemenea a tranzacțiile rapide, sigure și eficiente din punct de vedere al costurilor, așa că a decis să folosească Lightning pentru achizițiile sale la McDonald's. Cu Lightning, se poate bucura de mese știind că plățile sunt procesate instantaneu, în siguranță și cu comisioane mici. În plus, deoarece Lightning Network oferă incluziune financiară, Mina poate plăti pentru mesele sale chiar dacă se află într-o zonă îndepărtată din El Salvador.

Pentru a începe să folosească Lightning, Mina descarcă mai întâi un portofel Lightning pe telefonul ei. Apoi își alimentează portofelul trimițând niște bitcoin din portofelul ei Bitcoin obișnuit către noul portofel Lightning. Acest proces se numește „alimentarea portofelului" sau „alimentarea unui canal de plată". Mina poate alimenta portofelul cu orice sumă de bitcoin cu care se simte confortabil, dar este important de menționat că suma de bitcoin blocată în portofelul Lightning nu poate fi folosită în tranzacții on-chain.



Odată ce portofelul Lightning este alimentat, Mina îl poate folosi pentru a face plăți către McDonald's.

McDonald's are un nod Lightning, așa că Mina poate deschide un canal de plată cu ei trimițând niște bitcoin din portofelul ei Lightning către o adresă specifică furnizată de McDonald's. Acest lucru mută bitcoinul ei de pe blockchain-ul Bitcoin într-o tranzacție off-chain pe Lightning Network.

Cu canalul de plată deschis, Mina poate acum să facă achiziții la McDonald's fără a fi nevoie să deschidă un canal nou sau să plătească comisioane mari de fiecare dată. Canalul rămâne deschis atât timp cât Mina și McDonald's doresc să îl folosească. De exemplu, dacă Mina cumpără un hamburger pentru 0.0005 bitcoin, canalul ține evidența că Mina are acum 0.9995 bitcoin. Și dacă cumpără un milkshake pentru 0.0003 bitcoin a doua zi, canalul ține evidența că Mina are acum 0.9992 bitcoin.

Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

Când Mina decide că vrea să folosească soldul ei de bitcoin pentru altceva, închide canalul prin transmiterea unei tranzacții de închidere pe blockchain-ul Bitcoin. Acest lucru se face prin inițierea unei tranzacții de închidere în portofelul Lightning, iar tranzacția conține soldul final al canalului, agreat de ambele părți. Tranzacția este apoi transmisă pe blockchain-ul Bitcoin și confirmată de un miner. Odată ce tranzacția este confirmată, canalul este închis, iar monedele bitcoin rămas în canal vor fi returnați către Mina și McDonald's.

Este important de menționat că închiderea unui canal poate dura ceva timp până să fie confirmată pe blockchain. În această perioadă de așteptare, fondurile sunt încă blocate în canal și nu pot fi folosite pentru tranzacții on-chain. Mina va primi o notificare odată ce tranzacția de închidere este confirmată.

Acum că am configurat portofelul Lightning și am citit despre cum să folosim Lightning Network pentru a trimite tranzacții, vom juca un joc în care trimitem satoshi (cea mai mică unitate de bitcoin) către alți elevi din clasă prin Lightning Network.

Aceasta este o hartă a întregii lumi. Cu Lightning Network, poți trimite satoshi către orice utilizator de pe rețea care are un portofel Bitcoin Lightning. Plata va ajunge în câteva secunde și va costa doar câțiva cenți.

Verifică singur:

Activitate: Exercițiu în clasă: Ștafeta portofelului Lightning

1. Mai întâi, va trebui să descarci un portofel Lightning pe telefonul sau computerul tău.
2. Urmează instrucțiunile pentru instalarea portofelului pe dispozitivul tău din secțiunea 8.3 a acestui capitol.
3. După ce portofelul este instalat, deschide-l și urmează pașii pentru configurare. Acest lucru poate implica crearea unui portofel nou sau restaurarea unuia existent și securizarea acestuia cu o parolă sau altă formă de autentificare.
4. Generează o factură Lightning, o adresă sau un cod QR pentru a primi bitcoin.
5. Când portofelul tău este configurat și ești gata să primești satoshi, profesorul îți va oferi ție și grupului tău o sumă inițială de satoshi, trimițându-i direct în portofelul tău.

A Scopul grupului vostru este să transferați satoshi din portofelul unei persoane în portofelul alteia folosind Lightning Network până ajung la ultima persoană din grup.

B Pentru a trimite satoshi altei persoane, deschide portofelul și urmează instrucțiunile pentru efectuarea unei plăți. Va trebui să furnizezi factura Lightning a destinatarului sau să scanezi un cod QR și să introduci suma de satoshi pe care dorești să o trimiți.

C Dacă grupul vostru este primul care reușește să trimită satoshi la ultima persoană, ați câștigat! (puteți păstrați satoshi).

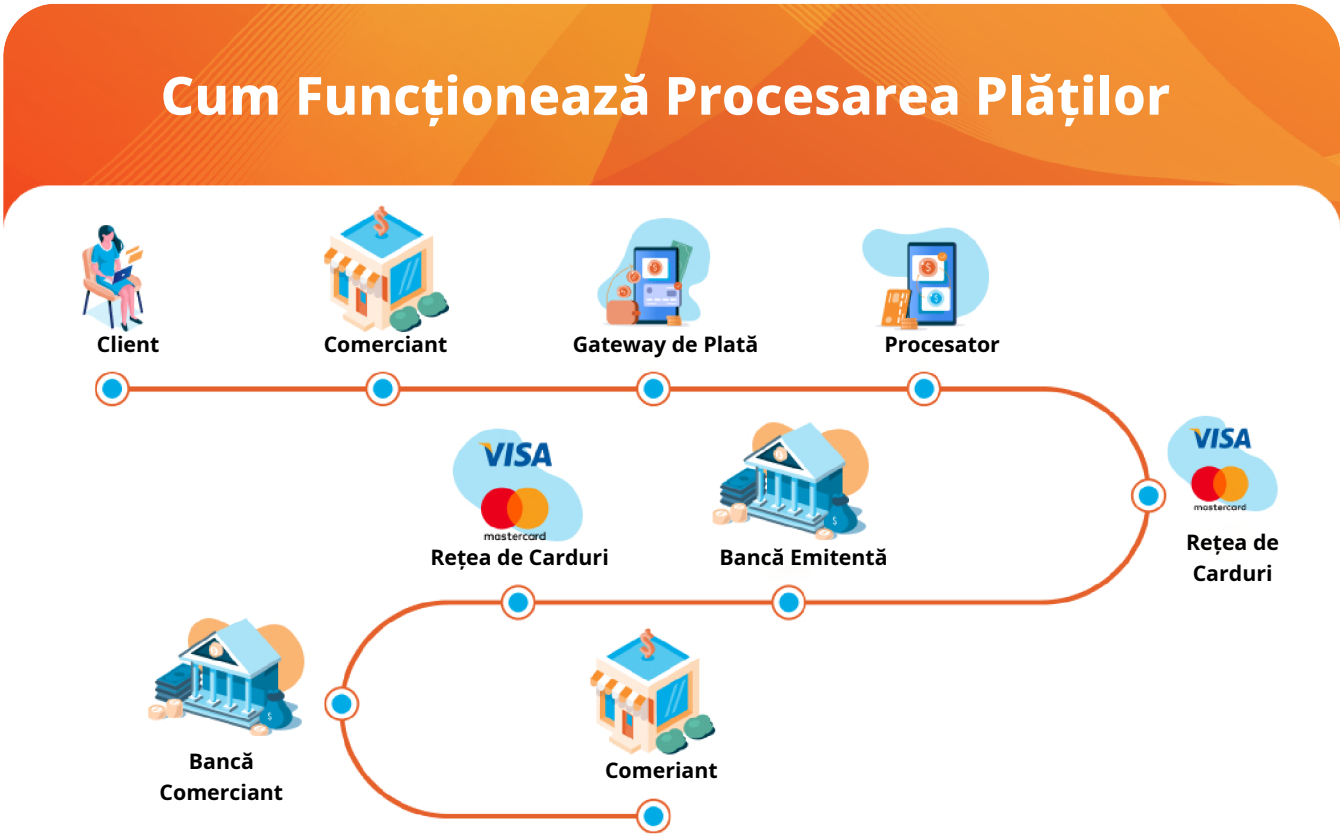
Discutări de dificultăți a avut grupul tău cu această activitate. A fost ușor, rapid și ieftin să trimiți o tranzacție? Crezi că Lightning Network este ușor de folosit și de înțeles?

Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

8.5 Cumpărarea cafelei și a alimentelor cu Bitcoin

Te-ai întrebat vreodată dacă poți folosi bitcoin pentru a cumpăra o cafeaua sau pentru a-ți face cumpărăturile? Se pare că poți. Există multe opțiuni atât online, cât și fizic, care îți permit să plătești cu bitcoin. Vom explora câteva dintre aceste opțiuni și instrumente care te vor ajuta să găsești magazine locale unde poți cheltui bitcoin.

Chiar dacă plata cu cardul de credit sau cu o aplicație poate părea ușor de înțeles pentru cel care plătește, procesarea plății este de fapt foarte complexă și implică multe părți diferite.



Când cumperi lucruri, sunt implicate multe părți, iar fiecare parte percepe o taxă. Pentru comercianți, aceste comisioane pot fi mari—peste 3% din preț, ceea ce este o sumă semnificativă pentru ei.

Și asta fără să mai menționăm comisioanele de schimb valutar!

Comisioane procesare carduri de credit

$100	-$1.75	-$0.14	-$0.30	-$97.81
Clientul Plătește	Banca Emitentă	Card Network Processors	Procesatori rețele carduri	Merge către comerciant

Cu Bitcoin și Lightning Network, afacerile pot primi plăți instantanee din orice colț al lumii printr-un sistem monetar deschis, sigur, nativ internetului, fără granițe și rezistent la cenzură.

În continuare, vom vedea câteva modalități prin care comercianții pot accepta cu ușurință plăți în bitcoin.

8.5.1 Online: Pluginuri de Plată - Ecommerce

BTCPayServer este un procesator de plăți open-source care permite comercianților să accepte plăți în bitcoin cu puține cunoștințe tehnice. Este complet gratuit și nu percepe niciun comision.

Afaceriile online pot integra BTCPayServer cu ușurință adăugând pluginul BTCPay pe site-ul lor.

Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

Deoarece BTCPay Server este un proiect open-source, nu o companie, poți contribui la proiect după ce înveți mai multe despre acesta și despre programare.

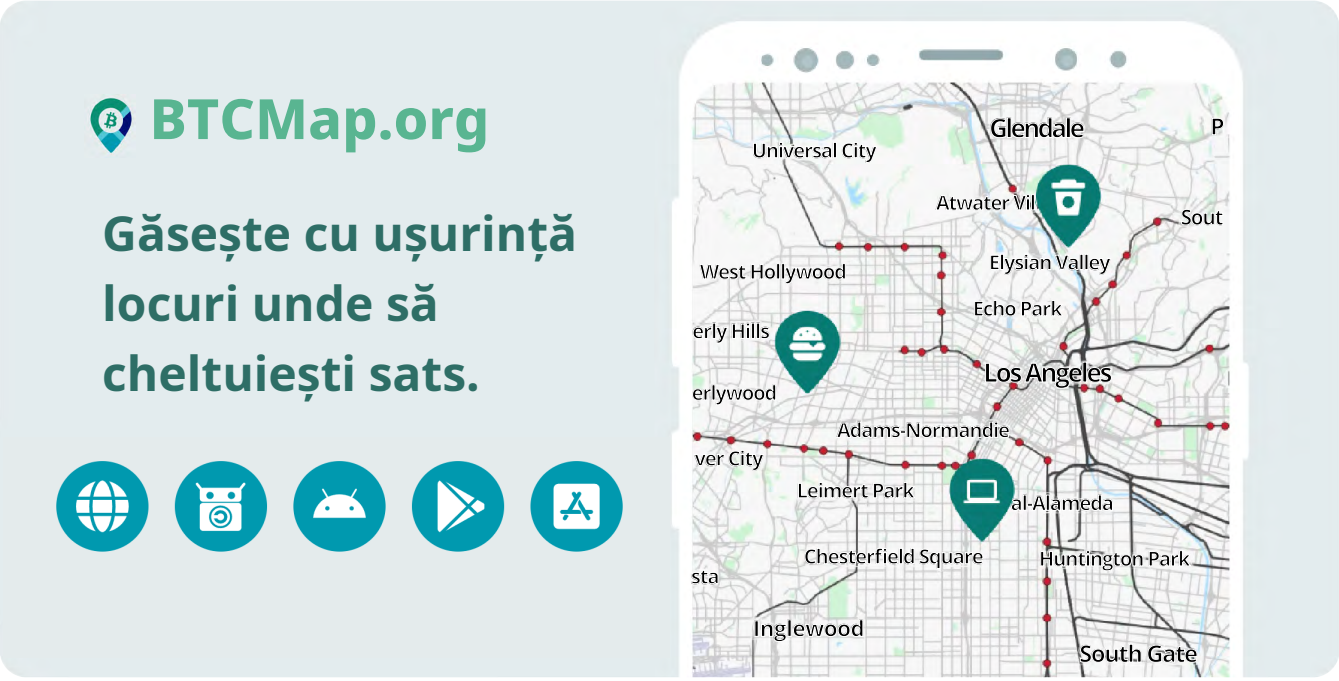
Vezi BTCPayServer la https://btcpayserver.org/ pentru mai multe informații despre cum poți folosi acest sistem de plată pentru afacerea ta fizică sau online.

8.5.2 Fizic: Găsește un Comerciant în Zona Ta

Magazinele fizice pot folosi BTCPayServer pentru a accepta plăți sau pot descărca pur și simplu un portofel Bitcoin și pot accepta plăți direct de pe telefon.

Pentru a găsi un comerciant care acceptă Bitcoin în zona ta, accesează BTCMap.org și caută regiunea ta.

BTCMap.org este o hartă open-source unde comercianții care acceptă Bitcoin își pot lista afacerile. Este un instrument puternic pentru cei care doresc să cheltuiască bitcoin.



8.5.3 Instrumente Tranziționale: Vouchere, Carduri Cadou și de Plată

Pentru a achiziționa produse sau servicii de la afaceri care încă nu acceptă Bitcoin, există un instrument intermediar pe care îl poți folosi: cardurile cadou.

Unele afaceri se concentrează pe cumpărarea și vânzarea de carduri cadou în schimbul bitcoin. Asta înseamnă că poți obține un card cadou pentru magazinul la care vrei să mergi, în schimbul bitcoin, și apoi să folosești cardul direct la magazin.

8.5.4 Economii Circulare și Bitcoin ca Mediu de Schimb

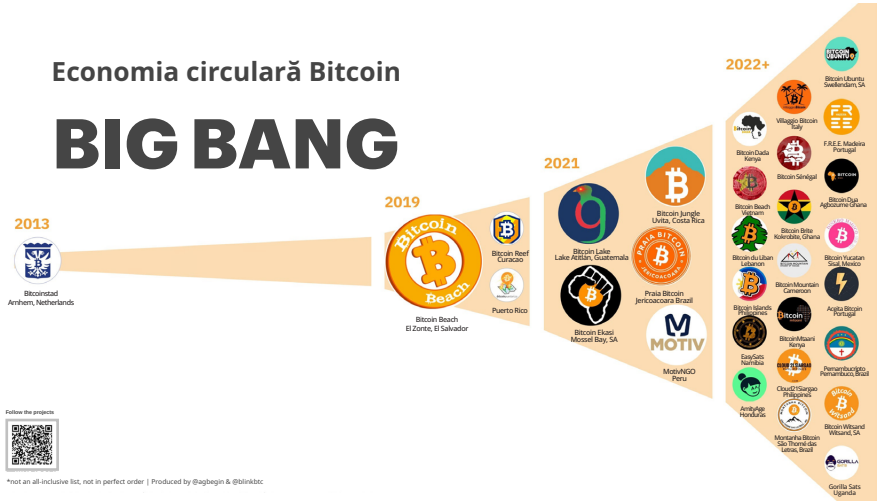
Conceptul de economie circulară provine din ideea de a minimiza risipa într-o economie prin reutilizarea și reciclarea cât mai multor produse și subproduse.

Pornind de la acest concept, o economie circulară Bitcoin este una în care tranzacțiile se fac în bitcoin și unde banii sub formă de bitcoin rămân și cresc în cadrul economiei, beneficiind indivizii și afacerile.

Lightning Network: Folosirea Bitcoin în Viața de Zi cu Zi

Rețeaua Lightning permite economiilor circulare Bitcoin să prospere peste tot în lume datorită tranzacțiilor bitcoin aproape instantanee și cu comisioane mici.

Prima economie circulară Bitcoin creată vreodată se află în Arnhem, Olanda. A fost creată cu mult înainte să existe Rețeaua Lightning, dar atunci comisioanele on-chain erau foarte mici!



A doua a fost Bitcoin Beach, situată în El Zonte, El Salvador. Aceasta a valorificat puterea Rețelei Lightning pentru a oferi comunității, care în mare nu avea access la servicii de banking, plăți digitale instantanee direct cu smartphone-urile!

Astăzi, sute de economii circulare sunt create peste tot în lume, alimentate de Bitcoin, Rețeaua Lightning și resurse educaționale.

Primul Meu Bitcoin

Pe BTCMap.org poți căuta comunități Bitcoin unde vei întâlni alți utilizatori Bitcoin și vei găsi afaceri care acceptă Bitcoin. Unii dintre profesori și elevi chiar au adăugat afaceri și economii circulare pe BTCMap.org, iar când vei fi pregătit, poți face și tu acest lucru!

Resursă: btcmap.org/communities

La finalul Capitolului 8, ai descoperit cum să folosești Bitcoin în viața de zi cu zi prin Rețeaua Lightning. Rețeaua Lightning face tranzacțiile mai rapide și mai accesibile, oferind o privire asupra modului în care Bitcoin va continua să se schimbe și să evolueze în straturi.

În Capitolul 9, vom investiga partea tehnică a Bitcoin. De la criptografie la noduri, mineri și multe altele, pregătește-te să descoperi cum funcționează cu adevărat Bitcoin.

Capitolul #9

O Introducere în Partea Tehnică a Bitcoin

9.0 Introducere

Activitate: Urmărește “How Bitcoin Works under the Hood”

9.1 Chei Publice și Private: Securitate prin Criptografie

9.1.1 Criptografie Chei Publice/Private

9.1.2 Explicația Hashingului

Activitate: Generează Hash SHA256

9.2 Modelul UTXO

9.3 Noduri și Mineri Bitcoin

9.3.1 Ce este un nod Bitcoin și cum îl configurez?

Activitate: Urmărește Video despre Noduri Bitcoin

9.3.2 Ce este un miner Bitcoin și cum funcționează minatul?

9.4 Ce este Mempool-ul?

Activitate: Mempool

9.5 Cum funcționează tranzacțiile Bitcoin de la început la sfârșit

Caietul elevului

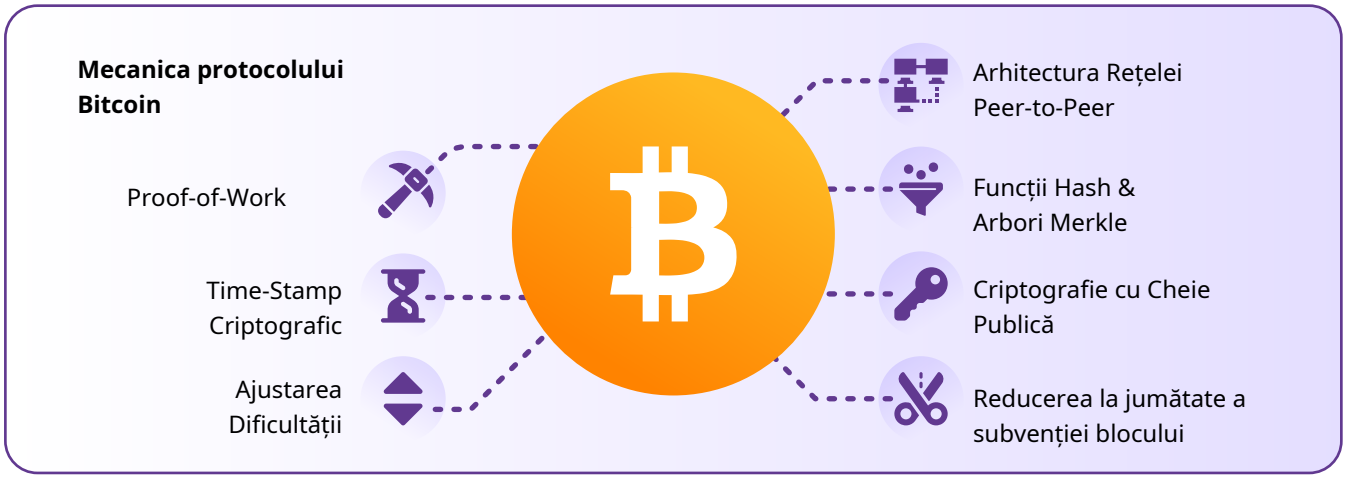
Limba Română | 2025

O Introducere în Partea Tehnică a Bitcoin

9.0 Introducere

> Bitcoin nu este „nereglementat”; este reglementat de algoritmi în loc să fie reglementat de birocrații guvernamentale. Ne-corupt.
>
> **My First Bitcoin**

În acest capitol, vom analiza mai atent tehnologia care permite rețelei Bitcoin să funcționeze într-un mod complet descentralizat. Vom explica pe înțelesul tuturor ce se întâmplă atunci când trimiți o tranzacție bitcoin, cum sunt procesate aceste tranzacții și ce rol au minerii și nodurile în rețeaua Bitcoin. Vom aborda unele concepte dificile și tehnice în acest capitol. Un lucru important de reținut: mulți oameni nu înțeleg cum funcționează internetul, totuși îl folosesc zilnic pentru a trimite emailuri, a contacta prieteni pe rețelele sociale și chiar pentru a-și plăti facturile. Învățarea părții tehnice despre cum funcționează Bitcoin este o călătorie lungă pe care nu toată lumea vrea să o parcurgă, chiar dacă decide să-l folosească drept bani. Deși te încurajăm să continui să înveți despre aspectele tehnice ale Bitcoin, vom păstra acest capitol focusat pe conceptele cheie de bază.



Dacă vrei să aprofundezi partea tehnică a modului în care funcționează Bitcoin, am inclus resurse la finalul acestui caiet de lucru. De asemenea, te poți înregistra pe site-ul nostru pentru Diploma Bitcoin - Ediția Tehnică pentru a fi notificat când acest curs mai tehnic va fi disponibil.

Hai să începem uitându-ne la un videoclip care arată cum funcționează rețeaua Bitcoin.

Activitate: Vizionați “How Bitcoin Works under the Hood”

Așa cum ai văzut în videoclip, rețeaua Bitcoin este pur și simplu un registru sau o evidență a tranzacțiilor stocată pe mai multe computere numite noduri. Registrul Bitcoin este pseudonim, ceea ce înseamnă că nu conține detalii personale, ci doar informații despre tranzacții și adrese. Registrul arată fiecare bitcoin și mișcările sale de la începutul rețelei, pe 3 ianuarie 2009.

Capitolul #9

Primul Meu Bitcoin

În continuare, vom analiza mai atent tehnologia care face posibil acest sistem.

9.1 Chei publice și private: Securitate prin criptografie

> Ceea ce ne oferă Bitcoin este o promisiune fermă: programul va rula exact așa cum este specificat.
> **My First Bitcoin**

9.1.1 Criptografie Chei Publice/Private

Criptografia este o metodă de a păstra informațiile secrete, ascunzându-le în cod.

- Criptarea este procesul de a lua informații și de a le transforma într-un cod special, făcându-le ilizibile pentru oricine nu are metoda corectă de decriptare. Este similar cu încuierea unui seif, unde doar persoana cu cheia sau combinația corectă îl poate deschide.

- Decriptarea, pe de altă parte, este procesul de a lua informațiile criptate și de a le face din nou lizibile, ca și cum ai descuia seiful și ai putea citi informațiile din interior.

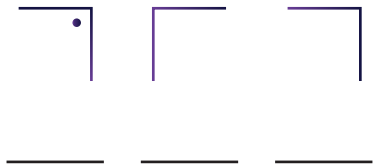
De exemplu, să presupunem că John vrea să-i trimită lui Arel un mesaj secret care nu este destinat altcuiva. Ei sunt de acord să folosească metoda de criptare Pigpen Cipher pentru a deghiza mesajul înainte de a-l trimite. Doar cei care au cifrul pot decripta mesajul, făcându-l ilizibil pentru oricine altcineva. Deși această metodă nu este considerată sigură astăzi, ilustrează principiul criptografiei cu cheie privată pentru trimiterea mesajelor.

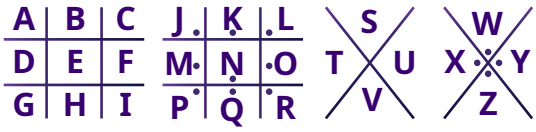
Cum se rezolvă

Pigpen Cipher

Când rezolvi Pigpen Cipher, jucătorul primește un mesaj criptat și un cifru. Pentru a decripta mesajul, jucătorul va găsi simbolul din mesajul criptat pe cifru pentru a găsi litera decriptată.

Exemplu de mesaj criptat:





Deci, cum funcționează criptografia în tranzacțiile bitcoin?

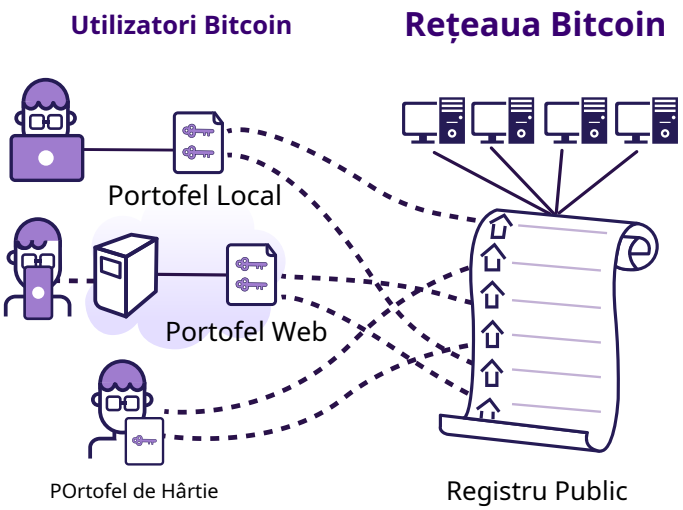
În criptografia tradițională cu cheie privată, Ioan și Aurel ar trebui să împartă mai întâi o cheie secretă, cum ar fi o parolă sau Pigpen Cipher. Ioan ar folosi apoi această cheie pentru a cripta mesajul înainte de a-l trimite lui Aurel. Aurel, care cunoaște și el cheia secretă, ar folosi aceeași cheie pentru a decripta mesajul și a-l citi.

Totuși, dacă altcineva deține cheia și interceptează mesajul, ar putea să-l decripteze și să-l citească.

O Introducere în Partea Tehnică a Bitcoin

Criptografia cu cheie publică, tipul folosit în tranzacțiile bitcoin, a rezolvat această problemă. Cu criptografia cu cheie publică, Ioan și Aurel nu trebuie să-și împărtășească parola sau metoda de criptare. În schimb, fiecare are două chei diferite: o cheie publică (care poate fi împărtășită cu oricine) și o cheie privată (care trebuie păstrată secretă).

În acest caz, când Ioan vrea să-i trimită un mesaj lui Aurel, poate folosi cheia publică a lui Aurel pentru a cripta propriul mesaj înainte de a-l trimite. Când Aurel primește mesajul, doar el îl poate decripta cu cheia sa privată. Oricine altcineva, chiar dacă interceptează mesajul, nu îl va putea citi. Șansele de a fura cheia sunt, de asemenea, mult mai mici, deoarece nici măcar Ioan și Aurel nu trebuie să-și împărtășească cheia unul altuia.



Așadar, principalul avantaj al criptografiei cu cheie publică față de cea privată este că permite comunicarea securizată fără ca expeditorul și destinatarul să fie nevoiți să share-uiască mai întâi o cheie secretă (sau o altă metodă de criptare precum cifrul Pigpen), care ar putea fi interceptată de o terță parte.

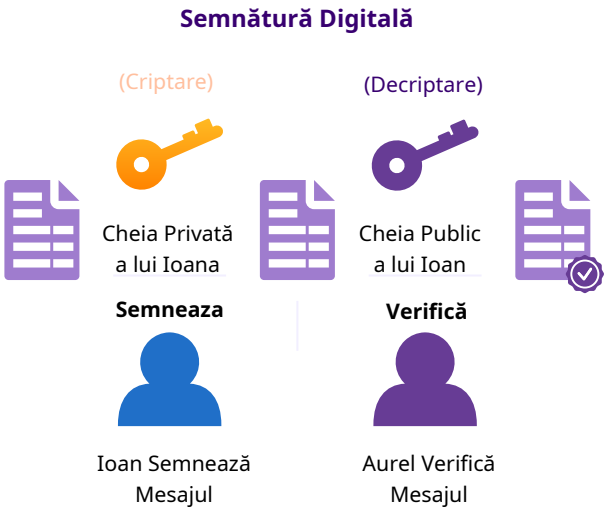
În Bitcoin, criptografia cu cheie publică nu este folosită pentru a trimite mesaje criptate. În schimb, este folosită pentru a crea semnături digitale unice care fac tranzacțiile bitcoin imuabile. O semnătură digitală este o modalitate de a dovedi autenticitatea unei tranzacții bitcoin, într-un mod similar cu semnarea unui document fizic.

Criptografie cu cheie publică (pentru fiecare tranzacție între doi utilizatori):

Fiecare utilizator are două chei: o cheie privată, care este păstrată secretă, și o cheie publică, care poate fi share-uită.

Cheia privată servește ca formă de identificare și dovadă a proprietății, confirmând: „Această adresă îmi aparține și am control asupra ei.”

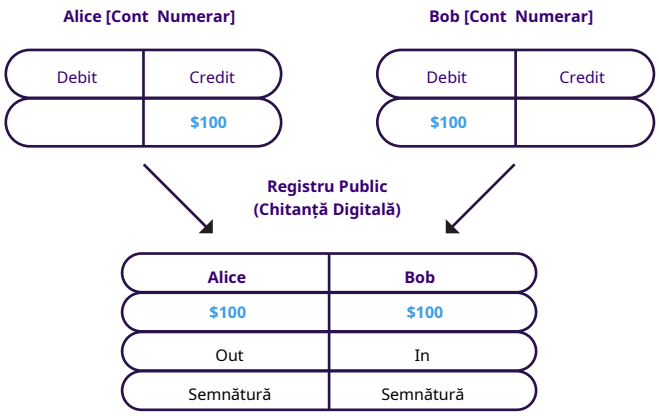
Se creează semnături digitale pentru a identifica tranzacțiile unice.



Capitolul #9

Primul Meu Bitcoin

- Tranzacțiile Bitcoin implică transferul unei anumite sume de bitcoin direct în contul altei persoane.
- Doar adevăratul deținător al monedelor bitcoin are controlul de a trimite banii către altcineva. Acest lucru asigură că proprietatea este protejată față de actori rău intenționați.
- Ca măsură suplimentară de protecție, fiecare tranzacție pe care o trimiți în Bitcoin primește automat o SEMNĂTURĂUNICĂ . Această semnăturăunică este susținută de o tehnologie rezistentă la manipulare care ajută rețeaua să verifice că adevăratul proprietar al monedelor bitcoin, și nu altcineva, i-a trimis.



Cum funcționează acest lucru într-o tranzacție reală cu bitcoin:

1. **Crearea tranzacției:**

   Un utilizator inițiază o tranzacție bitcoin specificând detalii precum adresa destinatarului și suma de bitcoin care urmează să fie trimisă.

1. **Generarea semnăturii digitale:**

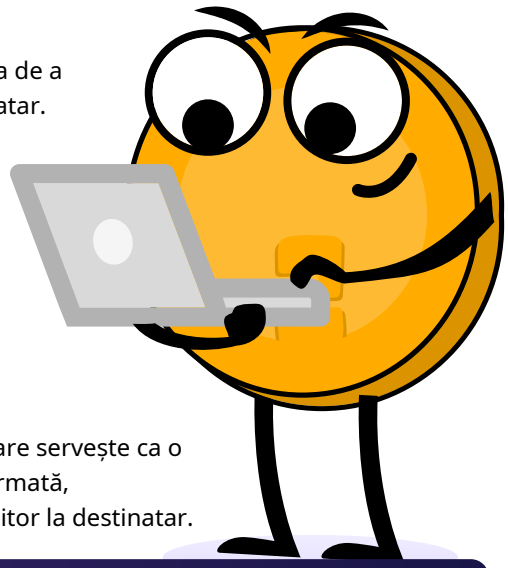
   Expeditorul generează o semnătură digitală unică folosind cheia privată.

2. **Transmiterea tranzacției:**

   Tranzacția semnată este transmisă rețelei Bitcoin, indicând intenția de a transfera proprietatea monedelor bitcoin de la expeditor la destinatar.

3. **Verificarea în rețea:**

   Nodurile din rețeaua Bitcoin primesc tranzacția și folosesc cheia publică a expeditorului pentru a verifica semnătura digitală.



4. **Confirmarea pe rețeaua Bitcoin:**

   Dacă verificarea are succes, tranzacția va fi adăugată în registru, care servește ca o evidență sigură și transparentă a tuturor tranzacțiilor. Odată confirmată, proprietatea monedelor bitcoin este transferată oficial de la expeditor la destinatar.

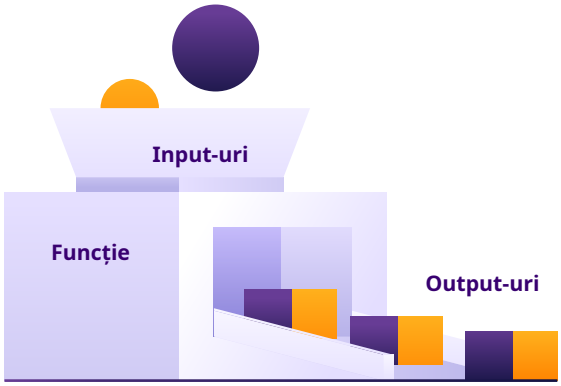
În concluzie, semnătura digitală, creată cu cheia privată a expeditorului, servește drept dovadă criptografică a autenticității și proprietății, permițând rețelei descentralizate Bitcoin să valideze și să înregistreze tranzacția în registru.

9.1.2 Explicarea Hashingului

Vă rugăm să nu vă lăsați intimidați de termenii tehnici și conceptele matematice care urmează. Înțelegem că nu toată lumea este pasionată de matematică, dar s-ar putea să vă surprindeți și să vedeți că și cele mai complexe idei pot fi înțelese cu puțin efort.

Ce este o funcție?

O funcție este ca o mașină care primește niște informații și le transformă în ceva nou. Informația pe care o dai funcției se numește input. Noua informație creată de funcție se numește output. Funcțiile ajută calculatoarele să îndeplinească sarcini și să rezolve probleme.



Gândește-te la o rețetă pentru a face o salată. Rețeta (sau funcția) îți spune ce ingrediente să folosești și cum să le amesteci pentru a obține salata. Poți pune ingrediente diferite, dar rețeta îți va da mereu salata ca rezultat. Funcțiile pot fi folosite pentru a face lucrurile mai ușoare și mai eficiente.

Această rețetă este o funcție care ia ingredientele ca input și generează salata amestecată ca output.

În Bitcoin, funcțiile sunt utilizate pentru a executa tranzacții. Știm deja că tranzacțiile în bitcoin sunt, în esență, transferuri de valoare (bani) de la o adresă la alta. Pentru a efectua o tranzacție, sunt folosite mai multe funcții criptografice pentru a valida tranzacția și a actualiza starea registrului Bitcoin.

Funcțiile folosite într-o tranzacție bitcoin includ verificarea autenticității input-urilor tranzacției, verificarea că expeditorul are fonduri suficiente și actualizarea soldurilor adreselor relevante. Odată ce o tranzacție este verificată și adăugată într-un bloc din registru, devine parte din evidența permanentă a tuturor tranzacțiilor din rețea.

Ce este o funcție unidirecțională?

O funcție unidirecțională folosește un set de instrucțiuni pentru a procesa informația și o transformă în ceva nou, la fel cum o rețetă de smoothie transformă ingredientele într-o băutură nouă. Dar, așa cum nu poți să "de-blendezi" un smoothie pentru a obține ingredientele nu poți inversa funcția unidirecțională pentru a obține informația inițială.

Capitolul #9

Primul Meu Bitcoin

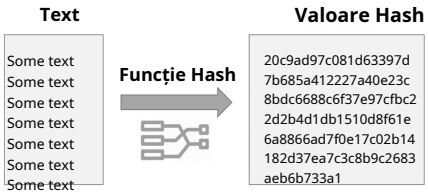
Criptografia cu cheie publică, din care face parte cheia publică, se bazează pe utilizarea funcțiilor unidirecționale, care fac dificilă determinarea cheii private pornind de la cheia publică. În teorie, nu este exact „imposibil” să găsești cheia privată pornind de la cheia publică, dar este extrem de dificil și ar necesita o cantitate uriașă de timp și putere de calcul pentru a realiza acest lucru.
Găsirea unei chei private pornind de la o cheie publică în Bitcoin este ca și cum ai încerca să găsești un ac într-un car cu fân de dimensiunea unui teren de fotbal. Acul reprezintă cheia privată, iar carul cu fân reprezintă toate posibilele chei private.

În același mod, funcțiile unidirecționale sunt concepute pentru a fi ireversibile și nu pot fi decriptate.

Ce este o funcție hash?

Hashing-ul este ca o amprentă pentru datele digitale. Este un proces prin care un mesaj digital este transformat într-un cod de lungime fixă, care servește drept identificator unic.

Asemenea unei amprente care poate identifica o persoană, un hash poate identifica un mesaj digital. Hash-urile sunt folosite în multe aplicații, inclusiv în tranzacțiile bitcoin.



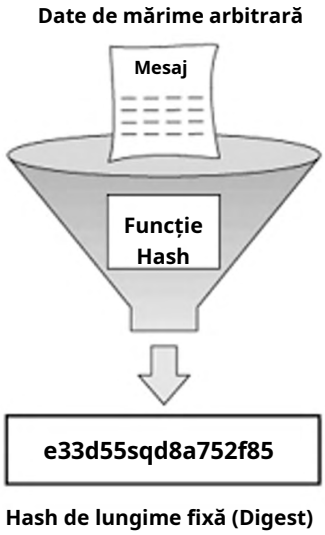
Cum este folosit hashing-ul în tranzacțiile bitcoin

În Bitcoin, fiecare tranzacție este hash-uită înainte de a fi adăugată într-un bloc din registru. Hash-ul acționează ca o semnătură pentru tranzacție, verificând că tranzacția este validă și nu a fost modificată. Dacă cineva încearcă să schimbe chiar și o singură literă din tranzacție, hash-ul va fi complet diferit, alertând pe ceilalți cu privire la schimbare.

Rolul hashing-ului în asigurarea securității

Hashing-ul este esențial pentru securitatea rețelei Bitcoin. Folosind hash-uri pentru a identifica tranzacțiile, rețeaua poate detecta orice încercare de a schimba sau manipula o tranzacție. Acest lucru ajută la prevenirea fraudei și asigură că toate tranzacțiile sunt înregistrate corect

O funcție hash este un tip de funcție unidirecțională care primește un input (numit „mesaj” sau „date”) și îl convertește într-o reprezentare numerică numită „hash”. Rezultatul hash este unic pentru datele de intrare, astfel încât chiar și o mică modificare a input-ului va duce la un hash complet diferit.



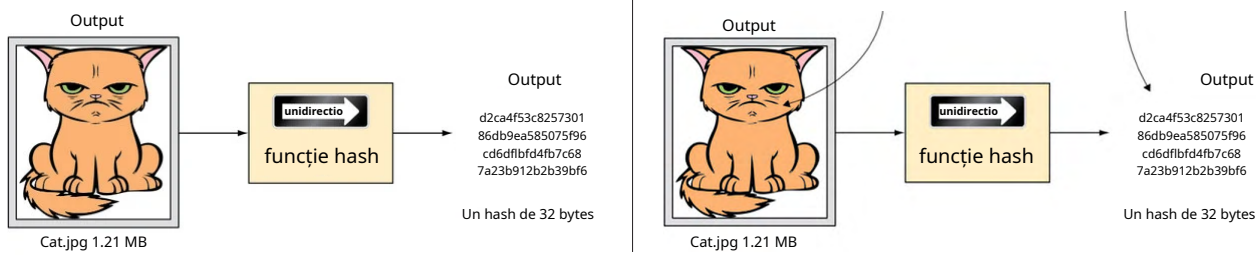
O funcție hash este ca o mașină de coduri secrete. Primește un mesaj și îl transformă într-un cod.

O Introducere în Partea Tehnică a Bitcoin

Codul arată întotdeauna la fel pentru același mesaj. Dacă modifici mesajul chiar și puțin, codul va fi complet diferit. Acest lucru ajută calculatoarele să păstreze informațiile și să verifice dacă ceva a fost schimbat.

Generează instant un hash SHA256 pentru orice șir de caractere sau valoare de intrare. Funcțiile de hash sunt folosite ca metode unidirecționale.

Activitate - Generează un Hash SHA256 →



Ouptu-ul sau hash-ul, are întotdeauna aceeași lungime, indiferent cât de lungă a fost informația originală.

Bitcoin folosește câteva tipuri specifice de funcții hash numite SHA-256 și RIPEMD160. Câteva exemple sunt mai jos:

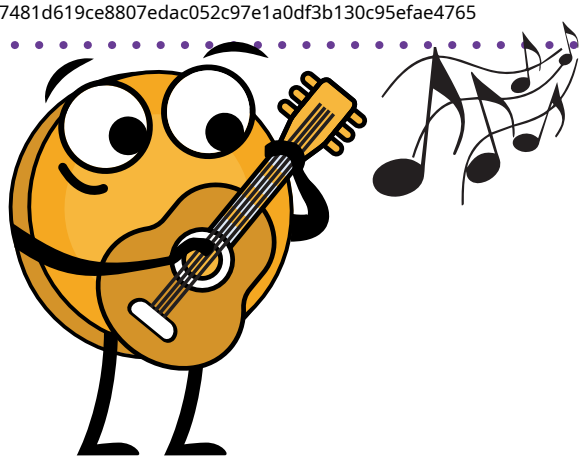
- Observă că o mică schimbare în al doilea input schimbă complet rezultatul față de primul exemplu.
- Al treilea input este un fișier uriaș, dar rezultatul are aceeași lungime fixă ca și celelalte două.

SHA256 hash of the string hello world
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

SHA256 hash of the string hello world.
7ddb227315f423250fc67f3be69c544628dffe41752af91c50ae0a9c49faeb87

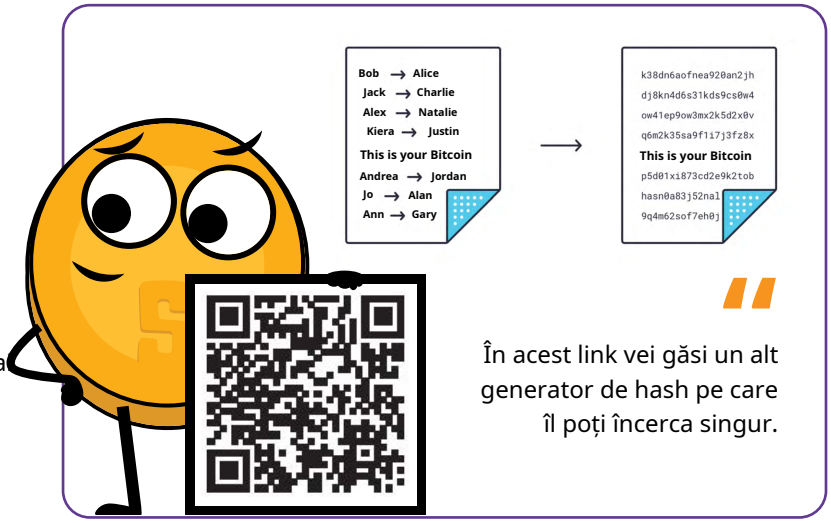
SHA256 hash of the downloadable iso file Ubuntu 18.10
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

Hashing-ul poate fi privit și ca o partitură muzicală care surprinde esența unei piese. Așa cum o partitură este o reprezentare unică a unei melodii, o valoare hash este o reprezentare unică a unui set de date. Comparând partitura unei piese cu interpretarea reală, un muzician poate determina dacă interpretarea este corectă. În mod similar, comparând valoarea hash a datelor primite cu valoarea hash originală, se poate determina dacă datele au fost modificate în timpul transmiterii.



Așa cum o mică abatere într-o interpretare muzicală poate face ca piesa să sune diferit, chiar și cea mai mică modificare a datelor originale va duce la o valoare hash diferită. Acest lucru face ca hashing-ul să fie un instrument puternic pentru asigurarea integrității și autenticității unei tranzacții bitcoin.

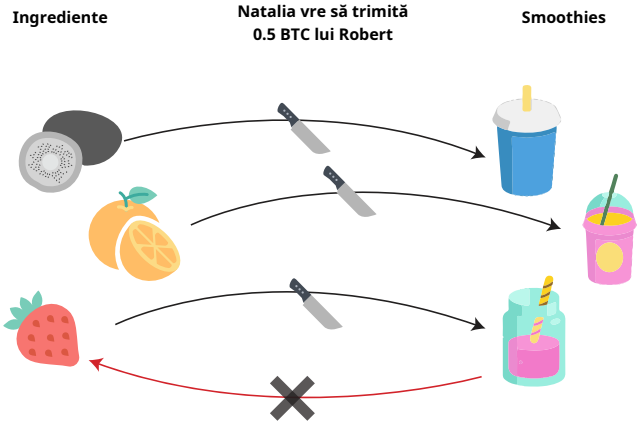
Procesul de codificare a cheii publice prin hashing este folosit pentru a îmbunătăți securitatea informațiilor, transformându-le într-un format de lungime fixă, ilizibil. Bitcoin folosește algoritmii SHA-256 și Ripemd-160 pentru a produce adrese publice. Rezultatul servește drept identificator unic pentru cheia publică și ajută la asigurarea integrității și securității tranzacțiilor stocate în registru. Prin criptarea informațiilor în acest mod, devine mai dificil pentru persoanele neautorizate să acceseze și să manipuleze datele.



În acest link vei găsi un alt generator de hash pe care îl poți încerca singur.

Hashare

O funcție hash primește orice intrare și produce o ieșire de lungime fixă (hash).



- **Determinist.**

  Aceleași ingrediente vor produce întotdeauna același smoothie.
- **Rezistență la pre-imagine.**

  Nu poți reconstrui o căpșună dintr-un smoothie.
- **Rezistență la corelație.**

  Schimbarea ușoară a ingredientelor duce la un smoothie complet diferit.
- **Rezistență la coliziune.**

  Este dificil să găsești ingrediente diferite pentru un smoothie care să rezulte exact același.
- **Viteză & Verificabilitate.**

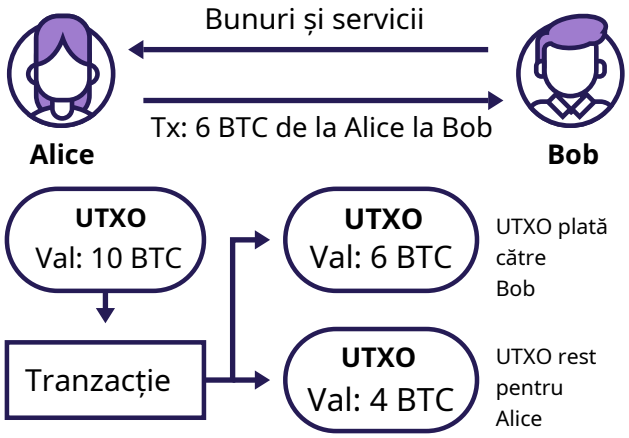
  Arunci fructele în mixer. Este rapid și ceea ce iese este cu siguranță un smoothie.

9.2 Modelul UTXO

UTXO - Unspent Transaction Output (Output de Tranzacție Necheltuit)

O Introducere în Partea Tehnică a Bitcoin

Ce sunt UTXO-urile?



În Bitcoin, tranzacțiile funcționează ca și cum ai sparge o bucată mai mare de aur în bucăți mai mici și ai trimite aceste bucăți mai mici atât altora, cât și ție însuți.

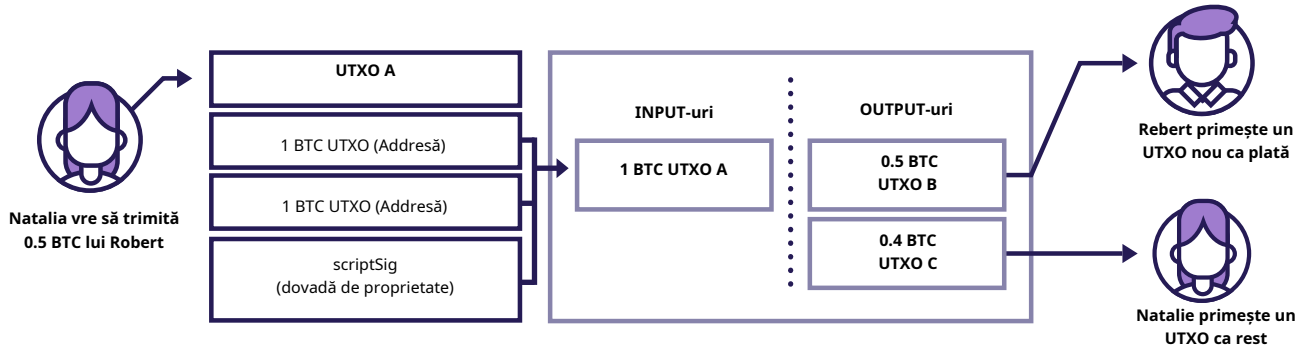
Poți privi UTXO-urile ca pe diferite dimensiuni și bucăți de bitcoin sau ca pe bancnote de valori diferite din portofelul tău. Când cheltuiești un UTXO, acesta este recreat într-un nou UTXO pentru destinatar, iar restul îți este trimis înapoi sub forma unui nou UTXO numit „UTXO de rest" (change UTXO). Este ca și cum ai folosi o bancnotă de 10$ pentru a cumpăra două cafele în valoare totală de 6$. Cafeneaua păstrează 6$ și îți dă 4$ rest.

Când trimiți bitcoin, trimiți întotdeauna întreaga sumă a unuia (sau mai multor) dintre UTXO-urile din portofelul tău Bitcoin. Ce se întâmplă? Trimiți o parte destinatarului, iar restul îl primești înapoi ca rest într-una dintre noile tale adrese Bitcoin. Restul primit se numește output de tranzacție necheltuit, sau UTXO (Unspent Transaction Output), și poate fi folosit ca input pentru o tranzacție viitoare.

Soldul portofelului tău Bitcoin este suma tuturor UTXO-urilor tale diferite. Deci, suma UTXO-urilor tale reprezintă suma de bitcoin pe care o deții.

> Este important să nu faci publice UTXO-urile tale, deoarece dacă cineva le cunoaște, îți poate urmări tranzacțiile bitcoin în rețea și, în cele din urmă, va ști câți bani deții.

În concluzie, de fiecare dată când faci o tranzacție, folosești unul sau mai multe dintre UTXO-urile existente pentru a cheltui bitcoin și se creează UTXO-uri noi (atât pentru tine, cât și pentru destinatar).



Când se face o tranzacție, suma de bitcoin trimisă este împărțită în mai multe output-uri, fiecare asociat cu o nouă adresă Bitcoin (un nou UTXO).

Capitolul #9

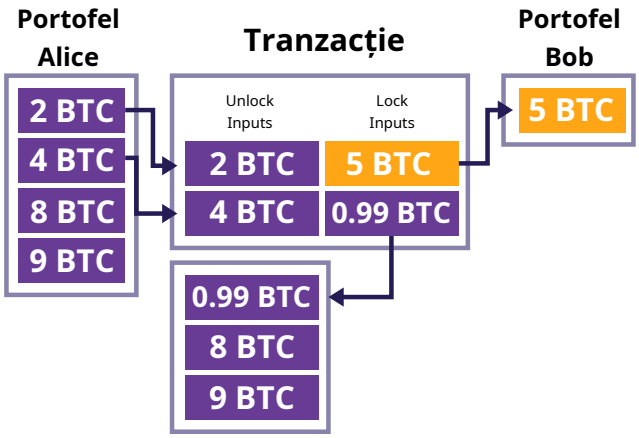
Primul Meu Bitcoin

Când trimiți bitcoin cuiva, vei folosi unul sau mai multe UTXO-uri ca sursă a fondurilor (input). Aceste UTXO-uri vor fi combinate, dacă este necesar, pentru a crea noi output-uri care aparțin atât destinatarului tranzacției, cât și ție. Aceste noi output-uri, sau UTXO-uri, vor deveni proprietatea destinatarului și a ta. Aceste UTXO-uri pot fi apoi folosite ca sursă de fonduri în alte tranzacții viitoare. Acest lanț de UTXO-uri creează un istoric transparent și ușor de urmărit al tuturor tranzacțiilor pe registrul Bitcoin, începând cu primul bloc (3 ianuarie 2009).

Un exemplu pentru a ilustra cum funcționează acest lucru: dacă vrei să trimiți doi bitcoin, dar ai doar un UTXO în valoare de cinci bitcoin, diferența de trei bitcoin îți este returnată ca „rest". Acest rest este un nou UTXO pentru tine și poți cheltui acel nou UTXO într-o tranzacție viitoare.

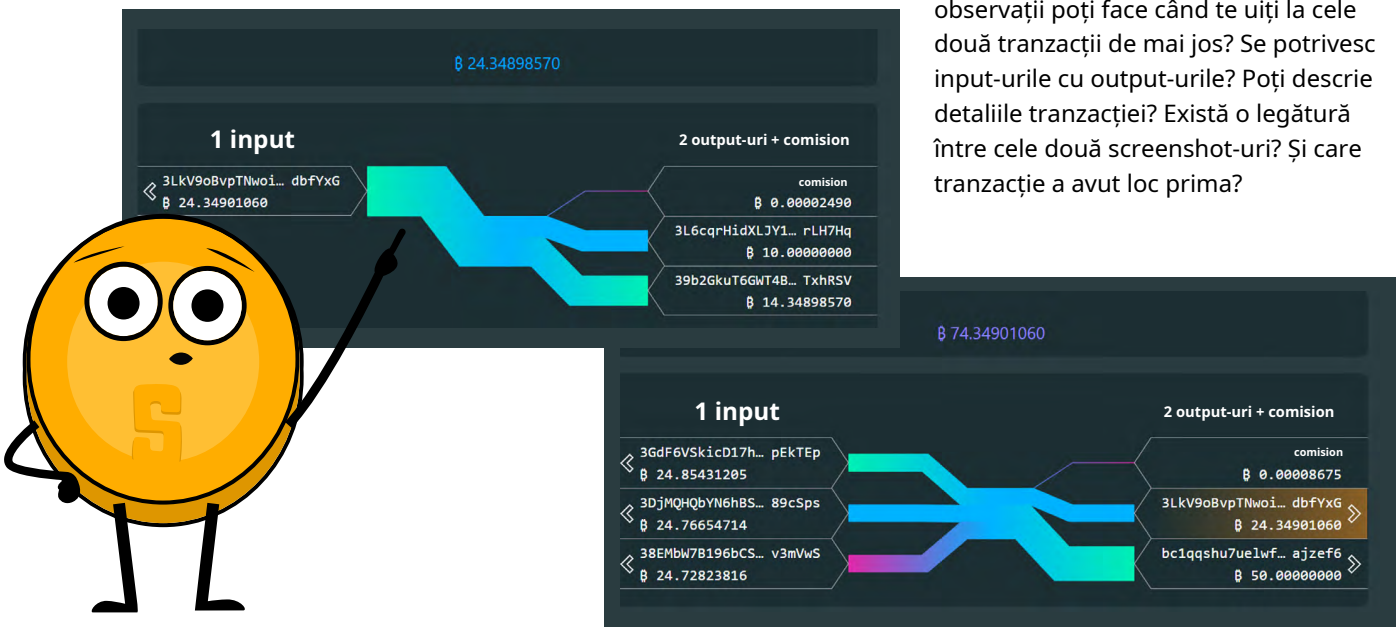
Un alt exemplu:

1. Alice vrea să-i trimită lui Bob cinci bitcoin.
2. Ea combină șase bitcoin din două dintre UTXO-urile ei.
3. Din aceste UTXO-uri, îi trimite lui Bob cinci bitcoin, primește 0,99 bitcoin ca rest înapoi la ea și trebuie să plătească un comision de tranzacție de 0,01.
4. După confirmare, tranzacția este adăugată în registrul Bitcoin, actualizând toate nodurile care au o copie a registrului.



Dacă Alice încearcă să folosească unul dintre output-urile deja cheltuite pentru a face o altă tranzacție, aceasta ar fi respinsă automat de noduri. Acest lucru se întâmplă deoarece nodurile mențin o copie a registrului Bitcoin (și a tuturor tranzacțiilor sale), astfel încât pot verifica cu ușurință soldul UTXO-urilor lui Alice și pot verifica dacă tranzacția nu este validă.

Mai jos este un screenshot real al unei tranzacții reale în care există doar un input. Totuși, soldul inițial ar putea, în alt caz, să fie suma mai multor UTXO-uri (mai multe input-uri). Ce observații poți face când te uiți la cele două tranzacții de mai jos? Se potrivesc input-urile cu output-urile? Poți descrie detaliile tranzacției? Există o legătură între cele două screenshot-uri? Și care tranzacție a avut loc prima?



9.3 O privire mai atentă asupra nodurilor și minerilor Bitcoin

În această secțiune, vom analiza mai detaliat două părți (și participanți) foarte importante ale rețelei Bitcoin, care au fost introduse pentru prima dată în Capitolul 6. Vom discuta despre:

4 **Noduri Bitcoin:**

Gardienii validării, a căror sarcină principală este să păstreze o copie a registrului Bitcoin, să se asigure că toate tranzacțiile sunt valide și că toată lumea respectă aceleași reguli.

Prin răspândirea acestei sarcini în întreaga lume, Bitcoin rămâne puternic împotriva potențialelor probleme. Aceste noduri ajută la menținerea sistemului de încredere și fidel ideii de descentralizare, unde nicio persoană sau grup nu are prea multă putere.

2 **Mineri Bitcoin:**

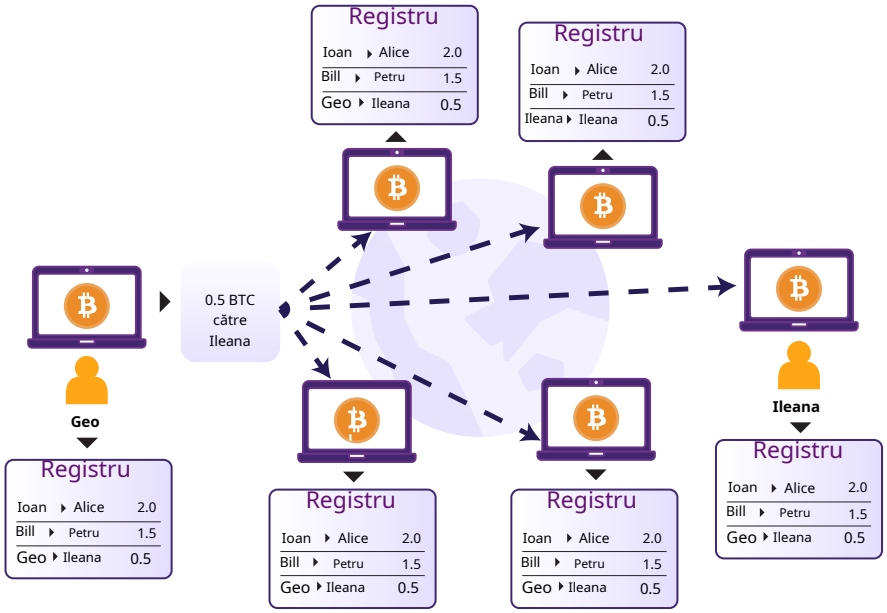
Arhitecții securității care folosesc computere puternice și electricitate pentru a verifica și confirma tranzacțiile, asigurându-se că totul este sigur. Această muncă ajută la menținerea registrului, sau blockchain-ului, rezistent la orice actori rău intenționați care ar încerca să-l compromită.

Împreună, nodurile și minerii Bitcoin lucrează ca o echipă pentru a menține un sistem descentralizat, sigur și puternic —o nouă modalitate de a gestiona banii, pe care oamenii din întreaga lume se pot baza. Să explorăm aceste roluri în detaliu pentru a înțelege cum contribuie la sistemul inovator Bitcoin.

9.3.1 Ce este un nod Bitcoin și cum pot să configurez unul?

Un nod Bitcoin poate suna tehnic, dar este doar un software care rulează o copie a registrului Bitcoin. Când rulezi propriul tău nod Bitcoin, câștigi o voce în stabilirea regulilor rețelei Bitcoin.

Imaginează-ți asta: dacă un grup de persoane încearcă să schimbe modul în care funcționează Bitcoin, de exemplu prin modificarea ofertei totale de bitcoin, ai un cuvânt de spus. Poți alege să nu-ți actualizezi nodul la noul sistem, ceea ce înseamnă că votezi pentru a menține regulile rețelei pe care o susții.



Să ne imaginăm un nod Bitcoin ca pe un polițist digital de trafic cu câteva sarcini esențiale:

1. **Gardieni ai validării:**

Un nod Bitcoin păstrează o copie digitală a blockchain-ului, care este ca un registru comun al tuturor tranzactiilor cu bitcoin. Multe noduri din întreaga lume detin această evidentă.

2. **Centru de comunicare:**

Nodurile se conectează între ele, creând o rețea vastă de comunicare. Ele împărtășesc informații, în special tranzacții care așteaptă să fie adăugate în blockchain, stocate într-o „sală de așteptare” numită „mempool".

3. **Verificator de calitate:**

Fiecare adăugare la blockchain este atent verificată. Nodurile se asigură că tranzacțiile sunt valide, respingând orice nu respectă regulile rețelei Bitcoin.

4. **Informator blockchain:**

Alte programe, precum portofelele, pot solicita unui nod informații despre blockchain, cum ar fi soldurile de bitcoin. Nodurile servesc drept centre de informare.

5. **Întâmpimă noduri noi:**

Când un nod nou dorește să se alăture, nodurile existente oferă cu generozitate o copie a blockchain-ului. Noul nod verifică independent validitatea fiecărei tranzacții.

Activitate:

Nodurile Bitcoin

Una dintre opțiunile de a rula propriul tău nod este să descarci software-ul Bitcoin Core și să îi acorzi timp pentru a descărca întregul blockchain. Odată pregătit, îl poți lăsa pornit și, aproximativ la fiecare 10 minute, sosesc noi blocuri cu tranzacții. Nodul tău verifică validitatea acestora, adăugându-le la copia ta locală a blockchain-ului.

Resursă

Bitcoin Core Software

Rularea unui nod oferă suveranitate și independență. Nu depinzi de alții; este propriul tău polițist de trafic. Spre deosebire de portofelul tău Bitcoin, care nu are o copie a blockchain-ului, un nod asigură autosuficiența. În loc să ai încredere în alții cu privire la deținerile tale de bitcoin (și starea rețelei Bitcoin), portofelul tău comunică cu nodul tău personal, făcând experiența digitală mai sigură și mai de încredere.

9.3.2. Ce este un miner Bitcoin și cum funcționează mineritul?

> Scopul mineritului nu este crearea de noi bitcoin; acesta este sistemul de stimulente. Minatul este mecanismul prin care securitatea Bitcoin este descentralizată.
>
> **My First Bitcoin**

O Introducere în Partea Tehnică a Bitcoin

Minerii colectează tranzacții neconfirmate, formează un bloc și consumă energie pentru a căuta o cheie valoroasă care va adăuga și securiza locul blocului în blockchain.

Minerii sunt într-o cursă pentru a adăuga următorul bloc în blockchain. Premiul căutat este un „hash valid de bloc", ascuns cu istețime printre miliarde de altele, și doar o cheie specifică atribuită de rețea îl poate debloca. Imaginează-ți un uriaș stog de fân plin cu milioane de chei, fiecare reprezentând un hash unic de bloc. Rețeaua a ales o cheie specifică pentru a debloca o recompensă valoroasă. Minerii răscolesc stogul de fân, testând fiecare cheie în lacăt, dar doar un miner norocos va descoperi potrivirea perfectă.

Odată ce un miner găsește hash-ul corect al blocului, îl împărtășește rețelei împreună cu blocul său de tranzacții noi. Alți mineri verifică soluția pentru a se asigura că este potrivită. Dacă totul este în regulă, blocul este adăugat la blockchain, creând un registru public și securizat.

Minerii câștigă recompense în două moduri:

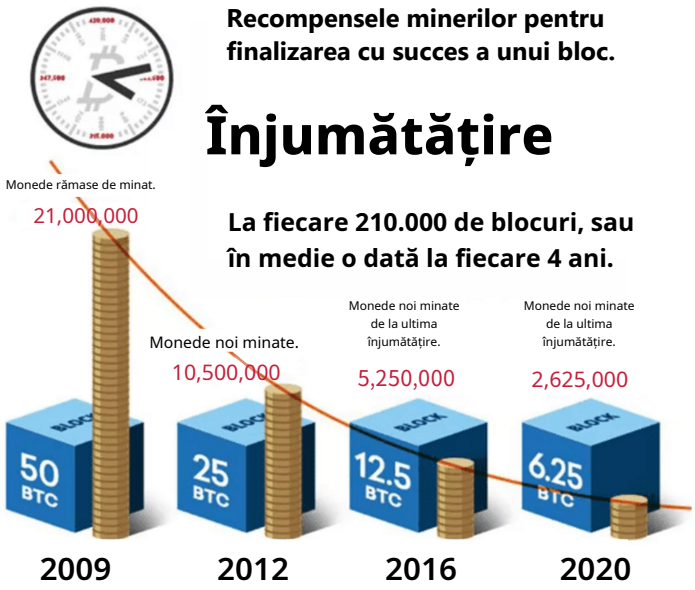
1. Recompense de bloc -block reward
2. Comisioane de tranzacție

Recompensele de bloc sunt noi bitcoin eliberați în circulație cu fiecare bloc adăugat la blockchain. Comisioanele de tranzacție sunt plăți mici în bitcoin pe care utilizatorii le fac pentru ca tranzacțiile lor să fie procesate mai rapid și prioritizate de către miner. Minerii pot alege ce tranzacții să includă în blocul pe care îl minează, de obicei acordând prioritate celor cu comisioane de tranzacție mai mari.

Înjumătățirile Bitcoin

O înjumătățire Bitcoin este o parte esențială a universului Bitcoin care ajută la menținerea rarității și valorii sale în timp. După cum știi, există o ofertă fixă de 21.000.000 de bitcoin în total. Această ofertă nu a fost disponibilă în totalitate din ziua lansării Bitcoin. În schimb, această ofertă intră în universul Bitcoin treptat.

Satoshi Nakamoto a conceput inteligent un sistem de recompensare a blocurilor pentru a distribui noul bitcoin fără o autoritate centrală. În primele zile ale Bitcoin, minerii primeau o recompensă generoasă de 50 de bitcoin pentru fiecare bloc minat, motivându-i să investească în echipamente puternice și electricitate.



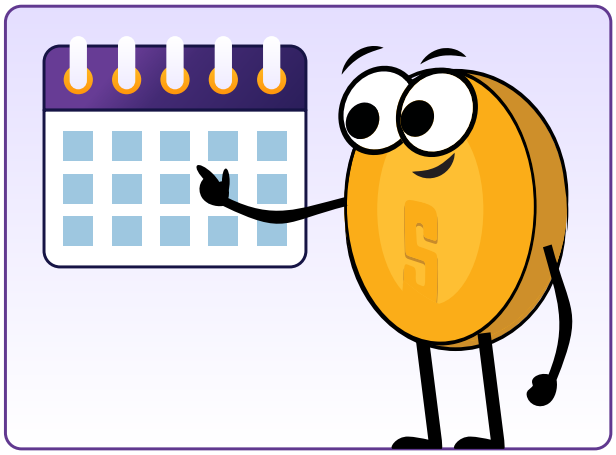
Pentru a menține rețeaua stabilă și a gestiona oferta de bitcoin nou, recompensa de bloc se înjumătățește la aproximativ fiecare 210.000 de blocuri. Acest eveniment, numit „înjumătățirea" (the halving), reduce numărul de bitcoin nou care intră în circulație și continuă să motiveze minerii să protejeze rețeaua și să susțină descentralizarea acesteia. Istoric, evenimentele de înjumătățire au dus la creșteri semnificative ale prețului pe piața Bitcoin datorită reducerii ofertei de bitcoin nou care ajung în circulație.

Capitolul #9

Primul Meu Bitcoin

Oferta în circulație se referă la cantitatea totală a unei monede. În cazul Bitcoin, oferta totală în circulație este numărul de monede care au fost minate și sunt în circulație la un moment dat, excluzând orice monede pierdute pentru totdeauna.

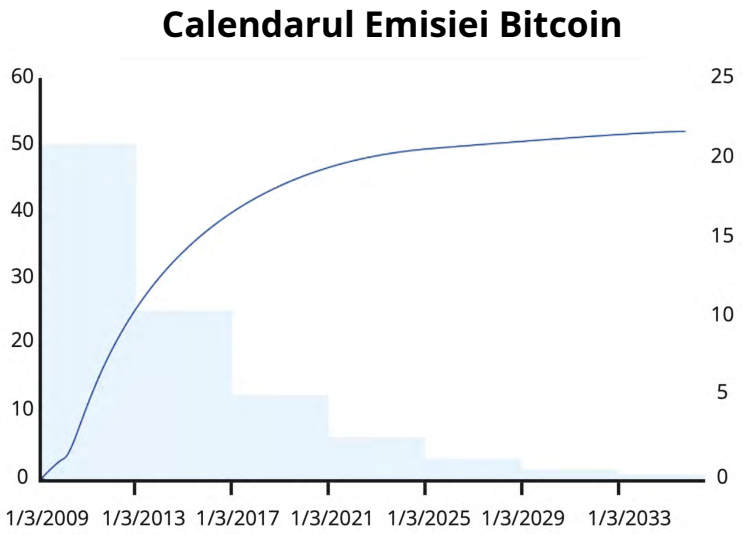
În timpul fiecărui eveniment de înjumătățire, minerii primesc recompense mai mici în bitcoin, ceea ce reduce rata de emitere a noilor monede. Drept urmare, dificultatea de minare a Bitcoin crește pentru a menține un timp de bloc de aproximativ 10 minute, asigurând adăugarea constantă de noi blocuri în blockchain. Reducerea recompenselor de minare nu înseamnă neapărat că minerii obțin profituri mai mici, deoarece pot câștiga și comisioane de tranzacție pentru verificarea tranzacțiilor și adăugarea lor în blockchain, ceea ce poate compensa scăderea recompenselor de minare.



Evenimentele de înjumătățire sunt programate în protocolul Bitcoin, făcând programul de emisie al monedelor bitcoin previzibil și transparent.

Programul de emisie al Bitcoin este planul prestabilit și public pentru eliberarea de bitcoin nou în circulație, conceput pentru a menține raritatea Bitcoin în timp.

Tabelul următor prezintă detaliile viitoarelor evenimente de înjumătățire pentru Bitcoin, inclusiv data estimată a următorului eveniment, numărul blocului la care va avea loc înjumătățirea, recompensa pe bloc în timpul acelui eveniment și procentul din oferta totală care va fi minat.

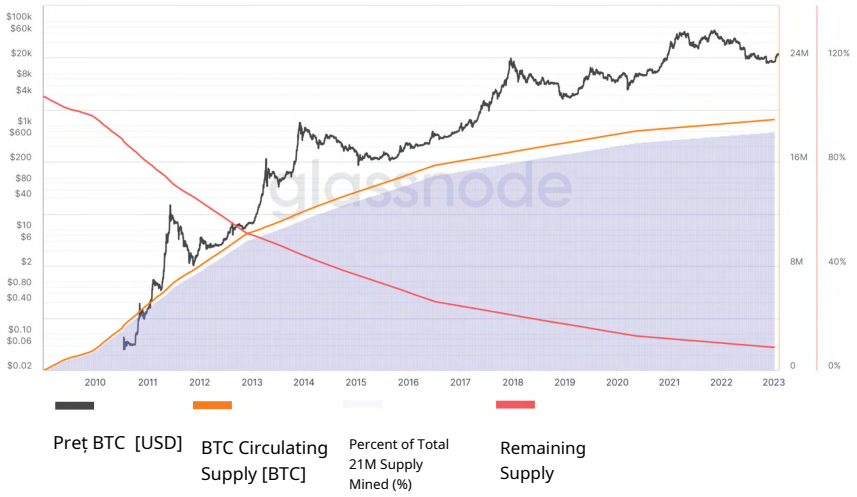


Eveniment	Data Estimată	Bloc	Recompensă Bloc	Procent Minat
A patra înjumătățire	2024	840,000	3.125	96.875 %
A cincea înjumătățire	2028	1,050,000	1.5625	98.4375 %
A șasea înjumătățire	2032	1,260,000	0.78125	99.21875 %

O Introducere în Partea Tehnică a Bitcoin

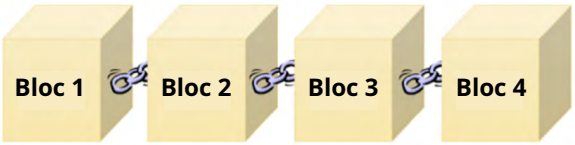
Pe măsură ce mai multe monede bitcoin sunt minate, oferta aflată în circulație și procentul din oferta totală minată vor continua să crească până când se va atinge oferta totală de 21.000.000. Oferta redusă, combinată cu cererea în creștere, poate duce la creșterea prețului Bitcoin (măsurat în dolari). Acest lucru îi avantajează pe cei care au adoptat devreme și îi motivează pe mineri să continue să securizeze rețeaua și să contribuie cu puterea lor de calcul și resurse.

Bitcoin: Procentul din totalul de 21 milioane minate

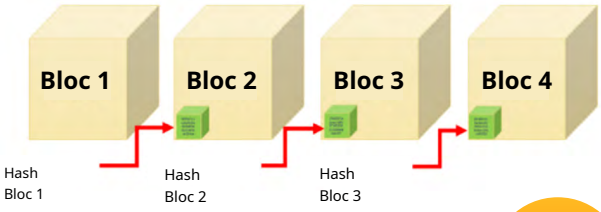


Ce este un hash de bloc valid în Bitcoin?

În Bitcoin, un hash de bloc valid este ca un cod special pe care minerii încearcă să-l găsească. Este un număr unic care ajută la urmărirea fiecărui bloc din blockchain, unde sunt stocate informațiile despre tranzacții. Blocurile se conectează într-un lanț, de la primul (genesis block) până la cel mai recent, creând o evidență publică a tuturor tranzacțiilor. Acest hash de bloc este esențial deoarece leagă fiecare bloc de cel anterior, făcând ușoară verificarea istoricului tranzacțiilor de către oricine. Este ca o amprentă digitală pentru fiecare bloc, asigurând corectitudinea și securitatea informațiilor. Hash-ul blocului acționează ca o modalitate de a confirma că datele din bloc nu au fost modificate.



Blocurile sunt „legate” între ele prin aplicarea unei relații specifice între blocuri. Mai exact, un bloc trebuie să conțină o „amprentă”, care este o valoare hash a datelor din blocul anterior. O funcție hash poate comprima un mesaj arbitrar (informațiile din bloc) într-o dimensiune fixă (de exemplu, 160 biți) și produce o amprentă a mesajului.

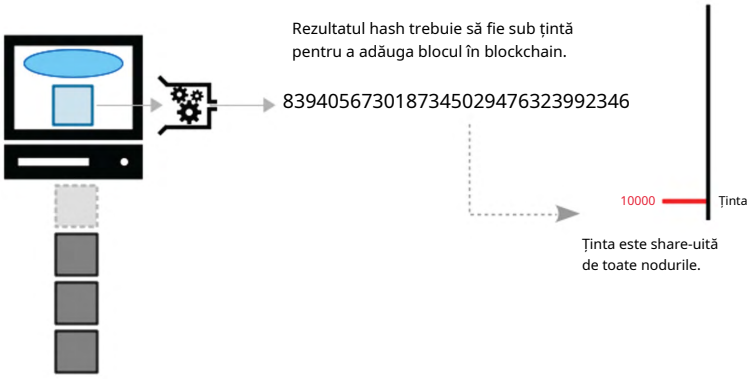


Satoshi Nakamoto, creatorul Bitcoin, a minat blocul inițial, care a conținut un total de 50 de bitcoin.

Cursa pentru minarea unui bloc

Minerii se angajează într-o competiție pentru a descoperi hash-ul de bloc care se aliniază cu ținta (un număr special) stabilită de rețea. Minerul care reușește primul să găsească hash-ul corect primește oportunitatea de a adăuga acel bloc în blockchain și de a-i atribui ID-ul hash corespunzător. Această soluție servește drept validare a autenticității blocului.

Minarea poate fi comparată cu o cursă în care scopul este să ajungi la linia de sosire cât mai repede posibil. Dificultatea de a găsi hash-ul blocului este ajustată periodic, asigurând că fiecare bloc continuă să fie minat la aproximativ 10 minute (pe măsură ce minerii intră și ies din rețea). Acest mecanism se numește „ajustarea dificultății”.



Să presupunem că numărul țintă stabilit de rețeaua Bitcoin este 1.000. Minerii trebuie să folosească puterea lor de calcul și energie pentru a căuta un hash de bloc (un anumit număr) care să fie mai mic decât 1.000. Primul miner care găsește un hash de bloc mai mic decât 1.000 are dreptul să adauge noul bloc la blockchain și este recompensat cu bitcoin.

Nivelul de dificultate în mineritul Bitcoin este o măsură a cât de dificil este să găsești un hash de bloc valid care să respecte ținta stabilită de rețea. Acesta este ajustat la fiecare 2016 blocuri, sau aproximativ la fiecare două săptămâni, pentru a asigura că blocurile sunt adăugate la blockchain la un ritm constant. Nivelul de dificultate este exprimat ca un număr, iar cu cât nivelul de dificultate este mai mare, cu atât este mai greu să găsești un hash valid.

De exemplu, ia în considerare două hash-uri diferite:

Hash 1: 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK
Dificultate: 1

Hash 1: 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK
Dificultate: 2

În acest exemplu, Hash 2 are un nivel de dificultate mai mare decât Hash 1 deoarece este un hash mai lung cu mai mulți de zero la început. Ar fi mai greu pentru mineri să găsească Hash 2 deoarece calculatoarele lor ar trebui să facă mai multă muncă.

Găsind un hash de bloc valid, un miner demonstrează că a efectuat munca necesară pentru a adăuga noul bloc la blockchain și este plătit cu o recompensă în bitcoin, plus comisioane de tranzacție, pentru efortul său. Proof-of-Work (PoW) este metoda pe care rețeaua Bitcoin o folosește pentru a valida tranzacțiile și a adăuga noi blocuri la blockchain.

O Introducere în Partea Tehnică a Bitcoin

PoW menține Bitcoin în siguranță, făcând dificil pentru oricine cu intenții malițioase să preia controlul.

Pe scurt, sarcinile minerilor constau în:

1. **Gruparea tranzacțiilor în blocuri:**

   În timp ce nodurile verifică tranzacțiile nou create care așteaptă în „Mempool”, minerii selectează un subset dintre acestea pentru a le include în blocul lor candidat.

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

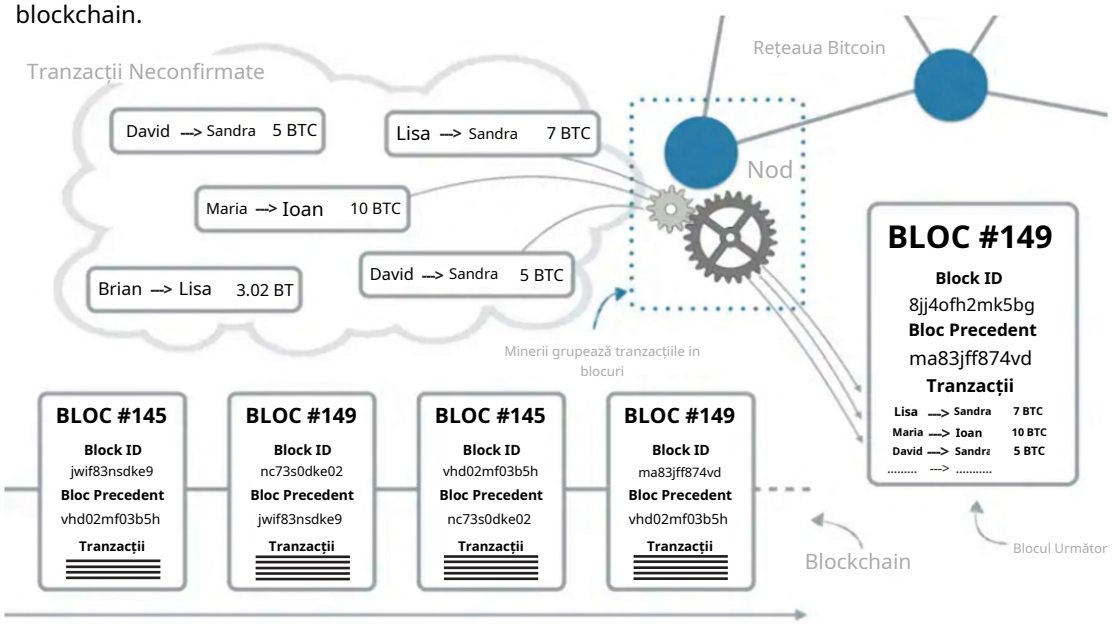
   Minerii concurează între ei pentru a găsi hash-ul de bloc valid.

3. **Transmiterea blocurilor valide:**

   După ce găsesc hash-ul de bloc valid, propagă noul bloc în rețea.

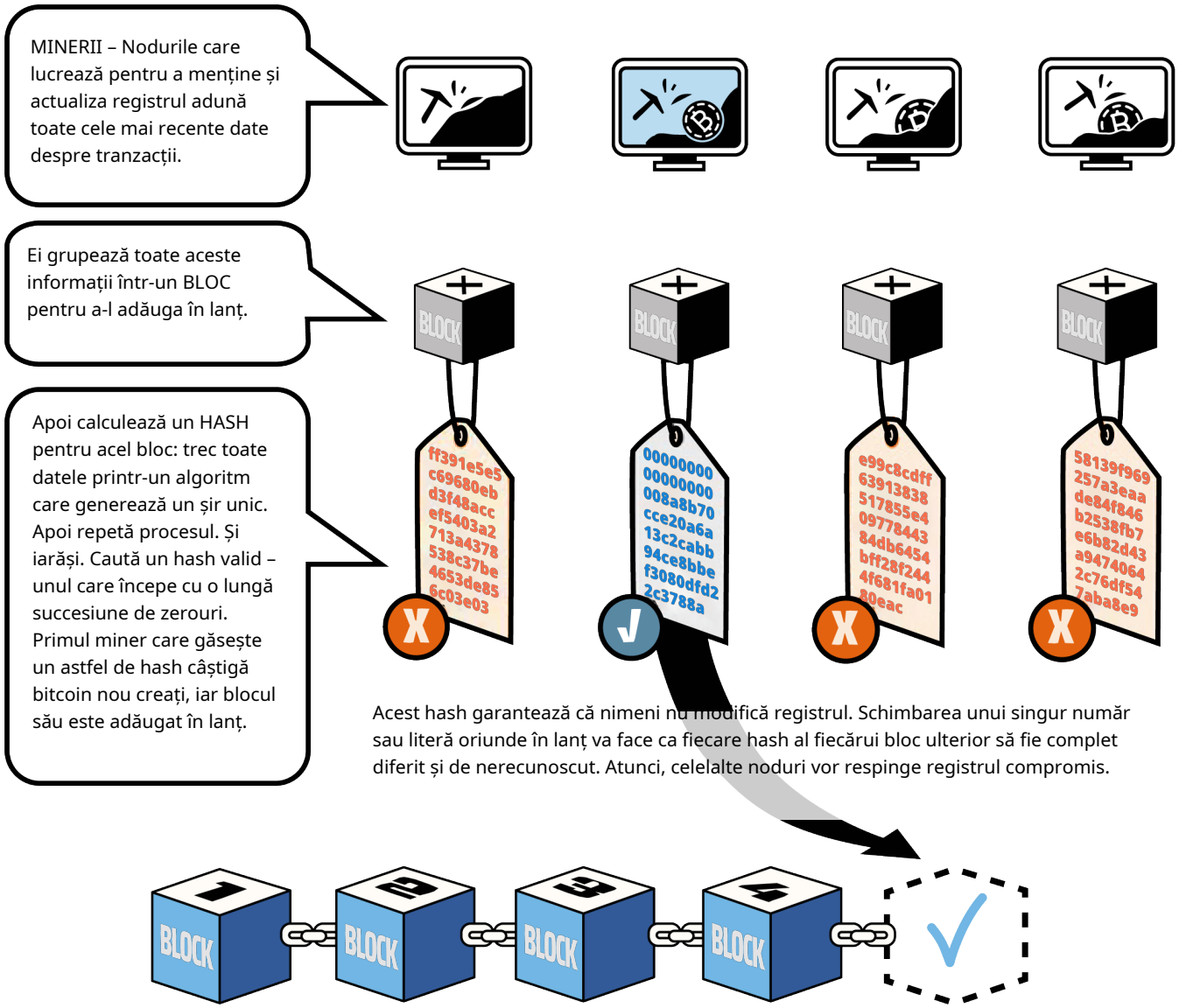
4. **Obținerea recompenselor:**

   În final, primesc bitcoin nou creat și comisioane de tranzacție pentru adăugarea cu succes a blocului la blockchain.



Mai mulți mineri pot lucra simultan la crearea de noi blocuri. Primul miner care descoperă un hash de bloc care respectă ținta stabilită de rețea îl anunță rețelei, iar ceilalți mineri verifică tranzacțiile din blocul candidat al acelui miner pentru a se asigura că sunt valide. Dacă tranzacțiile sunt într-adevăr valide, blocul este adăugat la blockchain. Celelalte blocuri create de ceilalți mineri în acel moment nu sunt adăugate și sunt eliminate. Acest proces ajută la menținerea consensului în rețea și previne cheltuirea dublă.

Un bloc candidat este un set de tranzacții luate în considerare pentru a fi adăugate la blockchain, dar care nu a fost încă adăugat.

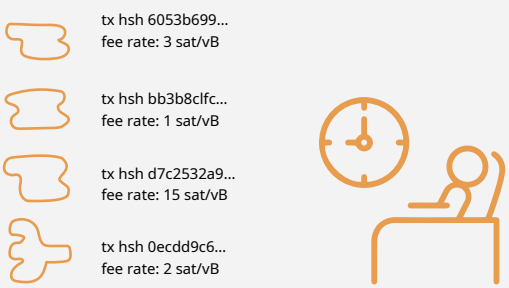


9.4 Ce este Mempool-ul?

„Mempool” sau Memory Pool este ca o sală de așteptare pentru tranzacții. Când faci o tranzacție, aceasta este mai întâi transmisă către Mempool înainte de a fi verificată, selectată și adăugată la blockchain. Imaginează-ți că aștepți la coadă la un restaurant. Numele tău este adăugat pe o listă de persoane care așteaptă o masă. Când o masă devine disponibilă, gazda îți strigă numele și te așază la masă. În mod similar, o tranzacție bitcoin este adăugată în Mempool atunci când este efectuată și este confirmată și adăugată la blockchain atunci când un miner o include într-un bloc.

O Introducere în Partea Tehnică a Bitcoin

Un mempool este locul unde tranzacțiile așteaptă să fie confirmate și incluse într-u



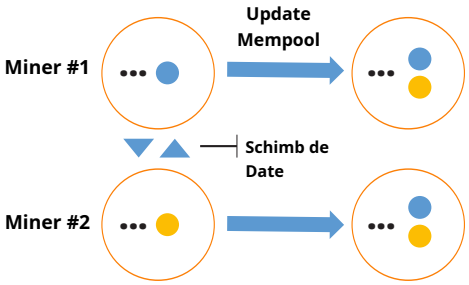
Scopul principal al unui mempool este să:

Transmite tranzacțiile neconfirmate.

Furnizează minerilor tranzacții pentru a le mina.

Când un nod primește pentru prima dată o tranzacție de la un alt nod, trebuie să verifice dacă tranzacția este legitimă. Nimeni nu vrea tranzacții defectuoase

Sincronizarea mempool permite nodurilor să își împărtășească tranzacțiile cu alte noduri prin trimiterea unui mesaj care conține o listă cu tranzacțiile verificate din mempool.



Acceptarea în Memory Pool (ATMP) implică verificarea unor aspecte precum:

- Am deja această tranzacție?
- Există un conflict cu o altă tranzacție din mempool?
- Bitcoin-ul de intrare acoperă bitcoin-ul de ieșire?
- Demonstrează semnăturile că ieșirile anterioare pot fi cheltuite?
- Comisionul este suficient de mare?

Cum sunt verificate și adăugate tranzacțiile în Mempool?

Când noile tranzacții sunt transmise în rețeaua Bitcoin, nodurile verifică aceste tranzacții pentru a se asigura că sunt valide și că fondurile nu au fost cheltuite anterior. Odată ce aceste tranzacții sunt verificate, nodurile le vor adăuga în Mempool-ul lor. Nodurile vor partaja apoi tranzacțiile cu alte noduri pentru a le verifica suplimentar. În final, dacă majoritatea nodurilor sunt de acord, tranzacțiile vor fi puse la dispoziția minerilor pentru a fi selectate și incluse într-un bloc. Totuși, există mai multe motive pentru care o tranzacție ar putea să nu fie confirmată după 72 de ore:

1. **Comisioane de tranzacție mici:**

   Tranzacțiile cu un comision mic pot să nu fie procesate suficient de rapid, deoarece minerii sunt mai predispuși să aleagă tranzacțiile cu comisioane mai mari pentru a le include în blocurile lor.

2. **Congestie în rețea:**

   Dacă rețeaua este congestionată, poate exista o întârziere în confirmarea tranzacțiilor, chiar dacă acestea au un comision mare.

3. **Tentativă de dublă cheltuire:**

   Dacă un actor rău intenționat încearcă să cheltuiască de două ori, tranzacția sa poate fi respinsă de rețea.

4. **Date incorecte sau incomplete:**

   Dacă o tranzacție conține date incorecte sau incomplete, aceasta poate fi respinsă de rețea.

5. **Tranzacție formatată greșit:**

   Dacă o tranzacție este formatată greșit, aceasta poate fi respinsă de rețea.

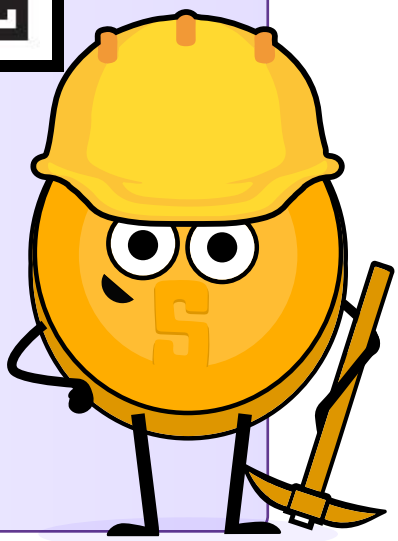
Pentru a evita respingerea tranzacțiilor, este recomandat să includi un comision suficient de mare pentru a te asigura că tranzacția este procesată rapid și să verifici de două ori ca toate datele din tranzacție să fie corecte înainte de a o trimite.

Activitate: Mempool

1. Scanează următorul cod QR:

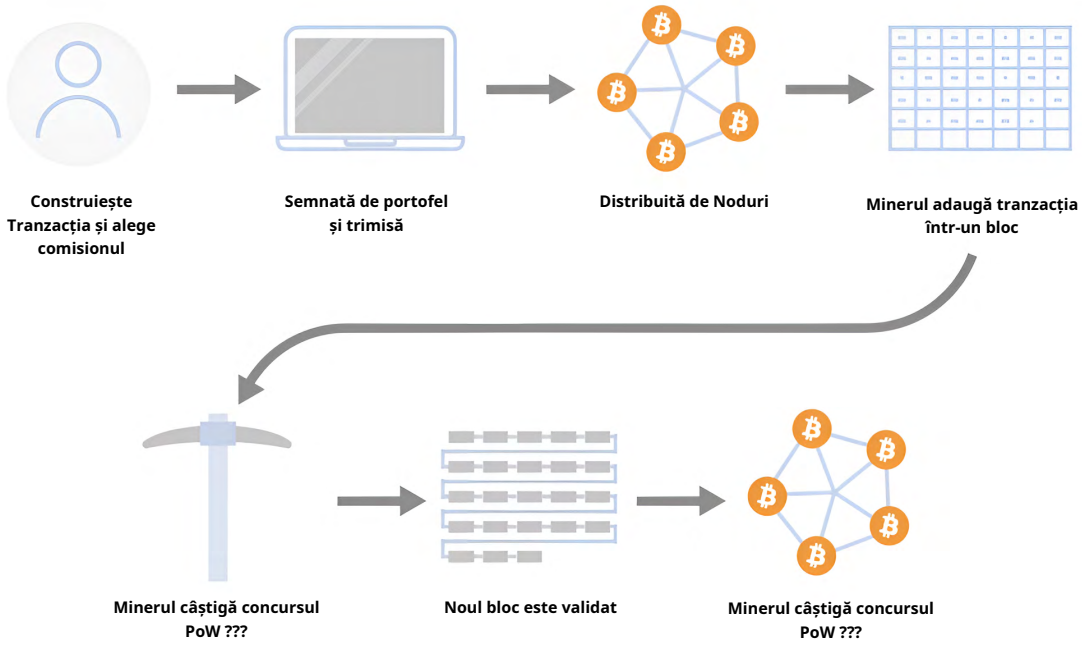
5. Analizează diferitele elemente afișate pe pagină, inclusiv cele mai recente blocuri, tranzacțiile confirmate, numărul de tranzacții, utilizarea memoriei și valoarea aproximativă a întregului bloc. Răspunde la întrebări:

   - Care a fost ultimul bloc minat?
   - Câte tranzacții au fost incluse în acel bloc?
   - Care este valoarea totală tranzacționată în bitcoin?
   - Care a fost dimensiunea în megabytes a blocului?
   - Cu câte zerouri începe nonce-ul blocului?
   - Cât bitcoin a câștigat minerul în total?
   - Care a fost valoarea totală a comisioanelor primite de miner pentru adăugarea tranzacțiilor în rețea?
   - Alege una dintre tranzacțiile cu cea mai mare valoare din bloc. Către câte adrese Bitcoin a fost distribuită suma?



O Introducere în Partea Tehnică a Bitcoin

1. Adam vrea să trimită bitcoin către Gelu. El alege unul dintre UTXO-urile sale, creează o tranzacție și adaugă toate detaliile necesare, inclusiv suma de bitcoin pe care dorește să o trimită, adresa de primire a lui Gelu și un comision de tranzacție peste medie.
2. După o verificare finală pentru a se asigura că toate detaliile sunt corecte, Adam folosește cheia sa privată pentru a semna tranzacția.
3. Adam transmite tranzacția către rețeaua Bitcoin.



Din: 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. Nodurile din rețea primesc tranzacția și îi verifică validitatea conform regulilor de consens (cum ar fi verificarea semnăturii lui Adam și dacă are suficiente fonduri pentru a efectua tranzacția).
5. Tranzacția este marcată ca validă, iar nodurile o propagă către alte noduri din rețea, adăugând-o în Mempool.
6. Deoarece Adam a ales un comision de tranzacție suficient de mare, aproape toți minerii includ tranzacția sa în blocurile lor.

7. Proof-of-Work: Minerii concurează și încearcă să mineze blocul găsind hash-ul valid al blocului. Unul dintre mineri găsește hash-ul și transmite blocul său către rețea.
8. Nodurile primesc noul bloc minat și îi verifică validitatea. Aceasta include validarea tuturor tranzacțiilor din bloc și asigurarea că cerința Proof-of-Work este îndeplinită.
9. Majoritatea nodurilor sunt de acord că blocul este valid și îl adaugă la blockchain. Gelu primește bitcoinul confirmat pe adresa sa de primire.
10. Pe măsură ce blocuri suplimentare sunt adăugate la blockchain în ora următoare, numărul de confirmări pentru tranzacție crește. Pe măsură ce numărul de confirmări crește, Gelu capătă mai multă încredere în succesul și caracterul ireversibil al tranzacției.

Pe scurt, expeditorul semnează tranzacția cu cheia sa privată, nodurile verifică UTXO-urile tranzacției, iar minerii adaugă tranzacția verificată în blockchain. Destinatarul poate apoi accesa monedele bitcoin folosind cheia sa privată. Odată ce un bloc este minat, toate tranzacțiile incluse în acesta sunt considerate confirmate, iar UTXO-urile folosite ca inputuri în aceste tranzacții sunt considerate cheltuite și nu vor mai fi folosite din nou.

Pe măsură ce încheiem acest capitol, ai dobândit informații valoroase despre conceptele fundamentale ale modului în care funcționează Bitcoin. Am acoperit aspecte esențiale, de la bazele banilor până la partea tehnică a tehnologiei Bitcoin. Acum, să legăm totul împreună în următorul capitol. Te așteaptă Capitolul 10, unde vom aprofunda întrebarea semnificativă: „De ce Bitcoin?”

Capitolul 10

De ce Bitcoin?

10.0 Introducere

Activitate: Cum ar putea arăta un viitor cu Bitcoin?

10.1 Ce sunt Monedele Digitale ale Băncilor Centrale (CBDC) și cine le controlează?

10.2 Filosofia Bitcoin

Activitate: Discuție în clasă - Ai dreptul să-ți controlezi propriii bani?

10.3 Beneficiile Bitcoin

10.4 Un viitor împuternicit

Activitate: Discuție finală în clasă - Cum ți s-a schimbat perspectiva?

Caietul elevului

Limba Română | 2025

De ce Bitcoin?

10.0 Introducere

> Bitcoin este mai mult decât o monedă; este o revoluție care redă puterea oamenilor, oferind o doză de pace și libertate într-o lume însetată de autonomie.
>
> **My First Bitcoin**

În acest capitol final, vom rezuma lecțiile învățate de-a lungul călătoriei noastre, vom adresa și discuta câteva întrebări importante și vom explora viitorul Bitcoin.

Bitcoin nu este doar o tehnologie; este un tip de rețea care alimentează o nouă formă de bani a cărei ofertă nu poate fi modificată unilateral de nimeni. Umanitatea nu a avut niciodată o formă de bani cu ofertă fixă și fără control centralizat. Dacă este adoptat pe scară largă, Bitcoin este o unealtă care deschide accesul unei mișcări pentru schimbare pozitivă ce poate transforma viețile oamenilor din întreaga lume. Reprezintă o revoluție pașnică spre libertate și echitate colectivă, deschizând noi oportunități pentru umanitate prin crearea unui sistem monetar global comun.

Ca sistem global descentralizat, Bitcoin permite o mai mare libertate financiară, transferând puterea de la câțiva la mulți. Oferă o platformă sigură, rezistentă la cenzură, pentru stocarea și transferul valorii, împuternicind indivizii să-și controleze averea și să-și protejeze puterea de cumpărare. Acest lucru este deosebit de important în climatul economic incert de astăzi, unde sistemul financiar tradițional se confruntă cu provocări fără precedent.

Activitate: Urmărește videoclipul

Posibilitățile pentru schimbare pozitivă sunt imense, motiv pentru care te invităm să urmărești acest videoclip pentru a afla mai multe.

În continuare, vom analiza o altă formă de monedă digitală numită Monedă Digitală a Băncii Centrale (CBDC - Central Bank Digital Currency) și vom evalua cum sunt similare și diferite față de Bitcoin.

10.1 Ce sunt Monedele Digitale ale Băncilor Centrale (CBDC) și cine le controlează?

Monedele Digitale ale Băncilor Centrale, sau CBDC-urile, sunt versiuni digitale ale banilor fiat obișnuiți. CBDC-urile urmează aceleași reguli ca banii fiat tradiționali, unde o autoritate centrală, precum guvernul, poate crea mai multă ofertă și astfel poate reduce puterea de cumpărare a oamenilor.

Totuși, CBDC-urile oferă guvernelor și instrumente noi și puternice pentru a controla modul în care acești bani sunt folosiți de oameni din întreaga lume.

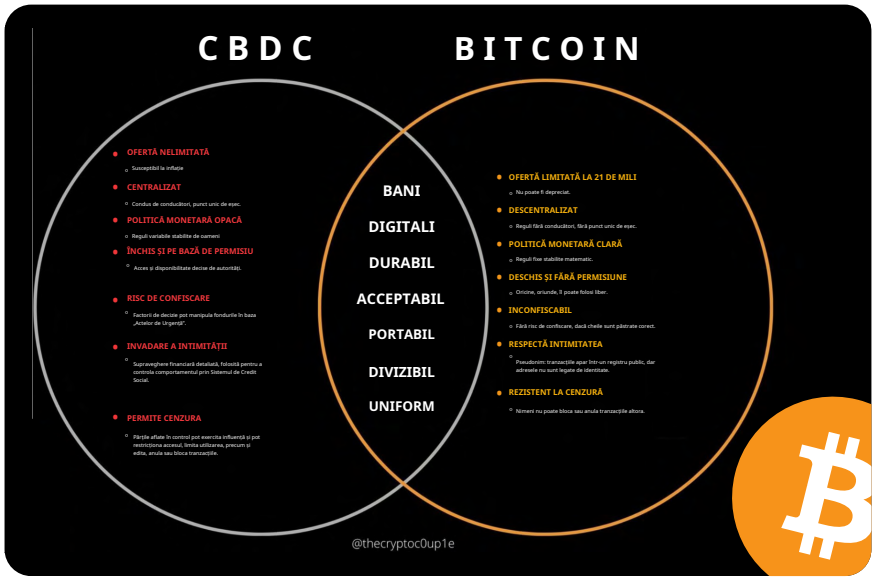
Poți verifica dacă țara ta testează CBDC-uri pe tracker-ul Fundației pentru Drepturile Omului la

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

Așadar, ce face ca CBDC-urile să fie diferite de banii fiat obișnuiți, în afară de faptul că sunt digitali? Este esențial să înțelegem că, spre deosebire de banii fiat sub formă de hârtie sau monede, CBDC-urile permit guvernului să urmărească și să controleze digital fiecare tranzacție la nivel global. Aceasta înseamnă că guvernul poate opri anumite tranzacții sau chiar îți poate îngheța întregul cont dacă nu îi place de tine sau de modul în care îți folosești banii.

De exemplu, imaginează-ți că vrei să trimiți bani unui membru al familiei dintr-o țară care are nevoie de ajutor, dar guvernul tău local îți respinge tranzacția pentru că nu este de acord cu liderii acelei țări. Sau imaginează-ți că mergi la magazin să cumperi ceva ce îți place, dar nu poți pentru că ți-ai exprimat opinia pe rețelele sociale.

CBDC-urile oferă guvernelor putere nelimitată de a controla modul în care banii sunt folosiți la nivel global, limitând capacitatea indivizilor de a cheltui banii după propriile alegeri. Unii chiar susțin că CBDC-urile ar permite guvernelor puternice să impună central politici tiranice la scară globală—prin simpla apăsare a unui buton—fără a mai fi nevoie de agenți umani de aplicare a legii.



Atât CBDC-urile, cât și Bitcoin sunt digitale, dar dincolo de această asemănare, ele reprezintă forme foarte diferite de bani, cu filozofii distincte, conducând la consecințe diverse pentru omenire.

De ce Bitcoin?

10.2 Filosofia Bitcoin

În capitolele 6 și 9, am descoperit că persoanele care rulează un nod ajută la menținerea regulilor Bitcoin în siguranță. Acest lucru este foarte important deoarece, pentru prima dată, oameni ca noi pot face parte dintr-o echipă care se asigură că regulile sistemului nostru monetar sunt protejate. Aceste reguli includ faptul că există doar o cantitate limitată de bani și că nici un participant nu poate schimba unilateral aceste reguli. Este o oportunitate unică pentru oamenii obișnuiți să ajute la păstrarea banilor noștri în siguranță și de încredere.

Filosofia Bitcoin este despre împuternicire, libertate, independență financiară, gândire critică și conceptul că toți ar trebui să avem un cuvânt de spus în regulile sistemului pe care îl alegem pentru noi înșine. Spre deosebire de sistemul fiat controlat de părți centrale puternice, Bitcoin funcționează pe o rețea unde nicio parte nu deține tot controlul. Asta înseamnă că, spre deosebire de alte tipuri de bani precum CBDC-urile, nimeni nu îți poate lua proprietatea sau să te oprească să îți cheltui banii așa cum dorești.

În lumea fiat, a avea mai multă bogăție se traduce direct în mai multă influență și control. În schimb, Bitcoin funcționează într-un mod care pune puterea în mâinile oamenilor. Este ca un efort de echipă unde toți, indiferent de cât de mulți bani au, joacă un rol esențial în sistem. Imaginează-ți o forță colectivă, unde dimensiunea financiară nu înseamnă automat că deții controlul total. Bitcoin este construit pe reguli de neschimbat și, în această armonie, este ca și cum însăși umanitatea controlează sistemul. Nu este vorba de câțiva oameni importanți care iau deciziile, ci de noi toți, ca o comunitate rezistentă, care ghidăm cursul Bitcoin fără ca o singură autoritate să îi spună ce să facă.

În timp ce în sistemul fiat cei puternici dictează regulile, în ecosistemul Bitcoin, forța colectivă a indivizilor susține rețeaua. Nicio entitate, indiferent de bogăție, nu poate dicta drumul ecosistemului Bitcoin. Este o inversare a dinamicii tradiționale de putere, unde reziliența sistemului nu stă în mâinile câtorva, ci în puterea colectivă a fiecărui participant.

Ideea este de a crea un sistem sigur, clar și echitabil, unde toată lumea poate accesa banii globali în mod egal.

Activitate: Discuție în clasă - Ai dreptul să-ți controlezi propriii bani?

1. Sunt banii o necesitate umană și un drept al omului? Și de ce?
2. Dacă nu poți cheltui banii cum vrei, nu îi poți trimite cui vrei sau nu îi poți lua cu tine într-o altă țară, sunt ei cu adevărat ai tăi? Și de ce?
3. De ce a încetat trocul să mai fie folosit? Care este problema cu dubla coincidență a dorințelor?
4. Ce eveniment istoric a avut cel mai mare impact asupra ta? De ce este important să înțelegem șocul Nixon și relevanța lui pentru toată lumea astăzi?
5. Cum este diferită o monedă cu ofertă fixă față de monedele fiat tradiționale?

6. Când a fost creat Bitcoin, de către cine, cu ce scop și cum definește acest scop conceptul de sistem descentralizat?
7. Care este diferența dintre un portofel custodial și unul non-custodial? Care a fost portofelul tău preferat?
8. Ce ai înțeles despre Lightning Network? Pentru ce tip de tranzacții l-ai folosi?
9. De ce susține rularea propriului Node rețeaua?
10. Cum te împuternicește controlul asupra propriilor bani în viața de zi cu zi și în planificarea viitorului?
11. În ce moduri libertatea financiară îți poate îmbunătăți capacitatea de a contribui pozitiv la comunitatea sau societatea ta?

10.3 Beneficiile Bitcoin

„Hiperbitcoinizarea" este un viitor teoretic în care Bitcoin devine sistemul monetar global dominant. Aceasta ar însemna că Bitcoin ar fi folosit de toată lumea, peste tot și pentru orice—de la cumpărarea cafelei la plata facturilor și chiar la achiziționarea de proprietăți.

Interesul tot mai mare pentru Bitcoin din partea indivizilor, companiilor, țărilor și guvernelor evidențiază impactul potențial al adoptării sale pe scară largă asupra economiei și societății. Iată câteva dintre beneficiile unei lumi hiperbitcoinizate:

1. **Un viitor auto-suveran:**

   Un viitor auto-suveran este unul în care oamenii din întreaga lume au control deplin asupra propriei identități digitale și a activelor lor. Acest lucru ar putea duce la o incluziune financiară mai mare, libertate, intimitate și securitate, contribuind astfel la creșterea bunăstării umane, abundenței și fericirii generale.

2. **O rezervă de valoare de încredere:**

   Raritatea digitală a Bitcoin îl face o rezervă de valoare de încredere, ceea ce ar putea încuraja mai mulți oameni să-l folosească ca mijloc de economisire pentru viitor.

3. **Schimbări în politica monetară:**

   Dacă Bitcoin ar fi adoptat pe scară largă, ar putea anula capacitatea guvernelor de a controla oferta de bani prin instrumente tradiționale de politică monetară. Adoptarea în masă a Bitcoin ar putea crește puterea de cumpărare a oamenilor și ar încuraja societatea să se orienteze către activități cu preferință de timp scăzută.

4. **Transparență și trasabilitate sporite:**

   Înregistrarea imuabilă și imposibil de falsificat a tuturor tranzacțiilor pe blockchain ar putea crește transparența și responsabilitatea în diverse industrii și sectoare. În prezent, entități puternice pot muta trilioane de dolari în întreaga lume fără vizibilitate clară asupra destinației sau utilizării acestor fonduri. Oferind o evidență deschisă și verificabilă a tranzacțiilor financiare, Bitcoin ar putea asigura ca mișcarea capitalului să devină mai responsabilă și accesibilă publicului.

5 O revoluție pe piața remitențelor:

Piața remitențelor implică transferul de fonduri de la o parte la alta, adesea peste granițe internaționale. În ciuda scăderii costurilor, remitențele rămân relativ scumpe comparativ cu transferurile bancare interne, mai ales pentru sume mici. Lightning Network oferă tranzacții rapide și cu costuri reduse, fiind potrivită pentru piața remitențelor și abordând costurile ridicate și alte provocări asociate, precum timpul de decontare lent și restricțiile legate de orarul de lucru.

1 Energie abundentă:

Când există multă energie accesibilă, societățile prosperă, iar multe industrii și comunități pot satisface nevoia tot mai mare de energie pentru locuințe, afaceri și tehnologii noi. Mineritul Bitcoin îi motivează pe mineri să folosească surplusul de energie care altfel s-ar irosi, provenit din surse regenerabile precum solar, eolian și hidro. Minerii Bitcoin folosesc acest surplus pentru a crea bitcoin nou prin activități de minare, securizează rețeaua și oferă excesul de energie înapoi rețelei electrice atunci când este nevoie.

10.4 Un viitor afirmat

Bitcoin este bani.

Banii ajută oamenii să comunice care activități, bunuri și servicii sunt cele mai importante în societate. După cum am văzut în acest curs, atunci când banii sunt controlați de autorități centralizate, aceștia vor fi manipulați.

Una dintre greșelile pe care omenirea le repetă de-a lungul istoriei este manipularea banilor, ceea ce afectează negativ indivizii, familiile, afacerile, guvernele și, în cele din urmă, prosperitatea umană globală.

Scoțând controlul banilor din mâinile autorităților centralizate și folosind în schimb bani cu o ofertă fixă pe care nicio parte nu o poate schimba, creăm o lume diferită—una în care nu trebuie să avem încredere că omul va face ceea ce este corect, ci una în care omul nu poate face ceea ce este greșit.

Aceasta este o lume fundamental diferită.

Iar tu, dragă elev, poți face parte din crearea acestei lumi. Folosind Bitcoin, rulând propriul tău nod și ajutându-i pe ceilalți să afle mai multe despre viitorul banilor, votezi pentru o lume diferită.

Activitate: Discuție finală de clasă - Cum ți s-a schimbat perspectiva?

Te rog să răspunzi la cele cinci întrebări de mai jos:

De ce avem nevoie de bani?

Ce sunt banii?

De ce Bitcoin?

Cine controlează banii?

Ce oferă banilor „valoare”?

Capitolul 10

Primul Meu Bitcoin

Notează întrebările puse de studenți care au fost selectate în timpul Capitolului 1 și răspunde-le.

1. **Reveniți la prima activitate din Capitolul 1 și comparați noile răspunsuri cu cele vechi.**
2. **Comparați și discutați răspunsurile și întrebările originale. S-a schimbat ceva?**
3. **Puneți-vă această întrebare finală: Care este următorul meu pas? Și cum pot folosi aceste cunoștințe noi pentru a mă împuternici?**

Dacă ești pregătit să faci pasul următor, consultă resursele suplimentare din secțiunea următoare, unde am selectat cele mai bune materiale pentru învățare și succes pe termen lung.

Resurse Adiționale

1. De ce să folosești Bitcoin?

a "The Bullish Case for Bitcoin" de Vijay Boyapati:

Acest articol argumentează de ce Bitcoin este un activ valoros și de ce are potențialul de a deveni o monedă globală dominantă. Autorul prezintă aspectele tehnice și economice care fac din Bitcoin o oportunitate solidă de investiție.

b "Why Bitcoin Matters" de Aleks Svetski (1 hour):

Acest videoclip explică importanța Bitcoin ca activ digital descentralizat și modul în care poate influența sistemul financiar actual. Vorbitorul analizează potențialul Bitcoin de a aduce libertate financiară oamenilor din întreaga lume.

c "Why Bitcoin" de Wiz:

Acest articol oferă o prezentare a beneficiilor utilizării Bitcoin ca monedă și depozit de valoare. Evidențiază natura descentralizată a Bitcoin și modul în care aceasta asigură o mai mare libertate și siguranță financiară.

2. Ce este Bitcoin?

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

https://www.youtube.com/watch?v=Lx9zgZCMqXE Acest videoclip oferă o explicație detaliată a aspectelor tehnice ale Bitcoin și modul în care funcționează.

b "What Is Bitcoin" de Greg Walker:

Această carte audio explorează contextul economic și istoric care a dus la crearea Bitcoin. Prezintă beneficiile unei monede descentralizate și potențialul Bitcoin de a deveni un standard global.

c "Intro to Bitcoin Austrian Thought" (1 oră

Acest videoclip vorbește despre crearea și primele zile ale Bitcoin. Explorează motivațiile creatorului misterios, Satoshi Nakamoto, și modul în care a evoluat conceptul Bitcoin.

3. Învățare suplimentară:

a "The Bitcoin Standard" (1 oră 40 minute)

Această carte audio explorează contextul economic și istoric care a dus la crearea Bitcoin. Prezintă beneficiile unei monede descentralizate și potențialul Bitcoin de a deveni un standard global.

b "Intro to Bitcoin Austrian Thought" (1 oră)

Această prelegere audio abordează Școala Austriacă de economie și legătura acesteia cu conceptul Bitcoin. Oferă o analiză detaliată a principiilor economice din spatele Bitcoin și modul în care acestea se aliniază cu gândirea austriacă.

c "Bitcoin Babies"

https://learning.chaincode.com/#FOSS Cursuri online și un program de rezidență care permit studenților să învețe abilitățile necesare pentru a lucra la dezvoltarea protocolului Bitcoin.

d BTC Sessions

Un canal YouTube dedicat exclusiv educației despre Bitcoin, cu tutoriale și ghiduri utile: https://www.youtube.com/@BTCSessions

4. Cursuri

a Summer of Bitcoin

https://www.summerofbitcoin.org/ Un program global de internship online de vară, axat pe introducerea studenților universitari în dezvoltarea și designul open-source pentru Bitcoin.

b Chaincode Labs

https://learning.chaincode.com/#FOSS Cursuri online și un program de rezidență care permit studenților să învețe abilitățile necesare pentru a lucra la dezvoltarea protocolului Bitcoin.

c Saylor Academy

Educație gratuită în multiple domenii: https://www.saylor.org/

5. Autori Importanți

- i 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
- i 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. Autori citați

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

b Anil Patel: Twitter: @anilsaidso

7. Alte resurse:

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.

Concepte cheie

Capitolul 1:

Introducere Curs:

Explorează obiectivele și așteptările cursului pentru Diploma Bitcoin.

Activitate de Reflexie – Definirea Banilor:

Participă la un exercițiu reflexiv oferind cinci răspunsuri la întrebări cheie despre bani.

Discuție în Clasă – De ce avem nevoie de bani:

- Participă la o discuție în clasă despre necesitatea banilor.
- Împărtășește și compară perspective individuale despre importanța banilor.
- Pune bazele înțelegerii rolului banilor în sistemele economice.

Capitolul 2:

Înțelegerea Banilor:

- Explorează definiția și conceptul de bani.
- Discută perspectivele diverse din cadrul clasei pentru a înțelege natura complexă a banilor.

Funcții, Proprietăți, și Tipuri:

- Aprofundează funcțiile, proprietățile și tipurile de bani.
- Recunoaște importanța acestor aspecte în definirea și utilizarea banilor.

Psihologia Banilor:

- Înțelege aspectele psihologice ale banilor, inclusiv raritatea, preferința temporală și compromisurile.
- Participă la activitatea "Preferința Temporală" pentru a corela elementele psihologice cu scenarii reale.

Capitolul 3:

Introducere în Istoria și EvoluțiaBanilor:

Explorează istoria și evoluția banilor. Înțelege cum formele antice de schimb au dus la dezvoltarea monedei pe care o folosim astăzi.

Revoluția Monedei Digitale

- Descoperă apogeul actual al evoluției banilor – moneda digitală.
- Înțelege cum există doar în formă electronică, permițând tranzacții instantanee și cu costuri reduse la nivel global.
- Află despre rolul pe care l-a avut Bitcoin în rezolvarea provocărilor monedelor digitale, pregătindu-le pentru utilizare la scară mondială.

Evoluția Monedei:

Explorează tranziția de la formele antice precum scoicile și mărgelele la apariția monedelor și a banilor de hârtie. Urmărește drumul de la hârtie la plastic, descoperind evoluția monedei de-a lungul istoriei.

Jocul Trocului (activitate):

Participă la o experiență practică de joc al trocului pentru a înțelege provocările schimbului direct și a aprecia nevoia unui sistem mai eficient.

Capitolul 4:

Originile Banilor Fiat:

Explorează originile banilor fiat printr-o scurtă prezentare istorică, înțelegând cum au devenit principala formă de monedă.

Băncicu Rezervă Fracționară (activitate):

Participă la activitatea despre Băncile cu Rezervă Fracționară pentru a înțelege modul de funcționare al acestui sistem, evidențiind dependența sa de datorie și implicațiile pentru economia generală.

Sistemul Fiat:

Înțelege aspectele fundamentale ale sistemului fiat, inclusiv natura sa ca sistem monetar prin decret, rolul băncilor cu rezervă fracționară și actorii cheie care controlează acest sistem.

Capitolul 5:

Puterea de cumpărare în scădere:

Înțelege conceptul de inflație monetară și impactul acesteia asupra puterii de cumpărare. Participă la activitatea Efectele Inflației: O Licitație pentru a experimenta efectele direct.

Consecințele sistemului fiat (activitate):

Participă la activitatea Consecințele Sistemului Fiat, care evidențiază repercusiunile mai largi ale cadrului monetar actual.

Monedele digitale ale băncilor centrale

Explorează peisajul în evoluție al Monedelor Digitale ale Băncilor Centrale (CBDC) și potențialul lor impact asupra viitorului banilor.

Povara globală a datoriei

Explorează impactul dublu al poverii globale a datoriei și al inegalității sociale. Recunoaște consecințele individuale și sociale, cu accent pe pierderea puterii de cumpărare și lărgirea decalajului de avere.

Cypherpunks și Decentralizarea:

Află povestea Cypherpunks și motivația lor de a căuta o monedă descentralizată. Diferențiază între sistemele centralizate și descentralizate, obținând perspective dintr-o scurtă istorie a monedelor digitale.

Capitolul 6:

Satoshi Nakamoto și crearea Bitcoin:

Explorează figura misterioasă a lui Satoshi Nakamoto și povestea originii Bitcoin, înțelegând motivațiile inițiale din spatele dezvoltării sale.

Activitate în clasă–Construirea Consensului:

Participă la activitatea Construirea Consensului într-o Rețea Peer-to-Peer pentru a obține perspective practice despre cum se realizează consensul în rețeaua Bitcoin.

Acceptarea Responsabilității Personale:

Evidențiază conceptul de responsabilitate personală în contextul Bitcoin, încurajând înțelegerea rolurilor individuale și a responsabilității în cadrul ecosistemului descentralizat.

Cum funcționează Bitcoin:

O privire asupra mecanismelor Bitcoin, inclusiv Mecanismul de Consens Nakamoto. Identifică actorii cheie din rețeaua Bitcoin, precum mineri, noduri, utilizatori, dezvoltatori și proiecte, și înțelege dinamica colaborativă dintre aceștia.

Bitcoin ca banidigitali sănătoși:

Examinează rolul Bitcoin ca bani digitali sănătoși, discutând evoluția, funcțiile și proprietățile sale și participă la o discuție în clasă dacă Bitcoin se califică drept bani sănătoși.

Concepte cheie

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