

# Diploma Bitcoin

*Finančno izobraževanje za Bitcoinovo dobo*

**Delovni zvezek za učence**

Slovenska različica | 2024

CIP - Kataložni zapis o publikaciji  
Narodna in univerzitetna knjižnica, Ljubljana

336.74:004

DIPLOMA Bitcoin : finančno izobraževanje za  
Bitcoinovo dobo / [prevedel Bitcoin društvo Slovenije]. -  
Šmarje pri Jelšah : B. Filipovac, 2024

Prevod dela: Bitcoin diploma  
ISBN 978-961-96233-3-6  
COBISS.SI-ID 212217091

***Ekipa Moj prvi Bitcoin je ustavila ta dokument  
in ga dala brezplačno na voljo v okviru organizacije  
Creative Commons.***

To delo je licencirano v skladu s

**Creative Commons**

**Attribution-ShareAlike**

**4.0 International (CC BY-SA 4.0)**



# Diploma Bitcoin

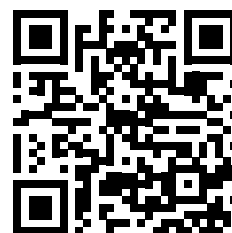
*Finančno izobraževanje za Bitcoinovo dobo*

***Delovni zvezek za učence***

Slovenska različica | 2024



<https://sl.myfirstbitcoin.io/>



## **Diploma Bitcoin**

*Desettedenska pot preobrazbe  
z neodvisnim, nepristranskim,  
kakovostnim in brezplačnim izobraževanjem*

Preden začnete preučevati Bitcoin morate dobro poznati osnove denarja, njegovo zgodovino in sedanji finančni sistem. Poznavanje teh pojmov zagotavlja zanesljive temelje za razumevanje edinstvene in nemirne narave Bitcoina. Skozi izobraževanje o razvoju denarja boste pridobili boljši vpogled v možnosti in omejitve sedanjega finančnega sistema ter kako Bitcoin slednje poskuša odpraviti. Brez tega osnovnega predznanja boste morda težko v celoti razumeli pomen in potencialni vpliv Bitcoina. Zaupajte učnemu procesu in ostanite osredotočeni, saj boste kot nagrado pridobili globlje razumevanje in spoštovanje tega najsodobnejšega področja.



# Povzetek

## Zgodba o Diplomi Bitcoin

Nič ni močnejšega od prave ideje ob pravem času.

Zgodba o Diplomi Bitcoin se je začela v Salvadorju, kjer je junija 2022 diplomiralo 38 učencev javnih šol.

Težko je verjeti, da je od tega šele leto in pol.

Število diplomantov se je v letu 2023 skokovito povečalo, saj je Diploma Bitcoin pridobilo več tisoč učencev iz vse države. Septembra, le 15 mesecev po podelitvi prvih diplom, se je začel še veliko večji pilotni program. Ministrstvo za izobraževanje v Salvadorju je pripravilo lastno Diploma Bitcoin z našim delovnim zvezkom kot temeljnim gradivom. Naši učitelji so skupaj s skupnostjo Bitcoin Beach začeli predavati vsebino Diplome Bitcoin 150 učiteljem javnih šol. Ti učitelji so se nato vrnili v svoje šole in o tem začeli poučevati svoje učence. Letos nameravamo nadaljevati z usposabljanjem dodatnih 700 učiteljev javnih šol po celi državi, upamo pa, da v obdobju dveh let zagotovimo kakovostno izobraževanje na področju bitcoina vsem šolam v Salvadorju.

Eden od naših prvotnih ciljev je bil posredovati znanje narodu in predstaviti, da je izobraževanje o Bitcoinu dobrina za množice. Te sanje se zdaj uresničujejo.

Salvador je v središču dogajanja, preostali svet pa je naše poslanstvo.

Delovni zvezek in številno drugo izobraževalno gradivo je splošno na voljo za javnost in navdušeni smo nad obsegom mednarodnega zanimanja. Leta 2022 so prvič v svetovni zgodovini v javnem šolskem sistemu začeli predavati vsebino Diplome Bitcoin in takoj naslednjega leta smo bili priča skokovitemu porastu. Vsebina diplome je bila prevedena v 12 jezikov in jo zdaj poučujejo v Gvatemali, Hondurasu, ZDA, Kanadi, na Kubi, v Dominikanski republiki, Južni Koreji, Kostariki, Braziliji, Urugvaju, Argentini, Indiji, Italiji, Mehiki, Južni Afriki, Zambiji, Keniji, na Portugalskem, v Združenem kraljestvu in Hongkongu. Tudi za leto 2024 pričakujemo, da bo rast zanimanja, tako kot v letu 2023, zasenčila preteklo leto. Ravno zato se je tudi Bitcoin društvo Slovenije odločilo prevesti Diploma Bitcoin v slovenščino in s finančno pomočjo podjetja NiceHash ter prostovoljci nam je to tudi uspelo.

To je globalno, decentralizirano gibanje.

Neodvisno, nepristransko izobraževanje o Bitcoinu, ki ga vodi skupnost, bo spremenilo svet. Pravzaprav ga je že spremenilo.

**Za boljši svet,**

**– Ekipa Moj prvi Bitcoin & Bitcoin društvo Slovenije  
2024**

# Kazalo vsebine

## 1. poglavje: Zakaj potrebujemo denar?

1.0 Uvod	01
1.1 Spoznajte Satoshija	01
Dejavnost: pet vprašanj o denarju	01
1.2 Razprava v razredu: zakaj potrebujemo denar?	04

## 2. poglavje: Kaj je denar?

2.0 Uvod	07
Dejavnost: razprava v razredu – »Kaj je denar?«	07
2.1 Definicija denarja	07
2.2 Funkcija denarja	09
2.3 Lastnosti denarja	10
2.4 Vrste denarja	13
2.5 Psihologija denarja: Redkost, časovna preferenca in kompromisi	14
Dejavnost: časovna preferenca	16

## 3. poglavje: Zgodovina denarja

3.0 Uvod	21
Dejavnost: Igra blagovne menjave	21
3.1 Razvoj od blagovne menjave do sodobne valute	23
3.1.1 Težave zgodnjimi oblikami denarja	23
3.1.2 Razvoj kovancev in papirnatega denarja	24
3.1.3 Prehod od stabilnega denarja k nestabilnemu denarju	25
3.1.4 Od papirja do plastike	27
3.2 Digitalna valuta	28

## 4. poglavje: Kaj je fiat denar in kdo ga nadzoruje?

4.0 Uvod	31
4.1 Kratka zgodovina fiat denarja	31
4.2 Fiat sistem	34
4.2.1 Denarni sistem z uredbo	34



4.2.2 Bančništvo z delnimi rezervami: sistem, ki temelji na dolgu	35
Dejavnost: Bančništvo s frakcijskimi rezervami	38
4.2.3 Kdo obvladuje fiat sistem in kako pridobi korist od tega?	39
4.3 Centralnibančne digitalne valute: prihodnost fiat denarja	41

## 5. poglavje: Kako težave vodijo do rešitev

5.0 Uvod v težavo	45
5.1 Zmanjševanje kupne moči	45
5.1.1 Denarna inflacija in njen vpliv na kupno moč	45
Dejavnost: učinki inflacije – dražba	46
5.2 Breme globalnega dolga in socialna neenakost	47
5.2.1 Vpliv na posameznike – izguba kupne moči	47
5.2.2 Vpliv na družbo – večanje premoženjske neenakosti	52
Dejavnost: posledice sistema fiat valut	53
5.2.3 Breme globalnega dolga	54
5.3 Cypherpunkovci in iskanje decentralizirane valute	55
5.3.1 Cypherpunkovci	56
5.3.2 Centralizirani in decentralizirani sistemi	57
5.3.3 Kratka zgodovina digitalnih valut	59

## 6. poglavje: Uvod v Bitcoin

6.0 Satoshi Nakamoto in vzpostavitev Bitcoina	63
6.1 Kako deluje Bitcoin?	65
6.1.1 Mehanizem Nakamotovega soglasja	65
6.1.2 Glavni akterji	67
Dejavnost: doseganje soglasja v omrežju enakovrednih udeležencev	69
6.2 Bitcoin kot stabilni digitalni denar	71
6.2.1 Uvod	71
6.2.2 Značilnosti Bitcoina	72
Dejavnost: razprava v razredu – ali je Bitcoin stabilni denar?	76
6.2.3 Sprejemanje osebne odgovornosti	76

## 7. poglavje: Kako uporabljati Bitcoin

7.0 Uvod	81
7.1 Pridobivanje in izmenjava bitcoinov	81
7.1.1 P2P: fizično	81
7.1.2 P2P: spletno	82
7.1.3 Centralizirane borze	82
7.2 Uvod v Bitcoinove denarnice	83
7.2.1 Samoskrbniške in skrbniške denarnice	83
7.2.2 Različne vrste Bitcoinovih denarnic	85
7.3.3 Odprta in zaprta koda	86
Dejavnost: ocenjevanje Bitcoinovih denarnic v razredu	87
7.3 Namestitev mobilne Bitcoinove denarnice	87
Dejavnost: namestitev/obnovitev Bitcoinove denarnice	87
7.4 Prejemanje in pošiljanje transakcij	89
Dejavnost: potek Bitcoinove transakcije	91
7.5 Varčevanje v bitcoinih	93
7.6 DYOR – Ne zaupaj, preveri	94

## 8. poglavje: Kako uporabljati Bitcoin

8.0 Uvod	97
Dejavnost: oglejte si videoposnetek »Bitcoin Lightning Network Explained: How it Actually Works« (Vpogled v Bitcoin Lightning Network: kako dejansko deluje)	98
8.1 Omrežje Lightning Network	100
8.2 Razločne vrste denarnic Lightning	100
8.2.1 Samoskrbniške in skrbniške denarnice	100
8.2.2 Odprta in zaprta koda	100
8.3 Namestitev denarnice Bitcoin Lightning	102
8.4 Pošiljanje in prejemanje transakcij Lightning	106
Dejavnost: štafeta v denarnici Lightning	107
8.5 Nakup kave in živil z bitcoini	
8.5.1 V spletu: vtičniki za plačila – elektronsko poslovanje	108
8.5.2 Osebno: poiščite trgovca v svojem območju	109
8.5.3 Prehodna orodja: darilne kartice in plačilne kartice	110
8.5.4 Krožne ekonomije in Bitcoin kot menjalno sredstvo	110

## 9. poglavje: Uvod v tehnično plat Bitcoin

	115
9.0 Uvod	
Dejavnost: Oglejte si »How Bitcoin Works Under the Hood« (Vpogled v delovanje Bitcoin)	115
9.1 Javni in zasebni ključi: varnost s pomočjo kriptografije	116
9.1.1 Kriptografski javni/zasebni ključi	116
9.1.2 Razlaga zgoščevanja	119
Dejavnost: generiranje zgoščene vrednosti SHA 256	121
9.2 Model UTXO	122
9.3 A Podrobnejši pregled Bitcoinovih vozlišč in rudarjev bitcoinov	125
9.3.1 Kaj je Bitcoinovo vozlišče in kako ga vzpostavite?	125
Dejavnost: oglejte si videoposnetek o Bitcoinovih vozliščih	126
9.3.2 Kaj je rudar bitcoinov in kako deluje rudarjenje?	126
9.4 Kaj je bazen transakcij?	132
Dejavnost: bazen transakcij	134
9.5 Potek Bitcoinovih transakcij od začetka do konca	135

## 10. poglavje: Zakaj Bitcoin?

10.0 Uvod	139
Dejavnost: kakšna je lahko prihodnost Bitcoin?	139
10.1 Kaj so centralnobančne digitalne valute (CBDC) in kdo jih nadzoruje?	140
10.2 Filozofija Bitcoin	141
Dejavnost: razprava v razredu: ali imate pravico do nadzora nad lastnim denarjem?	141
10.3 Prednosti Bitcoin	142
10.4 Opolnomočena prihodnost	143
Dejavnost: razprava v razredu: kako so se spremenili vaši pogledi?	143
Dodatni viri	147
Ključni koncepti poglavij	149
Glosar	153



## 1. poglavje

# ***Zakaj potrebujemo denar?***

1.0 Uvod

1.1 Spoznajte Satoshija

Dejavnost: pet vprašanj o denarju

1.2 Razprava v razredu: zakaj potrebujemo denar?

# Zakaj potrebujemo denar?

## 1.0 Uvod

Denar je eno najboljših orodij za zagotavljanje svobode, kar jih je človek kdaj izumil.

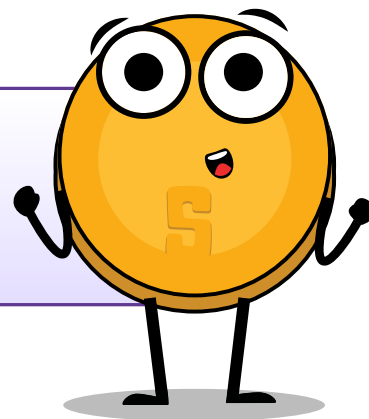
Friedrich Hayek

Dobrodošli v Diplomi Bitcoin. V tem poglavju bomo raziskali temeljno vprašanje, zakaj je denar v našem življenju bistvenega pomena. Ogledali si bomo naravo denarja in njegove različne oblike za boljše razumevanje njegovega pomena. Denar je nekaj, kar uporabljamo skoraj vsak dan, vendar ali dejansko razumemo, zakaj ga potrebujemo in kaj sploh je? Zakaj naši starši in družinski člani zamenjajo svoj čas za denar? Zakaj ga imajo nekateri ljudje več kot drugi? Zakaj je denar v drugih državah drugačen? Zakaj ga ne moremo ustvariti več, ko ga potrebujemo?

## 1.1 Spoznajte Satoshija



Pozdravljeni! Sem Satoshi, interaktivni pomočnik, ki vam bom pomagal skozi celotno Diplom Bitcoin. Zagotovil vam bom vire in uporabna priporočila, da si boste lahko podrobneje ogledali ključne koncepte.



**Dejavnost: začnimo poglavje z odgovori na spodnjih pet vprašanj:**

Razmislite o praktičnih načinih uporabe denarja, na primer o nakupu potrebščin, kot so hrana in želeni predmeti. Poskusite navesti konkretne primere in pri tem uskladiti ustvarjalnost z realnostjo.



## ***Zakaj potrebujemo denar?***

---

---

---

---

---

---

---

## ***Kaj je denar?***

---

---

---

---

---

---

---

# ***Zakaj potrebujemo denar?***

***Kdo nadzoruje denar?***

---

---

---

---

---

---

---

---

***Kaj daje denarju »vrednost«?***

---

---

---

---

---

---

---

---



***Imate kakšno vprašanje o denarju? Zapišite svoje vprašanje in ga izmenjajte z drugimi učenci.***

---

---

---

---

---




---

---

Razširite razpravo po razredu, izmenjajte in primerjajte sezname, da določite pet najpomembnejših razlogov, zakaj potrebujemo denar. Prepoznajte skupne ideje. Razmislite o svojih edinstvenih idejah, ki niso bile uvrščene na seznam, vendar so vredne premisleka. Zapišite ta dodatna spoznanja.

## 1.2 Razprava v razredu: zakaj potrebujemo denar?

Razred razdelite v skupine:

-  Učenci naj izmenjajo odgovore na prva štiri vprašanja in se o njih pogovorijo. Naj si zapišejo najboljše odgovore.
-  Učenci naj izmenjajo odgovore na zadnje vprašanje in glasujejo, katero vprašanje je bilo najbolj priljubljeno. Naj si zapišejo rezultat.
-  Ob zaključku predavanja vsebine Diplome Bitcoin na učenci znova pregledajo svoje odgovore in vprašanja.

Zdaj, ko bolje razumete, zakaj je denar potreben, bomo v naslednjih poglavjih raziskali, kaj je denar, kako se je razvijal skozi čas, kdo vpliva nanj in kakšna je njegova najnovejša oblika. Sklicujte se na sezname, ki ste jih ustvarili prvi dan predavanja, in povežite svoja spoznanja z razvojem ustvarjanja, definiranja in uporabe denarja skozi čas.



## 2. poglavje

# ***Kaj je denar?***

### 2.0 Uvod

Dejavnost: Razprava v razredu – »Kaj je denar?«

### 2.1 Definicija denarja

### 2.2 Funkcija denarja

### 2.3 Lastnosti denarja

### 2.4 Vrste denarja

### 2.5 Psihologija denarja: Redkost, časovne preference, in kompromisi

Dejavnost: Časovna preferenca

# Kaj je denar?

## 2.0 Uvod

Denar je zagotovilo, da bomo v prihodnosti imeli, kar si želimo. Čeprav trenutno ničesar ne potrebujemo, nam zagotavlja možnost, da zadovoljimo novo željo, ko se pojavi.

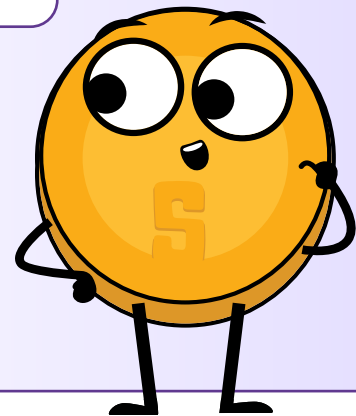
Aristotel

V tem poglavju, ki temelji na naši raziskavi o nujnosti denarja, obravnavamo temeljno vprašanje: Kaj je denar? Začeli bomo s skupinsko razpravo in dejavnostjo.

### Dejavnost: Razprava v razredu – »Kaj je denar?«

- Ne pojejte še bombona, ki je na mizi.
- Kdo bi bil pripravljen svojo sladkarijo zamenjati za bankovec za 1 USD?
- Zdaj pa zadržite roke v zraku, če bi bili še vedno pripravljeni svojo sladkarijo zamenjati za bankovec za 1 dolar igre Monopoli.
- Zakaj ali zakaj ne?
- Zakaj je en bankovec tako zaželen, drugi pa je ničvreden?
- Kaj daje denarju »vrednost«?
- Od kod prihaja denar in kdo odloča, koliko ga je treba natisniti?
- Zakaj ne bi natisnili več denarja in ga enakomerno razdelili med vse?

Edina razlika med tema dvema bankovcema je vaše prepričanje, da ima eden večjo vrednost kot drugi.



## 2.1 Definicija denarja

Ali ste kdaj razmišljali o tem, kaj je pravzaprav denar? Ali ste se kdaj vprašali, kaj je tisto, zaradi česar je denar ... denar? Večina nas ve, kako ga uporabljati, vendar jih le malo razume, od kod izvira in kako deluje. Denar je v bistvu način izmenjave blaga in storitev. Predstavlja vrednost teh predmetov v obliki, s katero je mogoče enostavno trgovati. Ta je lahko v različnih oblikah, kot so papirnati bankovci, kovinski kovanci in elektronska plačila. Vlade ali drugi organi običajno izdajajo in nadzorujejo denar, vendar je denar veliko več kot le fizično ali digitalno sredstvo menjave – je kot univerzalni jezik, ki nam omogoča trgovanje z ljudmi po vsem svetu, tudi če ne govorimo istega jezika ali imamo iste kulture. Lahko ste na primer na drugem koncu sveta in še vedno »govorite« z denarjem. To naredite tako, da izdelek položite na pult in ga zamenjate za lokalno valuto ali uporabite kreditno kartico.

## 2. poglavje

Denar je kot družbena pogodba, ki nam omogoča izmenjavo, ne da bi se morali zanašati na barantanje ali iskanje nekoga, ki bi si posebej želel to, kar nudimo. Če bi skupina ljudi začela sprejemati čokolado kot plačilo za večino blaga in storitev, bi čokolada postala denar (čeprav bi se v nekaterih delih sveta stopila, zato bi jo lahko imeli za slab denar).

Francoski ekonomist Jean-Baptiste Say je poudaril: »Denar ima pri menjavi le trenutno funkcijo. Ko je transakcija zaključena, spoznamo, da je bila ena vrsta blaga zamenjana za drugo.«

Z drugimi besedami, denar sam po sebi nima moči, da bi zadovoljil človekove želje. Je le orodje, ki nam omogoča zamenjavo enega blaga za drugo.



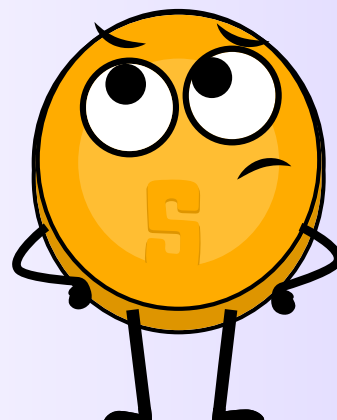
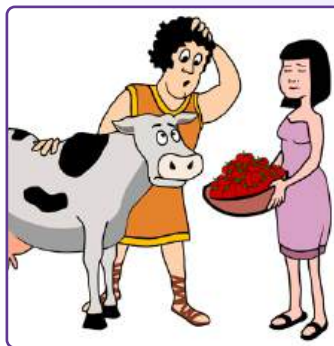
**Transakcija** je izmenjava ali prenos blaga in storitev. Gre za način izmenjave vrednosti med dvema ali več strankami.

Obstaja veliko različnih vrst transakcij, od preprostih izmenjav (kot je nakup sendviča v trgovini) do bolj zapletenih finančnih transakcij (kot je nakup hiše ali vlaganje v delnice ali obveznice). Transakcije lahko potekajo osebno, po telefonu, prek spleta ali na drug način, vanje pa so lahko vključene različne stranke, vključno s posamezniki, podjetji in finančnimi institucijami.

Kako preprosta ali izvedljiva bi bila ta trgovina brez denarja?

Bi zamenjali eno kravo za 1.000.000 jagod?

Ali pa 600.000 jagod? Kaj pa 50.000?



Oglejte si ta kratek videoposnetek!



Denar **JE** vrednost, **PO** kateri se blago izmenjuje.  
Denar **NI** vrednost, **ZA** katero se blago izmenjuje.

### Če povzamemo, denar:

Olajša trgovanje, saj ga vsi sprejemajo kot končno plačilo. Omogoča nam tudi merjenje vrednosti in primerjavo med različnimi dobrinami in storitvami. V nadaljevanju si bomo ogledali funkcijo denarja.

# Kaj je denar?


## 2.2 Funkcija denarja

Pri nakupu in prodaji blaga in storitev je denar ključni dejavnik. Denar ima v svetu več pomembnih funkcij, kot so:



### Hramba vrednost

Denar mora ohraniti svojo vrednost skozi čas, zato je uporaben kot način varčevanja in vlaganja vrednosti človeškega dela. Tako lahko ljudje z denarjem načrtujejo prihodnost ter si ga izposojajo in posojajo. Ko boste naslednjič varčevali za nekaj posebnega, se spomnite, da je denar več kot le sredstvo za plačevanje – je orodje, ki vam pomaga pri načrtovanju in vlaganju v vašo prihodnost.

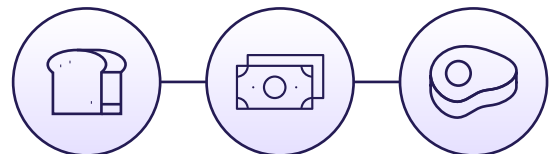
V kakšni obliki hranite svoje premoženje?		 BTC (USD)	 Zlato (USD)	 USD (EUR)
	14. marec 2019	3.846 \$	1.293 \$	0,8817 €
	14. marec 2020	5.258 \$	1.529 \$	0,90056 €
	Dobiček/izguba	+36,71 %	+18,25 %	+2,14 %



### Menjalno sredstvo

Če imate denar, vam ni treba najti nekoga, ki želi točno to, kar imate na voljo za menjavo. Namesto tega lahko z denarjem kupujete in prodajate vse, kar želite. Tako sta trgovanje in poslovanje veliko bolj priročna in učinkovita.

#### Menjalno sredstvo

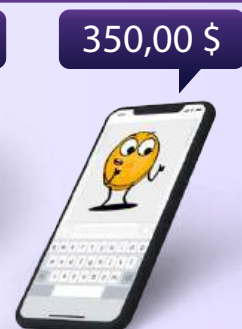
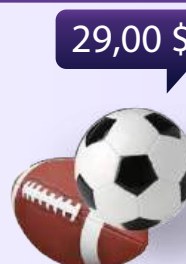
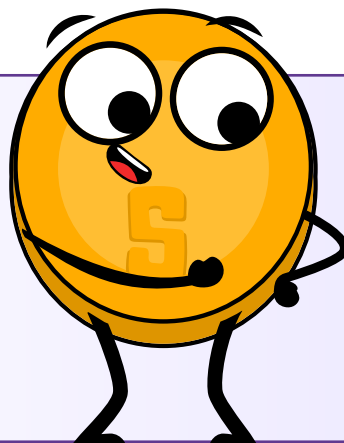


### Obračunska enota

Denar je univerzalni standard vrednosti, ki ljudem omogoča izražanje in primerjavo cen različnih dobrin in storitev. To omogoča bolj učinkovit in pregleden trg, na katerem se lahko ljudje odločajo o nakupu in prodaji na podlagi informacij.

#### Obračunska enota

Potrošniki poznajo vrednost nečesa, ko temu določite ceno (denarno vrednost).



Če bi želeli kupiti nov avto, bi lahko primerjali cene pri različnih prodajalcih in se na podlagi cene v dolarjih informirano odločili, katerega kupiti. Brez obračunske enote bi morali poskušati primerjati vrednost enega avtomobila z drugim na podlagi nečesa drugega, na primer števila krav ali časa, ki je bil potreben za izdelavo avtomobila.

Te tri funkcije omogočajo, da gospodarstva postanejo kompleksna in dinamična. Brez denarja bi bilo veliko težje kupovati in prodajati blago in storitve, naše gospodarstvo pa bi bilo veliko manj razvito.

### Vaja v razredu: Vsakemu primeru pripišite pripadajočo funkcijo denarja?

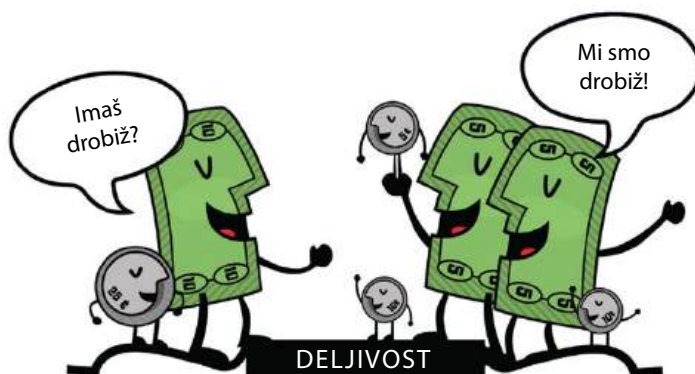
- ☀ Blaž se je odločil, da bo prihranil del svoje tedenske plače in kupil kužka.
- ☀ Anže v piceriji Julči kupi dve rezini pice za 8,30 EUR.
- ☀ Jernej se ne more odločiti, ali naj kupi vstopnice za koncert za 30 EUR ali smučarsko karto za 40 EUR.

## 2.3 Lastnosti denarja

Sčasoma so ljudje spoznali, da mora imeti denar določene lastnosti, da bi bil učinkovit kot menjalno sredstvo. Te lastnosti vključujejo trajnost, deljivost, prenosljivost, sprejemljivost, redkost in zamenljivost.

- ☀ **Trajnost** se nanaša na lastnost denarja, da je odporen na fizično propadanje in se ohranja skozi čas. To zagotavlja, da lahko denar v gospodarstvu kroži v sprejemljivem in prepoznavnem stanju. Zlato je trpežen material, ki je odporen na obrabo, zato dobro ponazarja lastnost trajnosti denarja.

- ☀ **Deljivost** se nanaša na možnost delitve denarja na manjše enote, tako da ga ljudje lahko uporabijo za nakupe v različnih zneskih. Papirnate bankovce je mogoče zlahka razdeliti na manjše vrednosti, zato dobro ponazarjajo značilnost deljivosti denarja.





# Kaj je denar?

☀ **Prenosljivost** se nanaša na to, kako enostavno je denar nositi in prenašati naokoli. To ljudem omogoča, da z denarjem brez težav kupujejo in prodajajo blago in storitve. Kreditne kartice so prenosne, saj jih je mogoče zlahka nositi v denarnici ali torbici, zato dobro ponazarjajo prenosnost denarja.



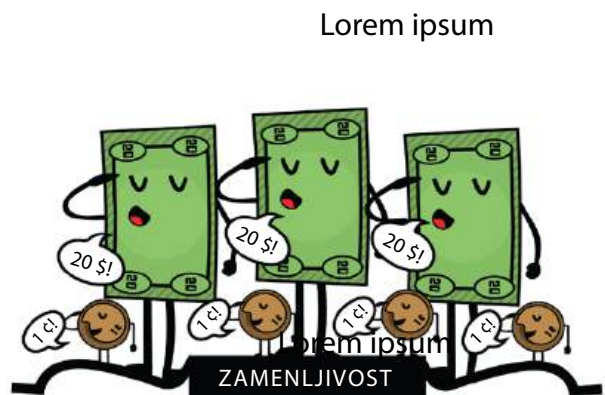
☀ **Sprejemljivost** se nanaša na široko razširjeno sprejetost denarja kot oblike plačila, tako da ga ljudje lahko zanesljivo uporabljajo za nakup in prodajo blaga in storitev. Euro je splošno sprejeto plačilno sredstvo, zato dobro ponazarja značilnost sprejemljivosti denarja.



☀ **Redkost** se nanaša na omejeno ponudbo denarja, kar pripomore k ohranjanju njegove vrednosti in preprečuje, da bi morali za nakup enake količine blaga porabiti več denarja. Zbirateljske znamke, zlasti redke in dragocene, so lahko dobra oblika denarja, saj so redke in lahko sčasoma pridobijo na vrednosti. Zbiratelji znamk pogosto uporabljajo svoje znamke kot način vlaganja premoženja in razpršenosti svojega imetja.



☀ **Zamenljivost** pomeni, da je ena denarna enota enakovredna drugi enoti enake vrednosti. Denar mora biti zamenljiv. Bakreni kovanci so enotne velikosti in teže, zato dobro ponazarjajo zamenljivost, značilno za denar. En cent je vedno en cent.



Lorem ipsum



Zaradi teh značilnosti je denar koristno in učinkovito orodje za pospeševanje trgovine in poslovanja ter je bistvenega pomena za razvoj in stabilnost gospodarstev.

### Vaja v razredu







Različna sredstva imajo različne lastnosti in v različnem obsegu opravljajo funkcije denarja. Družba na koncu določi, katero sredstvo se uporablja kot denar, in sicer na podlagi dejavnikov, kot so stabilnost, redkost, deljivost, prenosljivost in sprejemljivost kot menjalno sredstvo.






Da bi ugotovili, kako dobro različni predmeti ustrezajo posebnim značilnostim denarja, lahko vsako značilnost predmeta ocenite na lestvici od 1 do 5. S seštevanjem točk za vsak predmet lahko ugotovite, kateri je najprimernejši za obliko denarja.

[ 0 = grozno; 3 = dobro; 5 = odlično ]

\* Stolpca za Bitcoin ne izpolnite; k temu se bomo vrnili pozneje v tečaju.

Z naslednjimi vprašanji ugotovite, v kolikšni meri različni elementi v tabeli ustrezajo značilnostim denarja.

-  **Trajnost:** Ali lahko denar sčasoma vzdrži obrabo?
-  **Prenosljivost:** Ali je denar mogoče enostavno prenašati in uporabljati na različnih lokacijah?
-  **Zamenljivost:** Ali je denar zamenljiv z drugimi oblikami denarja?
-  **Sprejemljivost:** Ali je denar splošno sprejet kot oblika plačila?
-  **Redkost:** Ali je denarja malo in ga ni preveč?
-  **Deljivost:** Ali je denar mogoče razdeliti na manjše enote za transakcije?

Značilnosti dobrega denarja	 Krave	 Cigarete	 Diamanti	 Evri	 Bitcoin
Trajnost					
Prenosljivost					
Uniformnost					
Sprejemljivost					
Redkost					
Deljivost					
Skupaj					

# Kaj je denar?

## 2.4 Vrste denarja

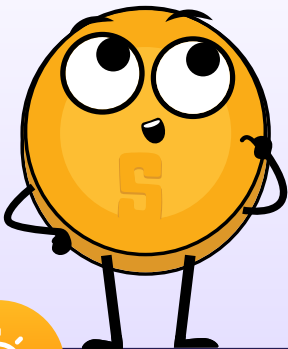
Denar lahko razdelimo v dve glavni kategoriji: fizični in digitalni.

Fizični denar vključuje:

- ✿ Fiatni denar, ki so papirnati bankovci in kovanci, ki jih izdajo vlade in so sprejeti kot menjalno sredstvo.
- ✿ Reprezentativni denar, ki predstavlja terjatev do fizičnega blaga.
- ✿ Naturalni denar, ki je fizični predmet z lastno vrednostjo in je splošno sprejet kot menjalno sredstvo. Na primer zlato in srebro.



Ni ves denar enak!



### Naturalni denar



Predmeti, kot je ta smodnik, so nekoč služili kot naravni denar.

### Reprezentativni denar



Reprezentativni denar, kot je ta srebrni certifikat, je bilo mogoče zamenjati za srebro.

### Fiatni denar



Danes so bankovci centralne banke fiatni denar, ki ga je zvezna vlada razglasila za sprejemljiv način plačevanja dolgov.



**Digitalne valute** se lahko uporabljajo za spletne transakcije in vključujejo elektronske valute, stabilne kovance in kriptovalute.

**Elektronske valute** so digitalne različice običajnega denarja, kot so dolarji ali evri, in se lahko uporabljajo za spletno kupovanje in prodajo prek digitalnih **plačilnih poti**.



Plačilne poti so infrastruktura, ki omogoča pretok elektronskih valut in drugih digitalnih sredstev z enega mesta na drugo. V tradicionalnem finančnem sistemu pa je vedno prisoten posrednik, na primer banka ali finančna institucija, ki zaračuna pristojbino in ima pooblastila za sprejemanje, preklic, vračilo ali odložitev transakcij.

V posredniškem finančnem sistemu so glavne vrste digitalnih plačilnih poti kartična omrežja, ki omogočajo prenos sredstev med finančnimi institucijami in trgovci, ko stranka opravi nakup z debetno ali kreditno kartico, ter digitalne denarnice, ki so spletni računi, ki uporabnikom omogočajo shranjevanje in upravljanje njihovih elektronskih valut ter izvajanje plačil s prenosom sredstev z njihovega računa na račun prejemnika.



### Centralnibančne digitalne valute (CBDC):

Digitalne različice fiatne valute države, ki jih izdaja in podpira centralna banka, posreduje pa vlada.



### Stabilni kriptožetoni

Digitalne valute, ki so zasnovane tako, da ohranjajo stabilno vrednost v primerjavi z nekim sredstvom, kot je ameriški dolar.



### Kriptovalute

Vrsta digitalne valute. Nekatere kriptovalute so decentralizirane in jih urejajo pravila, druge pa so centralizirane in jih nadzoruje majhna skupina ljudi.

Navsezadnje je valuta, ki deluje brez posrednikov, bolj učinkovita in koristna za družbo, saj preprečuje, da bi nekaj posameznikov nadzorovalo ponudbo denarja in koncentriralo svojo moč. Toda vzpostavitev valute, ki bi omogočala varne transakcije, ne da bi se bilo treba pri tem zanašati na zaupanje med strankami, je bila že od nekdaj velik izziv. Da bi to dosegli, je treba ustvariti valuto, ki bo delovala podobno kot internet, kjer je nadzor razdeljen med vse in nikogar hkrati. Za to je potrebno soglasje vseh strani, vključno s tistimi, ki imajo moč, da se odpovedo nadzoru za večje dobro.

## 2.5 Psihologija denarja: Redkost, časovne preference in kompromisi

Predstavljajte si, da ste obtičali v puščavi in vam je ostala le še ena steklenica vode. Ste žejni in si obupno želite piti, vendar veste, da boste vodo potrebovali za preživetje, dokler je ne boste ponovno našli. To je klasičen primer redkosti – vira (vode) je na voljo le omejena količina, zato se morate odločiti, kako ga boste porabili. V tem primeru se lahko odločite, da boste vir porabljali na obroke in ga pili po majhnih požirkih v daljšem časovnem obdobju, da bo trajal čim dlje.



# Kaj je denar?



**Redkost** dobrine nas prisili, da pretehtamo prednosti in slabosti uporabe virov ter sprejemamo kompromise.

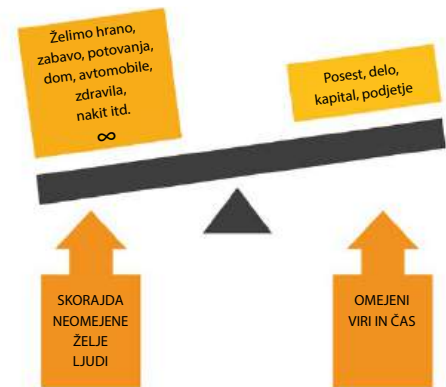
Lahko pa se odločite, da boste naenkrat popili čim več vode v upanju, da vam bo ta naval hidracije dal energijo, ki jo potrebujete za iskanje novih virov vode. Ne glede na to, katero izbiro boste izbrali, boste morali sprejeti težko odločitev. V tem primeru lahko izbirate med takojšnjo potešitvijo žeje in hranjenjem vode za pozneje. Ta koncept redkosti velja za vse vrste virov, ne le za vodo. Naj gre za denar, čas ali celo ljubezen in pozornost, nenehno se soočamo z odločitvami, kako razporediti svoje omejene vire.

Obstajata dve vrsti redkosti: človeško ustvarjena in naravna.

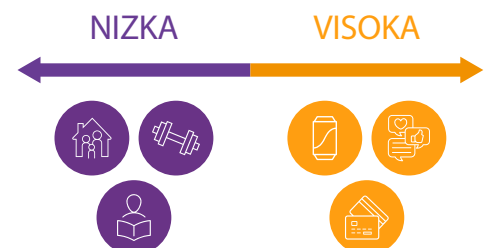
-  Redkost, ki jo je ustvaril človek, znana tudi kot centralizirana redkost, vključuje stvari, kot so omejene izdaje dizajnerskih torbic, redke kartice s podobami športnikov in oštevilčene umetnine. Te je mogoče zlahka kopirati ali ponarediti.
-  Naravna redkost, znana tudi kot decentralizirana redkost, vključuje stvari, kot so sol, školjke in plemenite kovine, kot je zlato. Te je težje posnemati ali ponarejati. Glavna razlika med njima je nadzor.

Centralizirano redkost nadzoruje en subjekt, na primer podjetje ali vlada, medtem ko decentralizirane redkosti ne nadzoruje nihče. Primer centralizirane redkosti, ki nesorazmerno prizadene revne, je nadzor nad osnovnimi viri, kot je čista voda. V nekaterih regijah dostop do čiste vode upravljajo zasebna podjetja ali vladni subjekti, ki lahko omejijo njeno distribucijo, kar vodi v pomanjkanje tega življenjsko pomembnega vira. Ta centraliziran nadzor lahko povzroči zvišanje cen ali neenakopraven dostop do čiste vode, kar pogosto najbolj prizadene revne skupnosti. Omejen dostop do čiste vode ne vpliva le na njihovo zdravje in dobro počutje, ampak tudi ohranja revščino, saj so morda prisiljeni plačevati višje cene za vodo ali prepotovati dolge razdalje, da jo dobijo.

Redkost dobrine vpliva na naše odločitve. Z njenim razumevanjem lahko izboljšamo sprejemanje odločitev. Pogosto moramo izbirati med takojšnjimi koristmi in dolgoročnimi koristmi in te odločitve oblikujejo našo pot do ciljev.



**Časovna preferenca** se nanaša na idejo, da ljudje na splošno raje dobijo nekaj ZDAJ kot pozneje.



Primer časovne preference:

Recimo, da imate možnost prejeti 100 EUR danes ali 110 EUR čez eno leto. Če imate visoko časovno preferenco, se boste morda odločili, da 100 EUR prejmete danes, ker vam je 100 EUR zdaj bolj pomembno kot koristi, ki bi jih imeli, če bi na dodatnih 10 EUR čakali eno leto. Po drugi strani pa, če imate nizko časovno preferenco, boste raje počakali na večjo nagrado, saj ste bolj osredotočeni na dolgoročno načrtovanje in vas manj zanima takojšnje zadoščenje.

### Dejavnost: Časovna preferenca

Visoka časovna preferenca v primerjavi z nizko časovno preferenco

- 1 Poslušajte učiteljevo razlago o izbiri sladkarij.
- 2 Odločite se, ali želite zdaj prejeti majhen bonbon ali čokoladi ali pa počakati do konca pouka in prejeti dva bonbona ali večji, bolj slasten priboljšek.
- 3 Odločite se za eno izbiro in o njej obvestite učitelja. Sladkarije lahko prejmete takoj ali ob koncu pouka, odvisno od vaše odločitve.
- 4 Sodelujte v razredni razpravi o dejavnosti in razmislite o svojem postopku odločanja ter konceptu časovne preference.

### Zaključek in razprava:

- Kateri dejavniki so vplivali na vašo odločitev, ali boste sladkarije vzeli zdaj ali počakali na večjo nagrado pozneje?
- Kaj menite o svoji odločitvi zdaj, ko je dejavnost končana?
- Ali si lahko predstavljate primere iz resničnega življenja, ko bi bila visoka časovna preferenca škodljiva in ko bi bila nizka časovna preferenca koristna?
- Katere so možne posledice izbire visoke časovne preference pred nizko časovno preferenco?

V primeru puščave to pomeni, da boste morda raje takoj popili vso vodo, čeprav to pomeni, da vam je kasneje ne bo več ostalo. To pa zato, ker je žeja, ki jo čutite zdaj, bolj pereča kot morebitna žeja, ki jo boste morda čutili v prihodnosti.

Po drugi strani pa, če se odločite, da boste vodo pili počasi, boste pokazali nižjo časovno preferenco. To pomeni, da ste pripravljeni počakati, da potešite žejo in izboljšate svoje možnosti za preživetje. Koncept oportunitetnih stroškov je tesno povezan z idejo redkosti in časovne preference.

# Kaj je denar?



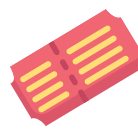
Izraz **oportunitetni stroški** se nanaša na vrednost naslednje najboljše možnosti, ki se ji odpoveste pri sprejemanju odločitve. **Vsaka odločitev vključuje kompromise.**

Današnja izbira



Nakup jagodnega smoothieja za 7 EUR

ZDAJ



Poraba 7 EUR za drug namen

POZNEJE



Prednost rednega varčevanja 7 EUR

V primeru puščave je oportunitetni strošek takojšnje porabe vse vode možnost preživetja, ki bi ga pridobili s tem, da bi vodo razporedili in porabili v daljšem časovnem obdobju.

Recimo, da ste se odločili, da boste vodo pili postopoma in v majhnih požirkih v daljšem časovnem obdobju. Tako imate energijo in hidracijo, ki ju potrebujete za iskanje dodatnih količin vode. Vendar med iskanjem naletite na kaktus, v katerem je majhna količina vode. To ni veliko, vendar je dovolj, da za trenutek potešite žejo. Če bi se odločili popiti vso vodo naenkrat, morda ne bi imeli dovolj energije, da bi poiskali več vode in naleteli na kaktus.

V tem primeru bi bil oportunitetni strošek porabe vse vode naenkrat priložnost, da bi našli kaktus in se dodatno hidrirali.

Ta primer ponazarja, da oportunitetni stroški ne vključujejo le neposrednega kompromisa med dvema možnostma, temveč tudi morebitne prihodnje priložnosti, ki jih lahko pridobimo ali izgubimo zaradi naših odločitev.

Na našo pripravljenost odpovedati se večji nagradi v prihodnosti v zameno za manjšo nagrado zdaj vpliva naša časovna preferenca oziroma to, koliko cenimo takojšnje zadovoljstvo v primerjavi z dolgoročnim načrtovanjem.

V tem poglavju smo se seznanili s temeljnim pojmom denarja, ki zajema njegovo definicijo, funkcije, lastnosti in različne vrste. Bistveni vidik naše razprave je vključeval razumevanje psihologije denarja s poudarkom na konceptih, kot so redkost, časovne preference in kompromisi. To raziskovanje je postavilo temelje za razumevanje zapletene narave denarja in njegove vloge v našem življenju. V naslednjem poglavju bomo govorili o zgodovini denarja in njegovem razvoju skozi čas.







## 3. poglavje

# ***Zgodovina denarja***

### 3.0 Uvod

Dejavnost: Igra blagovne menjave

### 3.1 Razvoj od blagovne menjave do sodobne valute

3.1.1 Težave z zgodnjimi oblikami denarja

3.1.2 Razvoj kovancev in papirnatega denarja

3.1.3 Prehod od stabilnega denarja k nestabilnemu denarju

3.1.4 Od papirja do plastike

### 3.2 Digitalna valuta

Delovni zvezek za učence

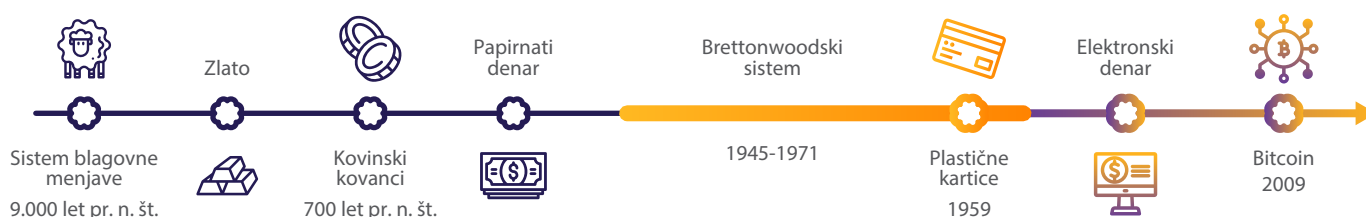
Slovenska različica | 2024

# Zgodovina denarja

## 3.0 Uvod

Denar se ni razvil sam od sebe, ampak je vzniknil na podlagi tržnega procesa. Niso ga ustvarile vlade. V daljšem časovnem obdobju se je spontano pojavil kot ustaljena praksa.

Murray Rothbard



Pred davnimi časi, ko ljudje niso imeli kovancev ali papirnatih bankovcev, ki jih uporabljamo danes. Takrat so imeli edinstven način trgovanja. Kot posebno valuto so uporabljali predmete, kot so školjke, ali plemenite kovine, kot je zlato. Morda se sliši čudno, vendar je bila to njihova različica denarja, nekaj, za kar so se vsi strinjali, da ima vrednost. V tem poglavju se bomo podali na potovanje skozi čas in iz prve roke spoznali razvoj denarja. Sledili bomo njegovim začetkom ter opazovali, kako se je skozi zgodovino spreminjal in prilagajal.

## Dejavnost: Vaja v razredu – igra blagovne menjave

Učitelj vam je dal majhen list papirja. Vaš cilj je, da v igri trgovanja skozi zgodovino zamenjate tisto, kar »imate«, s tistim, kar »želite«. Na vrhu papirja z majhnimi in berljivimi črkami napišite svoje ime.

### 1. krog: Blagovna menjava

Piše se leto 9.000 pr. n. št. Ni treba posebej poudarjati, da denar, kot ga poznamo, še ni bil izumljen. Nahajate se v Mezopotamiji in z blagovno menjavo izmenjujete blago in storitve.

Poleg tega številna podjetja za svoje storitve še vedno sprejemajo nedenarna plačila, ki jih vlade pri davčnem poročanju obravnavajo enako kot valutne transakcije.

List papirja prerežite po črtkani črti. Vaš cilj je, da tisto, kar »imate«, zamenjate tolikokrat, da boste končno dobili tisto, kar ste prvotno »želeli«. Svoje prvotne želje ne morete spremeniti. Za to vajo imate na voljo pet minut.



Ko se to, kar »imate«, ujema s tem, kar ste prvotno »želeli«, se vrnite na svoje mesto. Če po izteku časa ne najdete partnerja za menjavo, se vseeno vrnite na svoj sedež.



Dvignite roko, če ste po eni menjavi dobili, kar ste želeli. Dveh? Treh?

Na naslednja vprašanja odgovorite kratko in jedrnato.

1. Zakaj ste nekateri uspeli dobiti nekoga za menjavo, drugi pa ne?

---



---

2. Kakšne so prednosti blagovne menjave?

---



---

3. Katere so pomanjkljivosti blagovne menjave na podlagi vaših izkušenj s to vajo?

---



---



## 2. krog: Naturalni denar

Pospešeno se odpravite na zahodno obalo Afrike nekje v 14. stoletju pred našim štetjem. Barantanje je postalo utrudljivo in neučinkovito. Kot civilizacija smo se razvili in zdaj uporabljamo naradni denar.

Od lupin školjk kavri do kovancev



1.300 let pr. n. št.



1.000 let pr. n. št.



687 let pr. n. št.

Ti protokovanci so bili ovalne oblike, izdelani iz »elektrona« (zlitine zlata in srebra) in so imeli vzorec samo na eni strani.

### 1.300 PRED NAŠIM ŠTETJEM

V večini Azije, Afrike, Oceanije in nekaterih delih Evrope so lupine polžkov kavri prevladujoča oblika plačila.

### 1.000 PRED NAŠIM ŠTETJEM

Kitajska dinastija Vzhodnega Džova je začela uporabljati kovinske kovance.

### 687 PRED NAŠIM ŠTETJEM

Kralj Aliat iz Lidije (današnja Turčija) je naročil kovanje prvih kovinskih kovancev v zahodnem svetu.



### ZABAVNO DEJSTVO

V nekaterih delih Afrike so bile lupine polžkov kavri vse do 20. stoletja zakonito plačilno sredstvo.

# Zgodovina denarja

Učitelj vam je dal en makaron (zaradi preprostosti vaje). Predpostavimo, da je po dogovoru cena vsake dobrine vredna en makaron.

Vaš cilj je spet dobiti tisto, kar si »želite«, vendar je naša rasa zdaj nekoliko pametnejša in je našla način, kako rešiti določene težave.

- ☀ Zakaj imamo makarone za naravni denar?
- ☀ Kako lahko zdaj dobimo stvari, ki jih želimo?
- ☀ Ali je bila vaja z makaroni lažja?
- ☀ Zakaj menite, da je denar nadomestil blago?
- ☀ V čem je uporaba naravnega denarja učinkovitejša od blagovne menjave?
- ☀ Katere so slabosti uporabe makaronov kot denarja?
- ☀ Kaj mislite, da se je zgodilo, ko je Španija začela v vašo skupnost prinašati polne ladje makaronov (zlato in srebro iz Amerike nazaj v Španijo)?

---

---

---

---

---

## 3.1 Razvoj od blagovne menjave do sodobne valute

### 3.1.1 Težave z zgodnjimi oblikami denarja



Oglejte si kratek videoposnetek o izvoru menjave v seriji »Zgodovina papirnatega denarja«.

V ekonomijah z blagovno menjavo ljudje med seboj trgujejo na podlagi relativne vrednosti blaga in storitev, ki jih ponujajo. Takšne ekonomije so nezanesljive in jih je težko upravljati, zlasti v kompleksnih družbah.

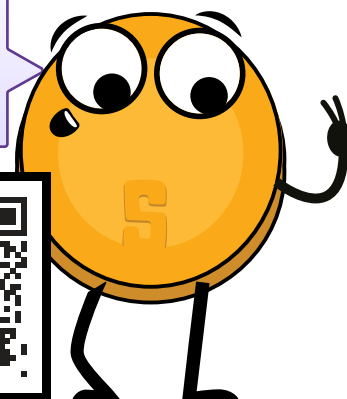
Dvojno sovpadanje želja je potrebno v vsakem sistemu menjave, saj morajo ljudje vedno najti nekoga, ki ima tisto, kar si želijo, in ki hkrati želi v zameno dobiti tisto, kar imajo sami.



Vzemimo za primer:

- ✿ Miha želi zamenjati svojo banano za Tomažev kokos.
- ✿ Toda Tomaž želi svoj kokos zamenjati le za Sandrin mango.
- ✿ Sandra pa želi svoj mango zamenjati le za Mihovo banano.
- ✿ Obtičali so v neskončnem krogu trgovanja s sadjem, ne da bi se dve želji ujemali.
- ✿ Miha predlaga, da svoje sadje zamenjajo za hladno gazirano pijačo, vendar ugotovijo, da so na oddaljenem otoku in da gazirane pijače ni.
- ✿ Odločijo se, da bodo sedeli na plaži in v tišini uživali v sadju.

To je druga epizoda z naslovom »Ne le rezanci« iz serije »Zgodovina papirnatega denarja«.



### 3.1.2 Razvoj kovancev in papirnatega denarja

Ko se znotraj vaše skupnosti vse bolj vključujete v trgovino in poslovanje, spoznate omejitve pri uporabi blagovne in drugih oblik nadenarne menjave. Odločite se, da boste kot denar uporabljali kovinske kovanice.



**Naturalni denar** je denar iz dragocenih kovinskih materialov, kot sta zlato in srebro. V preteklosti so bili uporabljeni kot hranilci vrednosti, menjalno sredstvo in v daljni preteklosti tudi kot obračunska enota.



Zavedate se, da to pomeni veliko spremembo v načinu delovanja denarja. Prehajate iz sistema stabilnega denarja (torej denarja, podprtega s plemenitimi kovinami) v sistem nestabilnega denarja (torej fiatna valuta, ki ni podprta s fizičnim blagom). Ta prehod se ni zgodil čez noč, temveč je bil proces postopen, na katerega je vplivalo več dejavnikov. Industrijska revolucija z množično proizvodnjo in urbanizacijo je odigrala pomembno vlogo, prav tako pa tudi rast naprednih finančnih sistemov, kot so banke in borze. Nastanek centralnih bank in drugih monetarnih organov je prispeval k centralizaciji ali nadzoru denarja, kar je vodilo k izdajanju fiatnih valut, ki so podpirale gospodarsko rast.

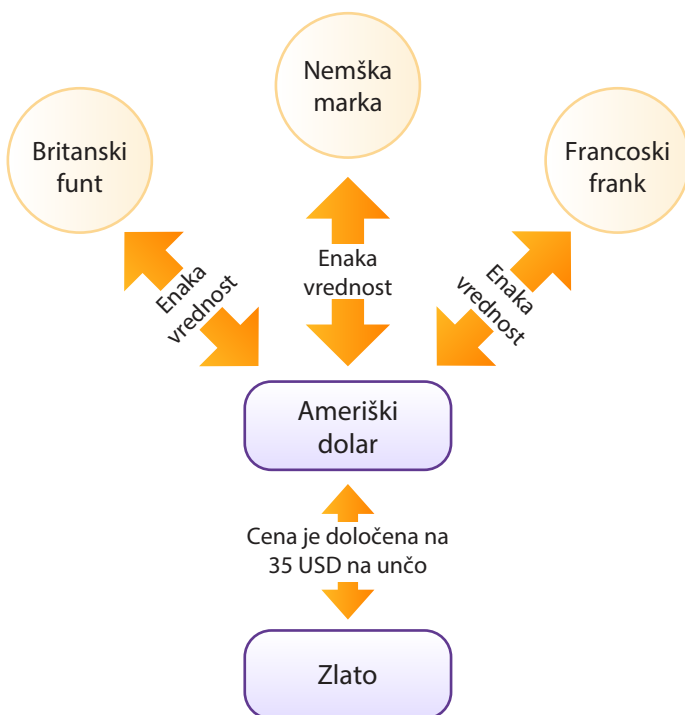


Vendar pa se začnejo pojavljati tudi **slabe strani te centralizacije**, kot so neodgovorna potrošnja, **povečan dolg** in manipuliranje državljanov z ekonomskimi spodbudami.

Do prve svetovne vojne ste lahko papirnati denar zamenjali za vnaprej določeno količino zlata. Vendar sta obe svetovni vojni in gospodarska kriza leta 1929 temu naredili konec. Leta 1944 je bil podpisan Brettonwoodski sporazum, ki je določil ameriški dolar kot svetovno rezervno valuto in vrednost ameriškega dolarja fiksno vezal na ceno zlata po stopnji 35 dolarjev za unčo. Valute drugih držav so vezane na dolar, kar prispeva k stabilizaciji mednarodnih finančnih trgov.

#### Brettonwoodski sistem

(1945-1972)



Žal se je sistem konec šestdesetih let prejšnjega stoletja začel krhati, kar je leta 1971 privedlo do Nixonovega šoka, ko je ameriška vlada ukinila zamenljivost dolarja v zlato. To pomeni konec zlatega standarda in začetek sveta, ki ga poganja ustvarjanje in kopičenje dolga.

V vsakdanjem življenju lahko opazite, da vrednost denarja ni več tako stabilna kot nekoč. Tako kot je z gibkim ravnilom težko natančno izmeriti dolžino mize, je zaradi življenja v fiatnem svetu, v katerem je vrednost denarja odvisna od nepredvidljivosti vladajočih, težko natančno izmeriti vrednost blaga in storitev. Čutite zmedo in nelagodje, ko se prilagajate svetu, v katerem vrednost denarja ni več vezana na fizično blago, kot je zlato.



# Zgodovina denarja

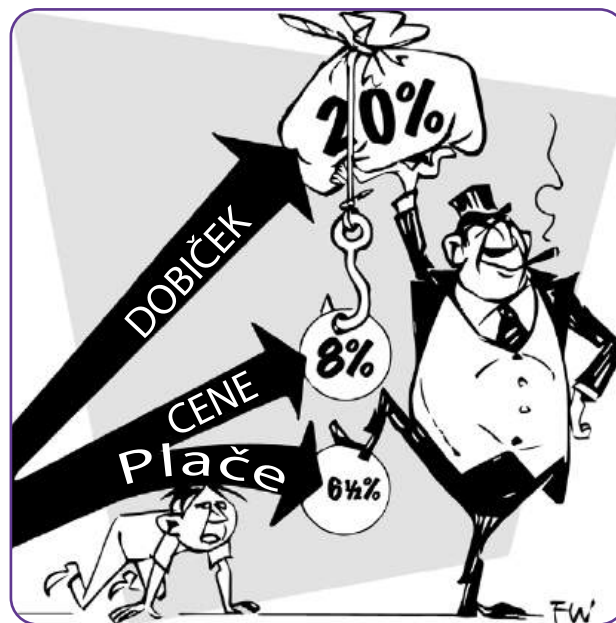
Vidite vplive te spremembe na svetovno gospodarstvo in začnete dvomiti o stabilnosti in zanesljivosti fiatnih valut. Zavedate se, da v sodobnem svetu dolar ni več tako fiksni in dosleden, kot je bil, ko je bil vezan na zlato, ampak je izpostavljen nihanju. Zato je dolar težje uporabljati kot obračunsko enoto, saj na njegovo vrednost vplivajo različni dejavniki, med drugim inflacija (rast cen), obrestne mere, moč gospodarstva države, politični dogodki, tržne špekulacije in povpraševanje v mednarodni trgovini. To je lahko zmeden in nepredvidljiv čas, ko se poskušate orientirati po nenehno spreminjajoči se vrednosti dolarja in njenem vplivu na vaše vsakdanje življenje.

Kljub prizadevanjem za izboljšanje kakovosti življenja s sodobnimi denarnimi sistemi, večjo učinkovitostjo, večjim dostopom do informacij in izboljšano komunikacijo se življenjski standard večine ljudi začne zniževati zaradi:

- ✿ zlorabe centralizacije,
- ✿ naraščajoče cene,
- ✿ stagnacija realnih plač,
- ✿ oslabitev valut,
- ✿ potreba porabiti več denarja za manj stvari.

To predstavlja izziv za osebe z nižjimi ekonomskimi viri, ki imajo lahko omejen dostop do izobraževanja, kreditov, sredstev, družbenih omrežij in političnega zastopstva, kar lahko vodi v zmanjšanje njihovih možnosti za uspeh.

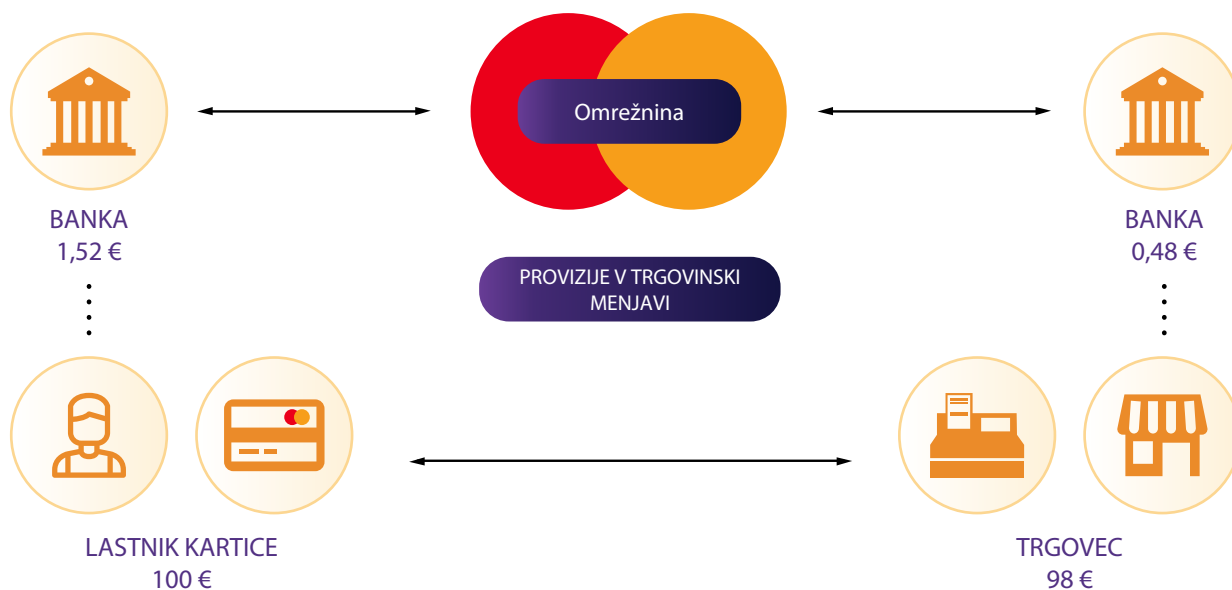
Posledično se zdi, da bogati še naprej bogatijo, revni pa postajajo še bolj revni.



## 3.1.4 Paper to Plastic

Od uvedbe prve kreditne kartice v petdesetih letih prejšnjega stoletja do danes smo prehodili dolgo pot. S tem preprostim plastičnim pripomočkom lahko brez težav kupimo, karkoli želimo, kadarkoli želimo. Kot da bi se odprl svet neskončnih možnosti. Naše navdušenje, ko smo odkrivali vse nove možnosti, je bilo še kako otipljivo ... vsaj tako smo mislili. Nismo pa vedeli, da bo naša odvisnost od kreditov imela boleče posledice, na primer povečanje skupnih stroškov blaga in spodbujanje določenega gospodarstva, ki je obsojeno na propad.





Z razvojem tehnologije se spreminja tudi način ravnanja z denarjem. Internet postaja pomemben dejavnik v finančnem svetu, saj spletno bančništvo in spletne strani za e-trgovanje omogočajo upravljanje in porabo denarja v celoti prek spleta.

Vzpon digitalnega denarja pomeni naslednji pomemben korak v tem razvoju, saj ponuja nove možnosti in spreminja način izvajanja finančnih transakcij.

## 3.2 Digitalna valuta

Za razliko od tradicionalnih valut digitalne valute obstajajo izključno v elektronski obliki. Shranjujejo in izmenjujejo se s pomočjo računalnikov in posebne programske opreme.

Digitalna valuta posameznikom omogoča, da svoj denar pošiljajo prek interneta. Podobno kot elektronska pošta omogoča takojšnje pošiljanje sporočil brez stroškov pošiljanja, nam digitalne valute omogočajo takojšnje pošiljanje in prejemanje vrednosti z zelo majhnimi stroški.

Valute, ki jih uporabljamo danes, postajajo vse bolj digitalne. Le majhen del zaloge denarja obstaja v obliki kovancev in papirnatih bankovcev. Banke in bančne storitve svojim uporabnikom ponujajo aplikacije za nemoteno izmenjavo denarja prek interneta. Toda od kod prihaja denar?

V tem poglavju smo bili priča prehodu od stabilnega denarja, ki ga je predstavljalo zlato, k nestabilnemu denarju v obliki papirne in zdaj digitalne fiatne valute. V naslednjem poglavju bomo raziskali, kako deluje sedanji finančni sistem in kako je nastal.



## 4. poglavje

# ***Kaj je fiatni denar in kdo ga nadzoruje?***

4.0 Uvod

4.1 Kratka zgodovina fiatnega denarja

4.2 Fiatni sistem

4.2.1 Denarni sistem z uredbo

4.2.2 Bančništvo z delnimi rezervami: Sistem, ki temelji na dolgu

Dejavnost: Bančništvo s frakcijskimi rezervami

4.2.3 Kdo obvladuje fiatni sistem in kako pridobi korist od tega?

4.3 Centralnobańčne digitalne valute: Prihodnost fiatnega denarja

Delovni zvezek za uńence

Slovenska razlińica | 2024

# Kaj je fiatni denar in kdo ga nadzoruje?

## 4.0 Uvod

Zgodovina človeštva je zgodovina denarja, ki izgublja vrednost.

Milton Friedman

V prejšnjem poglavju smo videli, kako se je denar razvijal skozi čas in kako je naš denarni sistem prehajal od stabilnega k nestabilnemu denarju, kar je oblikovalo svet, v katerem živimo danes. V tem poglavju bomo bolj podrobno govorili o tem, kako je ta razvoj pripeljal do današnjega fiatnega sistema in kako fiatni sistem deluje.

Kako je torej videti ta fiatni sistem in kako je nastal?

Da bi odgovorili na to vprašanje, se moramo najprej osredotočiti na ameriški dolar, sedanjo svetovno rezervno valuto, ki ima v današnjem svetu prevladujočo vlogo. Vsaka država posredno ali neposredno občuti vpliv odločitev v zvezi z ameriškim dolarjem. Da bi resnično razumeli, kako fiatni sistem deluje v vaši državi, je treba razvozlati zgodovinske niti, ki jo povezujejo z rojstnim mestom fiatnega sistema – Združenimi državami Amerike.

## 4.1 Kratka zgodovina fiatnega denarja

1815-1933	1913	1933	1934	1944	1971	1980
Zlati standard	Ustanovitev centralne banke, imenovane Federal Reserve	Odredba 6102. Vsak državljan je moral svoje zlato oddati po menjalnem tečaju 20,67 USD za unčo	Zakon o zlatih rezervah. Kraja bogastva ljudem z devalvacijo dolarja za 40 % na 35 dolarjev za unčo zlata	Brettonwoodski sporazum: Ameriški dolar je postal prevladujoča svetovna rezervna valuta	Nixonov šok, ki je z ukinitvijo možnosti zamenjave ameriških dolarjev za zlato spodbudil nastanek fiatnega sistema	Vrednost zlata se je povečala s 35 dolarjev za unčo leta 1970 na 870 dolarjev za unčo leta 1980, kar je povzročilo izgubo vrednosti denarja ljudi za 96 % v samo 10 letih

Vizualna časovnica

V 19. stoletju so civilizacije po vsem svetu uspevale na podlagi standarda stabilnega denarja, ki je zaradi redkosti, trajnosti in prepoznavnosti uporabljal plemenite kovine, kot sta zlato in srebro. Z razvojem svetovne trgovine je postalo prenašanje velikih količin kovin izziv, zato so se pojavila skladišča zlata in srebra. Ta skladišča so varno hranila dragocene kovine ljudi in zagotavljala papirnate certifikate, ki jih je bilo mogoče zamenjati za določene količine zlata ali srebra. V zameno za vložek denarja so posamezniki prejeli papirnate certifikate, neposredno vezane na točno določeno količino zlata ali srebra, ki so jo shranili. Ta neposredna povezava



med papirnati certifikati in oprijemljivim naravnim denarjem je zaznamovala zgodnje faze tega, kar danes poznamo kot banke.



Sprva so si banke prizadevale varovati denar strank, pozneje pa so se vključile v tvegane posojilne prakse in izdajale certifikate za zlato, ki ga niso imele. Ta praksa je pomenila nevarnost, da bo prišlo do množičnega izčrpavanja bank, če bi preveč strank hkrati zahtevalo svoj denar. Da bi odpravile tveganje, so banke v sodelovanju z vladami vzpostavile sistem,



ki legalizira nadaljnje kreditiranje. Leta 1913 so ustanovili Federal Reserve, centralno banko, ki je bila odgovorna za ustvarjanje novih papirnih certifikatov in reševanje bank v težavah. Vlade po vsem svetu so priznale vrednost zlata in srebra, kar je privedlo do spopadov in vojn za nadzor. V letih pred drugo svetovno vojno so voditelji, kot so Lenin, Stalin, Churchill, Roosevelt, Mussolini in Hitler, zasegli zlato v strateške namene.

V začetku tridesetih let prejšnjega stoletja se je v Združenih državah Amerike zgodila pomembna sprememba v načinu, kako je bil denar zavarovan s sredstvi. V tistem času je bilo veliko premoženja ljudi shranjenega v zlato. Leta 1933 pa je predsednik Roosevelt izdal odredbo 6102, ki je od vsakega državljana zahteval, da odda svoje zlato. To ni bila prostovoljna izmenjava – ljudje so bili primorani svoje zlato predati in če so to zavrnil, so jih doletele stroge kazni.

Vlada je določila menjalni tečaj 20,67 dolarjev za unčo zlata. To je pomenilo, da je oseba za vsako unčo zlata prejela papirnat certifikat v vrednosti 20,67 dolarjev. Ljudje so morali sprejeti te papirnat dolarje v upanju, da jih bodo nekega dne lahko zamenjali za zlato.

POŠTNI UPRAVITELJ: OBJAVITE NA VIDNEM MESTU. – JAMES A. FARLEY, generalni direktor

**NA PODLAGI IZVRŠILNEGA NALOGA  
PREDSEDNIKA**

izdano 5. aprila 1933

morajo vse osebe dostaviti

**1. MAJA 1933 ALI PREJ**  
vse **ZLATE KOVANKE, ZLATNINO IN  
ZLATE CERTIFIKATE**, ki so zdaj v njihovi lasti,  
na Federal Reserve Bank, podružnico ali agencijo  
katerekoli banke članice ameriške centralne banke.

**Izvršilni nalog**

O PREPOVEDI KOPIRANJA ZLATIH KOVANEC, ZLATNINE  
IN ZLATIH CERTIFIKATOV

Na predlagi predsednika, ki mu jih daje "U. S. Gold" zakon, in dne 6. oktobra 1933, in  
kot je bil sprejet v 2. členu zakona s dne 9. marca 1933, z naslovom "Zakon  
o nadzoru in preprečitvi izdajanja sredstev nacionalne banke v bančništvu in za"

4. Člen. Ob prejemu zlatih kovancev, zlatnine ali zlatih certifikatov,  
ki niso bili dostavljeni v skladu s predpisanim 2 ali 3, bo Federal Reserve Bank  
ali banka članica plačala enakovreden znesek katere koli druge oblike  
kovancev ali vrednosti, ki so jih prejeli v skladu s zakonom 20A.

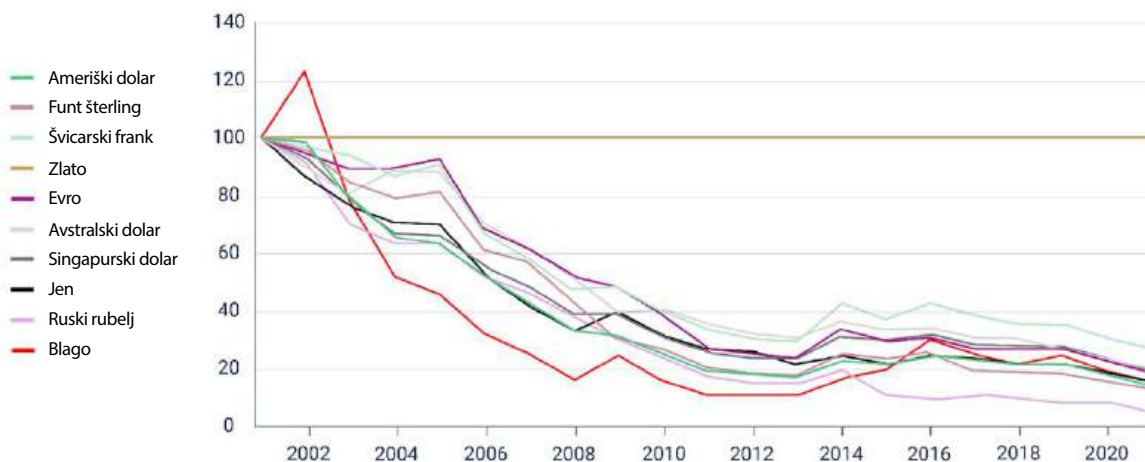
5. Člen. Banka članica izpolnjuje vse zlate kovance, zlatnino in zlate  
certifikate, ki jih prejme v lasti ali jih prejmejo izven tistih, ki so izvedli na podlagi

# Kaj je fiatni denar in kdo ga nadzoruje?

Leta 1934 je Zakon o zlatih rezervah ljudem omogočil, da svoje papirnate dolarje ponovno zamenjajo za zlato. Vendar je bil v tem tudi prikrit namen: vlada je namerno razvrednotila papirnate dolarje, tako da je menjalni tečaj povečala na 35 dolarjev za unčo zlata. Ta devalvacija je prizadela delavce iz nižjega in srednjega razreda, saj je pomenila, da so bili njihovi prihranki, ki so bili nekoč vredni več, zdaj zaradi zmanjšanja vrednosti papirnatih dolarjev vredni manj.

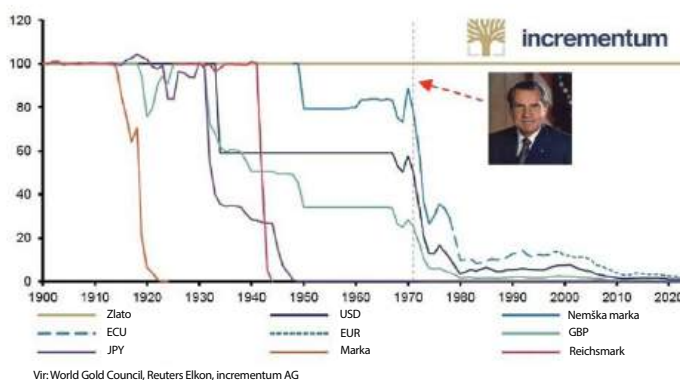
Po drugi svetovni vojni je bil z Brettonwoodskim sporazumom leta 1944 ameriški dolar uveljavljen kot svetovna rezervna valuta, ki jo je bilo mogoče zamenjati za zlato. Toda ta povezava med ameriškim dolarjem in zlatom je bila prekinjena leta 1971, ko je predsednik Nixon ukinil zamenljivost ameriškega dolarja v zlato. To je pomenilo pomemben premik, ki je privedel do sprejetja fiatnega denarnega sistema, v katerem vrednost valute ni podprta s fizičnim blagom, kot je zlato, temveč z zaupanjem in gotovostjo ljudi, ki jo uporabljajo. Ker so vlade in centralne banke zadržale večino zlata ljudi, je vrednost zlata skokovito narasla in leta 1980 dosegla 870 dolarjev za unčo.

Vrednost - unča zlata v dolarjih



Zgodba o tem, kako je človeška družba prešla s standarda stabilnega denarja v nestabilen (fiatni) standard, nam pove, kako so vlade in banke svojim državljanom odvzele plemenite kovine. Medtem ko je pravi denar končal v žepih vlad in bank, so ljudem ostali kosi papirja, katerih edina vrednost izhaja iz vladnih navodil, kako jih uporabljati.

Zlato in različne valute, merjene v zlatu, 1900–2023





## 4.2 Fiatni sistem

Glavna težava običajne valute je zaupanje, ki je potrebno, da valuta deluje. Centralni banki je treba zaupati, da ne bo razvrednotila valute, vendar je zgodovina fiatnih valut polna zlorab tega zaupanja.

Satoshi Nakamoto

Človeštvo je prešlo od stabilnega denarja, ki ga je obvladovalo veliko ljudi, k nestabilnem denarju, ki ga obvladuje peščica. Kako natančno deluje ta sistem?

### 4.2.1 Denarni sistem z uredbo

Za fiatni sistem je značilna njegova obvezna narava, ki jo ljudem nalagajo zakoni o zakonitem plačilnem sredstvu. Izraz »fiatni«, ki izhaja iz latinščine, pomeni »z dekretom« in predstavlja direktivo, ki jo izdajo oblasti.

Za razliko od denarja, ki je podprt z otipljivimi sredstvi, kot je zlato, fiatni denar takšne podpore nima. Njegova uporaba je predpisana z zakonom. Vsakdanje valute, kot so dolarji, evri, funti, juani, pesi in druge, sodijo v kategorijo fiatnega denarja.

Zakon o zakonitem plačilnem sredstvu: zakon, po katerem morajo vsi državljani obvezno sprejemati določeno vrsto valute.



Vrednost denarja temelji na prepričanju, da ga je mogoče zamenjati za blago in storitve, ter na iluziji, da bo ohranil svojo vrednost v daljšem časovnem obdobju. Fiatni denar je primerljiv z vstopnico za koncert: njegova vrednost ni v sami papirnati vstopnici, temveč v zagotovitvi, da bo skupina (vlada in njena centralna banka) izvedla odličen nastop (zagotovila gospodarsko stabilnost).

### Prednosti fiatnega denarja

- ☀ Preprosta uporaba: fiatni denar je priročen za vsakodnevne transakcije.
- ☀ Nižji stroški in tveganja: fiatni denar ne zahteva obsežnega varovanja kot zlato, zato je cenejši in varnejši.

### Pomanjkljivosti fiatnega denarja

- ☀ Nevarnosti inflacije: cene lahko nenehno rastejo, kar povzroča inflacijo in zgodovinske primere hiperinflacije.
- ☀ Centraliziran nadzor in manipulacija: majhne skupine lahko vplivajo na sistem in z njim manipulirajo, kar vodi v cenzuro in zaplenbo.
- ☀ Nevarnosti nasprotne stranke: če se vlada sooča z izzivi, lahko valuta izgubi vrednost.
- ☀ Možnost zlorabe: sistem je mogoče zlorabiti, kar vodi v korupcijo in izgubo zaupanja.

# Kaj je fiatni denar in kdo ga nadzoruje?

## Naturalni denar in fiatni denar: predstavljajte si razliko

Ne pozabite: pred pojavom fiatne valute so vlade kovale kovance iz dragocenega, redkega in težko dostopnega fizičnega materiala, kot sta zlato ali srebro, ali pa so tiskale papirnati denar, ki ga je bilo mogoče zamenjati za določeno količino fizičnega blaga. To je bil sistem, podprt z blagom.

V fiatnem sistemu je to bolj podobno denarju iz igre Monopoli. Denar v fiatnem sistemu sestavljajo kosi papirja, ki jih natisne centralna banka, vladna politika pa neposredno vpliva na njegovo vrednost. Vlada in centralne banke so v bistvu »bankirji v igri Monopoli«, ki nadzorujejo, kako igra deluje, kdo kaj dobi in koliko je to vredno. Z drugimi besedami, vlada obljublja, da bo dobro upravljala denarni sistem.

Če povzamemo, fiatne valute imajo vrednost samo zato, ker vlada predpisuje njihovo uporabo. Fiatni denar sam po sebi nima uporabne vrednosti.

Na kratko je fiatni sistem igra zaupanja, v kateri je vrednost našega denarja odvisna od obljub odgovornih, ljudje pa lahko le upajo, da bo njihova vlada delovala v korist vseh. Nato si bomo ogledali, kako banke ustvarjajo nov denar, kdo pri tem sodeluje in kako to vpliva na gospodarstvo.

## 4.2.2 Bančništvo z delnimi rezervami: sistem, ki temelji na dolgu

Dobro je, da ljudje v državi ne razumejo našega bančnega in monetarnega sistema, kajti če bi ga razumeli, bi po mojem mnenju prišlo do revolucije še pred jutrišnjim jutrom.

Henry Ford

Bančništvo z delnimi rezervami je eden glavnih delov fiatnega sistema, ki bankam omogoča, da posodijo znaten del depozita svojih strank. Ste se kdaj vprašali, zakaj banke svojim strankam ponujajo toliko storitev? Čeprav se morda zdi, da so velikodušne, ne smemo pozabiti, da so banke podjetja in da je njihov glavni cilj ustvarjanje dobička. Toda kako naj ustvarijo dobiček, če ljudem dovolijo, da si izposodijo denar?

Poleg obresti na depozite banke ustvarjajo prihodke tudi na druge načine, med drugim:

- zaračunavanje obresti za posojila, ki jih dajejo,
- zaračunavanje pristojbin za storitve, kot sta uporaba bankomata in vodenje računa,
- zaslužek z naložbami, kot so nakup in prodaja vrednostnih papirjev ali naložbe v nepremičnine,
- hranjenje odstotka posojil v rezervi in vlaganje ali posojanje preostalega,
- plačevanje obresti na bančne vloge in zaračunavanje provizij za tekoče in varčevalne račune.

Ko banka prejme depozit, mora zadržati le del depozita (obvezne rezerve), preostali del pa lahko posodi.





Če na primer položite 100 EUR z obveznimi rezervami v višini 10 %, lahko banka posodi 90 EUR, pri čemer obdrži le 10 EUR kot rezervo. Posojilojemalec položi 90 EUR na drugo banko, s čimer se cikel nadaljuje. Kljub začetnemu plogu 100 EUR se skupni denar v gospodarstvu poveča na 271 EUR, ki se na videz pojavi od nikoder. Ta pojav se imenuje multiplikacijski učinek.

Ta proces vodi v denarni sistem, ki temelji na dolgu, saj banke z vsakim posojilom ustvarijo novo valuto in tako povečajo skupno denarno maso. Ker se bančništvo z delnimi rezervami nadaljuje, se skupni dolg v gospodarstvu povečuje, kar prispeva k inflaciji.

Sistem temelji na neprekinjenem ciklu ustvarjanja valute s posojanjem, ki je podoben stalni oskrbi odvisnika z drogami. Če pa banke posodijo več denarja, kot ga imajo v rezervah, in hočejo vlagatelji hkrati dvigniti vloge, lahko banke propadejo.

V tem primeru centralna banka posreduje kot posojilodajalec v skrajni sili in zagotovi novo valuto, da bi preprečila propad bank. Centralna banka to doseže z odkupom premoženja ali neposrednim vplačilom valute na račune bank. V bistvu so banke rešene pred propadom s stalnim vnašanjem nove valute s strani centralnih bank. Ta sistem, ki ga sistematično rešuje centralna banka in ki temelji na dolgu, povzroča cikle ekonomske rasti in krčenja.

Predstavljajte si, da imate prijatelja, ki je po naključju tudi bančnik, imenujmo ga Darko.

Darko obožuje kolesa in si želi izposoditi tvoje kolo, ker bi rad obiskal veliko krajev. Vi mu posodite svoje kolo, Darko pa na zvit način začne isto kolo obljubljeni številnim drugim prijateljem ob istem času. Z enim resničnim kolesom, ki mu ga posodite, Darko ustvari več namišljenih koles in jih začne posojati prijateljem. Vsi njegovi prijatelji menijo, da lahko uživajo v prijetni vožnji, kadar koli si zaželi. Toda tu je težava – resnično kolo je samo eno! Vsi drugi so namišljeni in le prazne obljube.

Kaj se zgodi? Ko je v prometu več namišljenih koles, so vsi zelo zadovoljni, vsaj na začetku, saj na začetku nihče ne uporablja kolesa v istem trenutku. Zdi se, da ni težav, saj je koles na videz dovolj za vse. Tako vsi prijatelji začnejo načrtovati več stvari in razmišljati o vseh mogočih krajih, kamor se bodo odpravili s kolesi.

Na tem mestu pa se začne čar izgubljati. Nekega sončnega dne se vsi odločijo, da je popoln dan za vožnjo s kolesom. Vsi se pojavijo pred Darkovim pragom, navdušeni, da se bodo lahko zapeljali z navideznimi kolesi. Toda v realnosti je resnično le eno kolo. Sledi razočaranje in vrednost obljubljenih voženj se nenadoma zmanjša.

Podobno je v svetu posojil z delnimi rezervami. Banke posodijo več denarja, kot ga dejansko imajo, in nekaj časa vsi uživajo ugodnosti. V obtoku je več denarja in zdi se, da ga je dovolj. Toda če preveč ljudi hkrati poskuša dvigniti svoj denar, se pokaže prava vrednost: ni ga dovolj, da bi izpolnili vse obljube.

Ta scenarij vpliva na skupno dobro in vrednost vseh vpletenih. Obljuba obilja se spremeni v prevaro. Podobno kot navidezna kolesa izgubijo svojo navidezno vrednost, ko se vsi želijo peljati s pravim kolesom, se lahko vrednost denarja v gospodarstvu zmanjša, ko želijo vsi dobiti svoj delež resničnega denarja. Ko se to zgodi, ljudje ugotovijo, da denar, ki ga imajo v banki, v resnici ni v njej, kar povzroči paniko, obleganje bank in celo propad celotnih gospodarstev. Največje breme teh zlomov sta doslej vedno plačala isti skupini: nižji in srednji razred.

# Kaj je fiatni denar in kdo ga nadzoruje?

Povečanje števila posojil z bančništvom z delnimi rezervami (komercialne banke ustvarjajo fiatno valuto in jo posojajo strankam)



Rast



Povečanje denarne mase (novo ustvarjena valuta vstopi v sistem in napihne denarno maso)



Prevelike naložbe (stranke uporabijo posojila za naložbe v trge, kar povzroči povečanje povpraševanja)



Inflacija cen (rast cen zaradi novega povpraševanja)



Krčenje



Krčenje



Cene padejo (vlagatelji začnejo panično prodajati svoje naložbe po nižjih cenah, saj po njih ni več dejanskega povpraševanja)



Posamezniki in podjetja ne odplačujejo svojih posojil (ker se zmanjša vrednost njihovega zavarovanja)



Banke ne poravnajo svojih obveznosti (ker imajo zdaj v lasti premoženje, ki je manj vredno od vrednosti posojil, ki so jih odobrile)



Intervencija centralne banke, reševanje bank



Reševanje bank z novo valuto (centralna banka odkupi sredstva, ki jih imajo banke, po ceni, ki je višja od trenutne tržne vrednosti, da bi jih rešila, ali pa neposredno ustvari novo valuto in jim jo da)



Ponovitev (naraščanje števila posojil, priprava na naslednjo fazo rasti)

## Dejavnost: Bančništvo z delnimi rezervami

V naslednji vaji bomo raziskali, kako lahko bančništvo z delnimi rezervami vodi do razvrednotenja valute, inflacije in zmanjšanja kupne moči. Uporabili bomo poenostavljen primer, ki vključuje šest udeležencev, od katerih bo eden deloval kot banka, in stopnjo rezerv, ki se še danes pogosto uporablja: 10 %.

- ☀ Oseba A je na loteriji pravkar dobila 100.000 eurov in jih položi v banko (B). Z 10-odstotno stopnjo obveznih rezerv mora B hraniti 10.000 EUR v svojem trezorju, preostalih 90.000 EUR pa lahko posodi.
- ☀ Oseba C si od B izposodi najvišji znesek (90.000 EUR) in ga uporabi za nakup hiše od D.
- ☀ Oseba D položi 90.000 EUR, ki jih je prejela od osebe C, na banko (B). Skupni znesek depozitov v banki zdaj znaša 190.000 EUR.
- ☀ Oseba E pri banki B zaprosi za posojilo in banka ji posodi 90 % novega depozita, ki znaša 81.000 EUR.
- ☀ Oseba E s posojilom v višini 81.000 EUR kupi umetniško delo od osebe F, ki nato denar položi v banko (B). Skupni znesek evidentiranih depozitov zdaj znaša 271.000 EUR.

V tem scenariju je začetni depozit v višini 100.000 EUR po kroženju v gospodarstvu privedel do skupaj 271.000 EUR v depozitih.

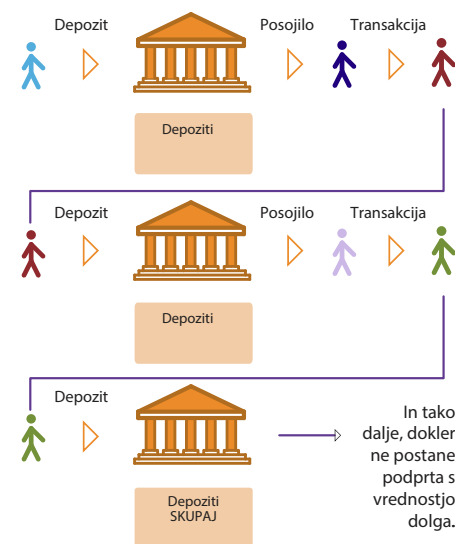
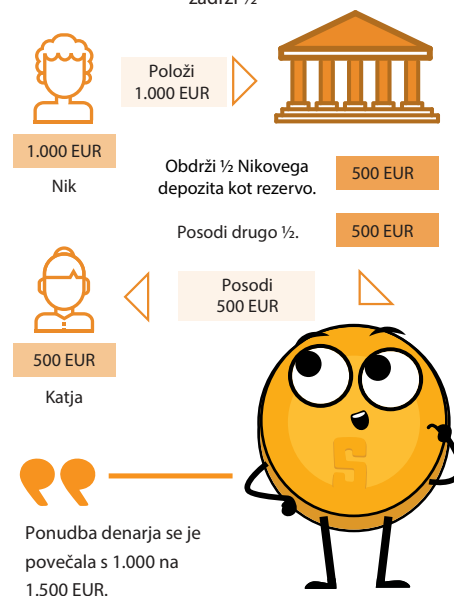
Če bi se stopnja obveznih rezerv znižala na 1 %, bi bil znesek ustvarjenega denarja bistveno večji ( $100.000 \text{ EUR} / 0,01 = 10.000.000 \text{ EUR}$ ). Koliko denarja bi bilo v tem primeru dejansko ustvarjenega s temi 100.000 EUR, če bi denar še naprej krožil po vsem gospodarstvu?

Treba je omeniti, da je Federal Reserve (ameriška centralna banka) z letom 2020 znižala stopnjo obveznih rezerv na nič odstotkov, da bi spodbudila gospodarstvo.

Potrebujemo naslednje prostovoljce:

- A = vlagatelj (dobitnik loterije) (svetlo modra)
- B = bančni blagajnik (banka)
- C = dolžnik št. 1 (temno modra)
- D = lastnik nepremičnine/vlagatelj (rdeča)
- E = dolžnik št. 2 (svetlo vijolična)
- F = lastnik umetniške galerije/vlagatelj (zelena)

Bančništvo z delnimi rezervami  
zadrži ½



# Kaj je fiatni denar in kdo ga nadzoruje?

## 4.2.3 Kdo obvladuje fiatni sistem in kako od tega pridobi korist?

V njem sodelujejo štirje glavni akterji: vlada, premožni posamezniki, finančni sektor in centralna banka. Skupaj nadzorujejo fiatni sistem.

☀️ **Vlada:** vlada je kot režiser fiatne predstave. Poleg pobiranja davkov se financira z novim dolgom, obveznicami, ki jih izdaja državna blagajna. Ko je povpraševanje po teh obveznicah nezadostno, preostali dolg odkupi centralna banka. To pomeni, da lahko še naprej opravlja svoje dejavnosti in uresničuje svoje interese, ne da bi za to potrebovala odobritev ljudi. To je tako, kot da bi dobili kreditno kartico, ne da bi morali dolg nemudoma odplačati. To se morda zdi dobro za vlado, vendar je to drago za vse ostale.

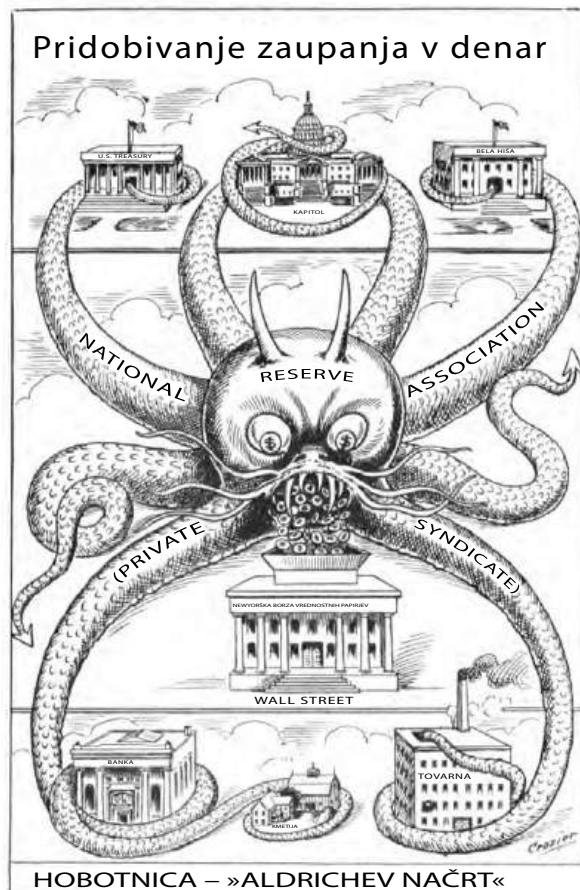
☀️ **Premožni posamezniki:** premožni posamezniki imajo od fiatnega sistema veliko koristi. Z možnostjo kopičenja dolga lahko vlagajo v sredstva, kot so blago, nepremičnine in delnice, ter tako skoraj brez težav ustvarjajo novo bogastvo.

☀️ **Finančni sektor (banke):** banke in druge finančne ustanove ne nadzorujejo neposredno finančnega sistema, imajo pa od njega veliko koristi. Brez odgovornosti lahko zasledujejo in pospešujejo ustvarjanje nove valute s posojili z delnimi rezervami, pri čemer imajo koristi od višjih prihodkov. Za banke to praktično nima posledic, saj je za njihovo reševanje uporabljena nova fiatna valuta, s katero je prepečen propad celotnega sistema.

☀️ **Centralna banka:** centralna banka je tista, ki vleče niti in domnevno nadzoruje rast denarne mase. Toda ravno v tem je trik – tudi za centralno banko veljajo vladni zakoni, ki služijo vladnim interesom. To je kot lutka, ki ga nadzoruje drug lutka. Morda se zdi, da je centralna banka tista, ki je odgovorna, vendar posredno izpolnjuje vladne želje, da natisne denar iz zraka, ko ga ta potrebuje.

Kako pridobivajo koristi: te skupine se okoriščajo na različne načine, ob tem pa ustvarjajo zapleteno mrežo nadzora. Vlada dobi sredstva brez neposrednih posledic, premožni posamezniki in banke brez težav zaslužijo denar, centralna banka pa skrbi, da se predstava nemoteno odvija naprej. Medtem lahko ostali prebivalci občutijo posledice in se soočajo z izzivi, ki jih prinaša tako delovanje sistema.

Na koncu lutkarji finančnega sistema ustvarijo predstavo, v kateri imajo nekateri veliko koristi, mnogi pa se sprašujejo o pravičnosti finančnega odra, na katerem so se znašli.



### Vloga centralnih bank

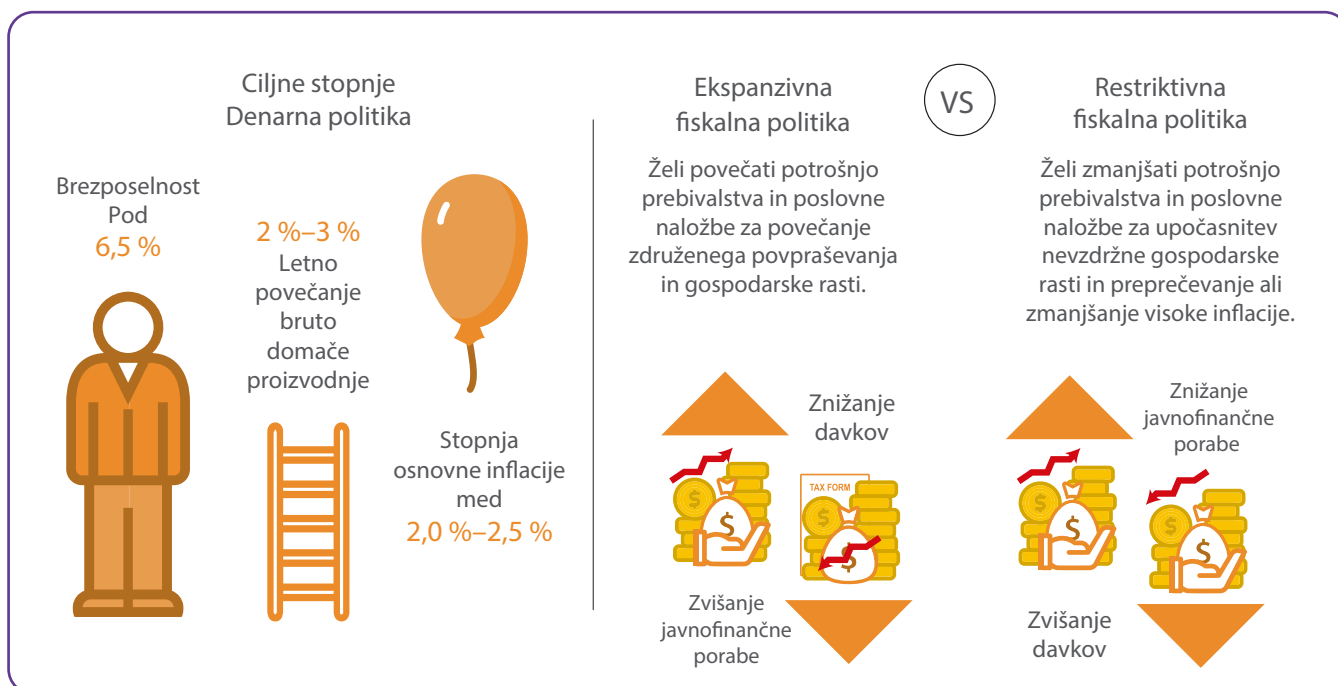
Centralne banke tiho oblikujejo delovanje gospodarstva. Njihova uradna naloga je zagotavljati stabilnost, integriteto in »ohranjati stvari stabilne«, vendar njihove metode razkrivajo bolj skrivnostno plat.

Centralne banke tesno sodelujejo z vladami in vlečejo niti denarne politike ter z orodji, kot so obrestne mere, nadzorujejo ponudbo denarja. V času krize tako rekoč iz nič natisnejo denar in ga prek komercialnih bank vložijo v gospodarstvo, da se zdi, da je vse v redu.

Ne samo, da centralne banke nadzorujejo stvari, ampak tudi regulirajo komercialne banke, določajo pravila igre in priskočijo na pomoč, ko se banke znajdejo v težavah (delujejo kot posojilodajalci v skrajni sili). Čeprav je videti, kot da je namen te mreže za nadzor zaščita, povzroča še večjo odvisnost gospodarstva in bank od njih.

Za razumevanje širšega finančnega sistema je ključno razumeti, od kod prihajajo bilijoni dolarjev finančnih spodbud in kdo odloča o njihovi dodelitvi. Vlade uporabljajo več orodij za upravljanje denarne mase v določenih časovnih obdobjih.

Centralne banke in vlade lahko z orodji denarne in fiskalne politike vplivajo na denarno maso in gospodarstvo. Ameriška centralna banka (Federal reserve) na primer z denarno politiko prilagaja obrestne mere in s tem vpliva na količino denarja v obtoku. Fiskalna politika po drugi strani vključuje uporabo politik porabe in davkov za vplivanje na gospodarsko dejavnost.



# Kaj je fiatni denar in kdo ga nadzoruje?

Politike deviznih tečajev, ponudbeni šoki in nadzor cen so dodatna orodja za uravnavanje denarne mase ter vplivajo na trgovino in gospodarstvo. Cilj teh politik je stabilizirati cene in nadzorovati inflacijo, vendar intervencije pogosto vodijo v cikle ekonomske rasti in krčenja, kar povzroča težave vsem, ki uporabljajo nadzorovano valuto.

Primer: Oznaka »prevelike, da bi propadle« se nanaša na finančne ustanove, ki so tako velike in medsebojno povezane, da bi imel njihov propad katastrofalne posledice za celoten finančni sistem. Med finančno krizo leta 2008 je več velikih bank veljalo za »prevelike, da bi propadle«, zato je ameriška vlada posredovala in zagotovila finančno pomoč, da bi preprečila njihov propad.

Eden od najbolj vidnih primerov ustanove, ki je bila v času finančne krize »prevelika, da bi propadla«, je bila investicijska banka Lehman Brothers. Ko je septembra 2008 banka Lehman Brothers razglasila stečaj, je to sprožilo učinek domin, med drugim skorajšnji propad zavarovalniškega velikana AIG in velik padec borznih tečajev. Ameriška vlada je morala posredovati in pomagati drugim velikim finančnim ustanovam, da bi preprečila nadaljnji kaos in zaščitila širše gospodarstvo.

Poznavanje delovanja teh politik je ključno za razumevanje omejitev centraliziranih fiatnih finančnih sistemov. Dokler ne boste razumeli težave, ne boste prepoznali rešitve. Zdaj, ko smo predstavili delovanje fiatnega sistema v preteklosti in sedanjosti, bomo razpravljali o tem, kakšna je trenutna prihodnost fiatnega sistema: centralnobačne digitalne valute ali valute CBDC.

## 4.3 Centralnobačne digitalne valute: Prihodnost fiatnega denarja

Centralnobačne digitalne valute (CBDC) so naslednji korak fiatnih valut. Za razliko od kombinacije fizičnih bankovcev, kovancev in digitalnih plačil so CBDC popolnoma digitalne oblike fiatnih valut, ki jih izdajo vlade in nadzorujejo centralne banke.

Predstavljajte si valuto, ki jo uporabljate vsak dan, vendar brez otipljivosti – brez kovancev, ki bi žvenketali v vašem žepu, ali bankovcev, ki bi jih bilo treba zložiti. CBDC se razlikujejo po tem, da vladam in centralnim bankam zagotavljajo višjo raven nadzora in spremljanja. Z valutami CBDC organi pridobijo pregled nad finančnimi transakcijami brez primere, kar olajša sledenje in urejanje pretoka denarja.

Vlade in centralne banke lahko zlahka prilagodijo obliko in ponudbo valut CBDC, manipulirajo z obrestnimi merami ter natančneje uporabljajo orodja denarne in fiskalne politike. V osnovi valute CBDC zagotavljajo bolj učinkovito sredstvo, s katerim lahko oblasti vplivajo in upravljajo svojo fiatno valuto.

Medtem ko se valute CBDC zdijo prihodnost fiatnega denarja, sedanji svetovni denarni sistem že deluje na čistem fiatnem standardu. Fiatne valute niso več vezane na zlato, zaradi česar se denarna ponudba znatno poveča brez kakršnih koli dejanskih omejitev.

Zdaj, ko bolje razumete delovanje fiatnega sistema, je čas, da v 5. poglavju raziščete njegove posledice.









## 5. poglavje

# ***Kako težave vodijo do rešitev***

### 5.0 Predstavitev težave

#### 5.1 Zmanjševanje kupne moči

##### 5.1.1 Denarna inflacija in njen vpliv na kupno moč

Dejavnost: učinki inflacije – dražba

#### 5.2 Breme globalnega dolga in socialna neenakost

##### 5.2.1 Vpliv na posameznike – izguba kupne moči

##### 5.2.2 Vpliv na družbo – večanje premoženjske neenakosti

Dejavnost: posledice sistema fiat valut

##### 5.2.3 Breme globalnega dolga

#### 5.3 Cypherpunksi in iskanje decentralizirane valute

##### 5.3.1 Cypherpunkovci

##### 5.3.2 Centralizirani in decentralizirani sistemi

##### 5.3.3 Kratka zgodovina digitalnih valut

# Kako težave vodijo do rešitev

## 5.0 Predstavitev težave

Kdor nadzoruje količino denarja v naši državi, je absolutni gospodar celotne industrije in trgovine ... ko boste spoznali, da celoten sistem tako ali drugače preprosto nadzoruje nekaj vplivnih ljudi na vrhu, vam ne bo treba razlagati, kako nastanejo obdobja inflacije in depresije.

James A. Garfield, predsednik ZDA

V 4. poglavju ste izvedeli, kako se finančni svet zanaša na sistem, ki morda ni tako močan, kot je sprva videti. Zdi se, da sistem fiatnih valut, ki ga poganjajo nenehni prilivi papirnatega denarja, koristi bolj peščici kot pa množici. V tem poglavju je razloženo, kaj sistem fiatnih valut pomeni za običajne ljudi in družbo. Na koncu si bomo ogledali zgodbo o skupini posameznikov, ki so zaznali te težave in si tiho prizadevali najti rešitev, ki bi lahko spremenila prihodnost človeške družbe.

## 5.1 Zmanjševanje kupne moči

### 5.1.1 Denarna inflacija in njen vpliv na kupno moč

Denarna inflacija je povečanje denarne mase v gospodarstvu, ki neposredno vpliva na povprečnega človeka z zmanjševanjem njegove kupne moči. Ko je v obtoku več denarja, se začne cikel inflacije cen. Pojavi se povečano povpraševanje po blagu in storitvah, kar posledično privede do rasti cen.

Za primer si oglejmo majhno skupino prijateljev – Aleša, Jaka in Erika. Vsak od njih ima en evro, na voljo pa jim je ena plastenka vode. Začetno stanje je preprosto: trije ljudje s skupaj tremi evri in ena plastenka vode. Predpostavimo, da se na primer lokalna vlada odloči, da vsakemu prijatelju nameni dodaten evro. Zdaj imajo skupaj šest evrov. S tem novim denarjem si vsi želijo kupiti plastenko vode. Ker želijo vsi trije prijatelji imeti isto plastenko, začnejo licitirati.

Povečano povpraševanje, podkrepljeno z dodatnim denarjem, jih spodbudi, da za plastenko vode plačajo več, kot je bila začetna cena. Na koncu se zaradi licitacije cena plastenke vode zviša. Posledično se zmanjša njihova kupna moč. Čeprav imajo več denarja, ne morejo kupiti toliko plastenk vode kot prej, kar kaže kakšen vpliv ima inflacija na vrednost njihovega denarja.

V tem primeru se je kupna moč prijateljev zmanjšala, ker so uporabljali obliko denarja, na katero so vplivali zunanji dejavniki, kot so dodatni evri, ki jim jih je zagotovila vlada. Pomanjkanje nadzora nad denarno maso in povečano povpraševanje sta povzročila dvig cen, zaradi česar so prijatelji z dodatnimi evri težje kupili enako količino blaga.


To nakazuje, kako so na kupno moč prijateljev vplivali dejavniki, na katere sami niso imeli vpliva, in poudarja pomen razumevanja ter skeptičnega sprejemanja sistemov, ki vplivajo na vrednost našega denarja.

Zdaj pa si oglejmo ta primer v resničnem življenju.


### Dejavnost: učinki inflacije – dražba

Cilj: razumeti pojem inflacije in njen vpliv na cene blaga ter storitev v gospodarstvu.

#### Definicije:


 Denarna masa: skupna količina denarja v obtoku v gospodarstvu v določenem trenutku. To vključuje:

- fizična valuta, kot so kovanci in bankovci,
- tekoči računi,
- varčevalni računi,
- računi denarnega trga,
- majhni vezani depoziti (kot so depozitni certifikati) pod 100.000 EUR.

 Dražba: javna prodaja, kjer je blago ali premoženje prodano najvišjemu ponudniku.

#### Vaja v razredu – sledite spodnjim navodilom:

1. Od učitelja boste prejeli naključno vsoto denarja Monopolija. Ta predstavlja denarno maso družbe.
2. V spodnjo tabelo zapišite celotno denarno maso.
3. Učitelj bo učencem ponudil čokoladico na dražbi. Če jo želite dobiti, morate z denarjem Monopolija zanjo oddati najvišjo ponudbo. Zmagovalno ponudbo zabeležite poleg denarne mase.
4. Učitelj bo nato dodal precejšnjo količino denarja Monopolija k skupni denarni masi. To predstavlja povečanje denarne mase v gospodarstvu. Kasneje boste izvedeli, kako se v gospodarstvu povečuje ali zmanjšuje denarna masa.

 Družbe so lahko pogosto nepredvidljive in nepravične, kar je razvidno iz primera dejavnosti, kjer učitelj naključno razdeli večjo vsoto denarja le nekaj izbranim učencem. To je odraz resničnih življenjskih razmer, kjer smo lahko priča neenakomerni porazdelitvi virov in priložnosti, ki hkrati poudarja tudi pogosto naključnost in nepravičnost.

5. Učitelj bo, enako kot prej, učencem na dražbi ponudil še eno čokoladico. Zmagovalno ponudbo zabeležite poleg denarne mase v tabeli.
6. Učitelj bo dražbo ponovil še tretjič.

# Kako težave vodijo do rešitev

Krog	Denarna masa	Zmagovalna ponudba
1		
2		
3		

## Zaključek:

1. Kako je povečanje denarne mase vplivalo na zmagovalne ponudbe za čokoladico?
2. Kakšna je povezava med povečevanjem denarne mase in inflacijo?
3. Kako je denarna masa pomembna v resničnem svetu?
4. Kaj menite, da se bo zgodilo s cenami blaga in storitev, ko bo v gospodarstvo pritekel nov denar? Ali menite, da so spremembe cenčasne ali trajne, in zakaj? Kako po vašem mnenju spremembe cen dolgoročno vplivajo na državljane?

## 5.2 Breme globalnega dolga in socialna neenakost

### 5.2.1 Vpliv na posameznike – izguba kupne moči

Andrej je študent, ki živi v majhnem stanovanju. Za krajši delovni čas dela v kavarni, da lahko plača življenjske stroške in šolnino. Takoj ko je začel živeti samostojno, je Andrej začel uspešno voditi svojo glavno knjigo.



Glavna knjiga je podroben zapis vseh denarnih transakcij. Z njo lahko učinkoviteje spremljamo vse denarne prilive in odlive.

Na začetku leta 2023 je za celoletne življenjske stroške, vključno z najemnino, hrano in drugimi potrebščinami, odštél 10.000 EUR. To so bile njegove transakcije januarja 2023:

## 5. poglavje

Datum	Opis	Znesek	Vrsta	Stanje
1. 1. 2023	Začetno stanje			1.600 EUR
1. 1. 2023	Najemnina za januar	800 EUR	V breme	800 EUR
5. 1. 2023	Živila	100 EUR	V breme	700 EUR
15. 1. 2023	Plača za krajši delovni čas	500 EUR	V dobro	1.200 EUR
20. 1. 2023	Gorivo za avtomobil	350 EUR	V breme	850 EUR
30. 1. 2023	Učbeniki	150 EUR	V breme	700 EUR

Iz glavne knjige je razvidno, da je bilo Andrejevo začetno stanje 1.600 EUR, od katerih je porabil (v breme) 800 EUR za plačilo mesečne najemnine. Nato je porabil 100 EUR za živila in prejel 500 EUR (v dobro) za svoje delo s krajšim delovnim časom, tako da je bilo njegovo stanje na računu 1.200 EUR. Nato je porabil denar za gorivo in učbenike, tako da mu je konec meseca ostalo 700 EUR.

Čez dvanajst mesecev gresta Andrej in dedek skupaj na kosilo, kjer se pogovarjata o podrobnostih Andrejevega proračuna za leto 2024. Andrej opazi, da njegov proračun ni več tako prožen kot nekoč in da so se življenjski stroški v zadnjem letu močno povečali. Medtem ko se Andrej sprašuje, kako je to mogoče, mu dedek pokaže naslednjo sliko.

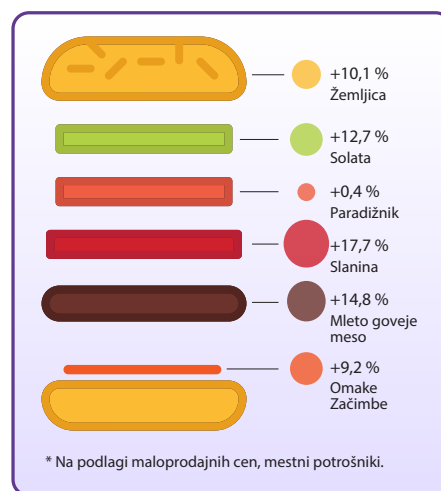
Andrej ne more verjeti svojim očem. Takrat ugotovi, da so se stroški blaga in storitev tekom časa močno povečali, zaradi česar se je zmanjšala njegova kupna moč.



Njegov dedek pravi: »Leta 1956 sem bil še mlad fant, ki je začel svojo pot v svetu. Spomnim se, da sem kot delavec v tovarni zaslužil 380 USD na mesec. Morda se ne zdi veliko, vendar je bilo to takrat spodobna plača. Pravzaprav mi je uspelo privarčevati dovolj denarja, da sem si lahko kupil hišo v predmestju.«

Dedek nadaljuje: »Višina stroškov za dobrine je bila v prejšnjem stoletju zelo drugačna. Leta 2020 si moral za 30 čokoladnih tablic Hershey's na primer odšteti 26,14 USD. Leta 1913 pa je bila cena za enako količino čokoladnih tablic samo 1,00 USD.«

Ta velika razlika v ceni kaže na spremembo kupne moči skozi čas in tekom let zaradi inflacije.



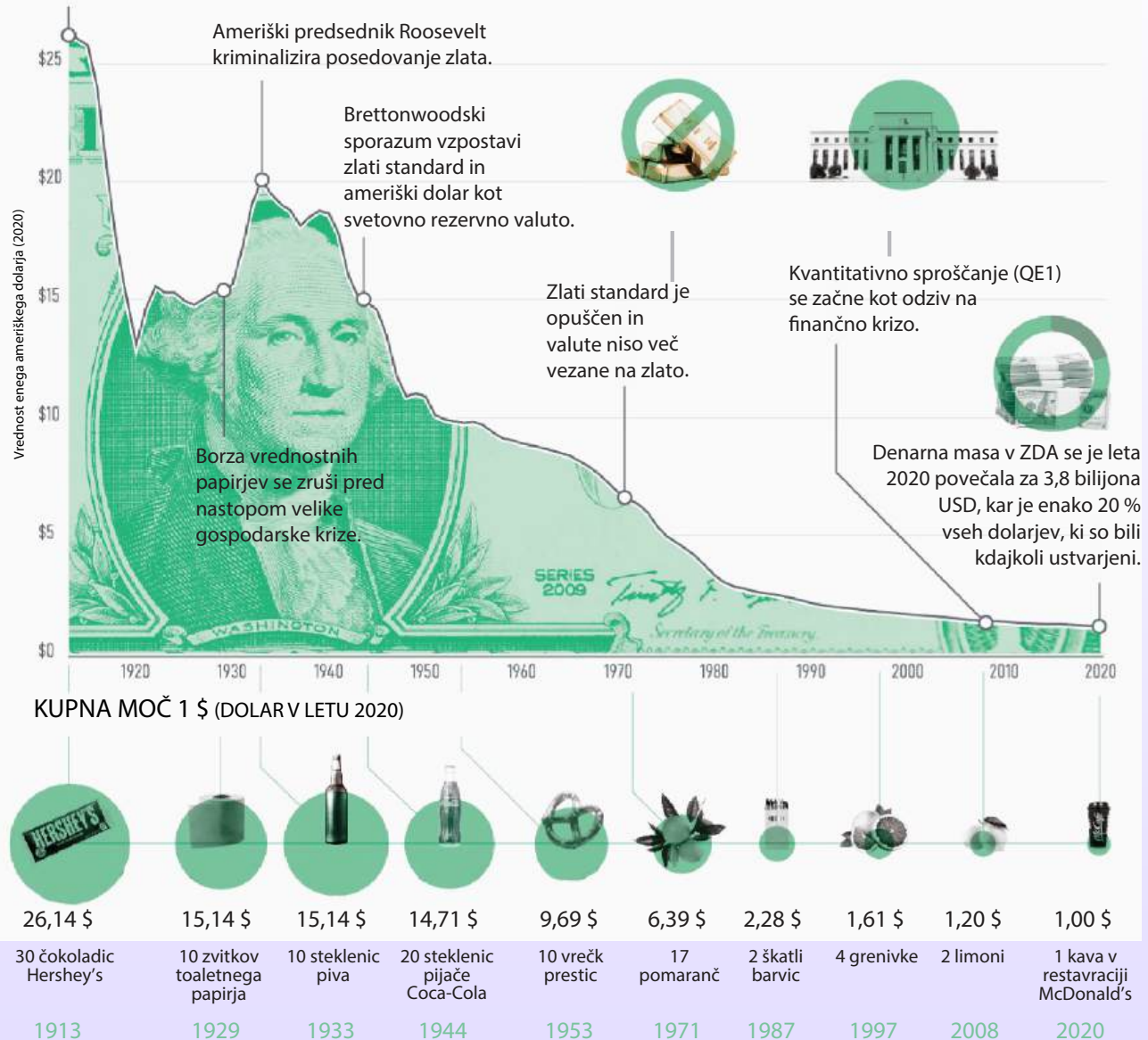
# Kako težave vodijo do rešitev

## Vrednost dolarja

### Kupna moč ameriškega dolarja

Kupna moč ameriškega dolarja se je v zadnjem stoletju zaradi naraščajoče inflacije in denarne mase močno zmanjšala.

Zakon o zveznih rezervah ustanovi centralno banko z možnostjo upravljanja denarne mase v državi.



Andrej: »Kaj? To je neverjetno. Ne morem si predstavljati, kako nizki bi bili stroški moje najemnine takrat v primerjavi s trenutnimi stroški «

Dedek: »Da, najemnina je bila takrat veliko cenejša. Oglejva si še en primer: takrat si za 1,00 USD lahko kupil približno 10 vrečk prestic. Leta 2020 sem za enako količino moral odšteti 9,69 EUR. Predstavljaš si, koliko znaša danes 10 vrečk prestic.«

Andrej: »Dedek, to je res zelo zanimivo. Kako si to doživljal ti, ko si bil mlajši?«

Dedek: »Andrej, ko sem bil mlad, so bile vse stvari veliko cenejše. Hlebec kruha je stal samo 0,18 USD, za dobre štiri litre bencina pa si moral odšteti zgolj 0,29 USD. Neverjetno je, za koliko so se zvišali življenjski stroški.«

Po pogovoru z dedkom se Andrej vrne domov in si znova ogleda svojo glavno knjigo. Ugotovi, da mora v svoj proračun za leto 2024 dodati 1.000 USD, če želi kupiti enako košarico blaga in storitev, kot jo je kupil prejšnje leto. To pomeni, da se je njegova kupna moč zmanjšala za 1.000 USD, saj mora zdaj za nakup enakega blaga in storitev porabiti več denarja. Medtem ko se Andrejeva plača zvišuje le minimalno, njegovi življenjski stroški vsako leto skokovito naraščajo.

V spodnji tabeli so prikazani Andrejevi stroški v prvem in drugem letu ter odstotek povečanja cene.

Če si želi Andrej zagotoviti enak življenjski standard, bo moral oddelati več delovnih ur na teden, da bo prejel dodatnih 1.000 USD.

Po podatkih ameriškega urada za statistiko dela so cene danes približno 30-krat višje kot leta 1913. To pomeni, da lahko danes za en USD kupimo le približno 3 % tistega, kar smo lahko kupili takrat.

Element	Strošek 1. leto	Strošek 2. leto	% povečanja
Najemnina	4.000 USD	4.500 USD	12.5 %
Živila	2.000 USD	2.300 USD	15 %
Potrebščine	4.000 USD	4.200 USD	5 %
Skupaj	10.000 USD	11.000 USD	10 %

Če bi imel Andrej možnost potovanja skozi čas, kjer bi lahko izbiral, ali želi vzeti 100 USD in iti v leto 1913 ali pa v leto 2023, kjer bi mu ostali samo 3 USD, je to enako, kot da bi moral izbirati med nakupom več dobrin v preteklosti in nakupom le nekaj majhnih priboljškov danes. Velika razlika v vrednosti kaže, za koliko se je kupna moč denarja z leti zmanjšala.

STROŠKI BIVANJA 1938	
BIVANJE	
Nova hiša	3.900,00 USD
Povprečni dohodek	1.731,00 USD na leto
Nov avto	860,00 USD
Povprečna najemnina	27,00 USD na mesec
Šolnina za univerzo Harvard	420,00 USD na leto
Vstopnica za kino	25 ¢
Gorivo	10 ¢ za galono
Poštna znamka v ZDA	3 ¢
HRANA	
Granulirani sladkor	59 ¢ za 10 funtov
Mleko z vitaminom D	50 ¢ za galono
Mleta kava	39 ¢ za funt
Slanina	32 ¢ za funt
Jajca	18 ¢ per dozen
(Na podlagi originalne slike)	



# Kako težave vodijo do rešitev

Če povzamemo podatke s števkami, Andrej na leto zasluži veliko več kot njegov dedek, vendar pa je imel znesek denarja Andrejevega dedka v tistem času veliko večjo vrednost in z njimi je lahko dedek kupil veliko več dobrin.

Rast produktivnosti in urne postavke  
(1948-2017)



OPOMBA: Urna postavka vključuje plače in prejemke za proizvodne delavce in delavce brez nadzorne funkcije.

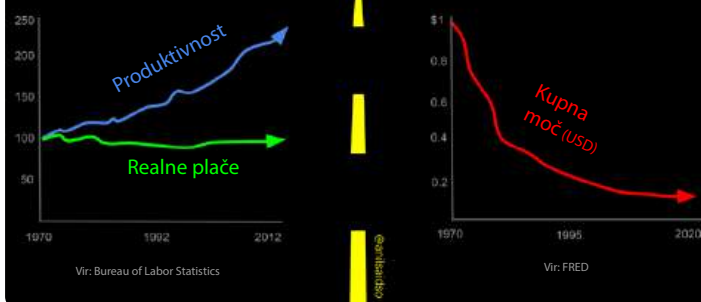
V današnjem svetu visoka inflacija ljudi odvrača od varčevanja.

Namesto tega se jih večina odloči takoj potrošiti denar, saj se njegova vrednost hitro zmanjšuje. Zaradi tega pesimističnega pristopa ne morejo načrtovati prihodnosti.

Kot je razvidno iz grafa, rast plače povprečnega posameznika po uskladitvi z inflacijo stagnira, kar pomeni, da kljub večji količini opravljenega dela obseg povišic ni enakovreden obsegu zmanjševanja vrednosti denarja.

Andrejev primer je le eden izmed mnogih. V svetu fiatnih valut je povsem običajno, da vlade ustvarjajo denar »iz nič«, da bi uresničile svoje načrte, posledice pa nosijo posamezniki po vsem svetu. Cene vsakdanjih dobrin, kot so kruh, stanovanja, živila in počitnice, so iz leta v leto višje. Medtem ko se bogati zaradi lastništva premoženja okoriščajo z inflacijo, pa običajni ljudje samo opazujejo, kako njihov težko prisluženi denar izgublja svojo vrednost. Rezultat? Ljudje in družine po svetu se soočajo s težavami, ki jih prinaša zmanjšanje kupne moči.

Pot v suženjstvo



Ljudje po svetu imajo več služb in daljše delovne čase, da bi ohranili enak življenjski standard. To je podobno tekalni stezi, kjer tečete čedalje hitreje, vendar se nikoli zares ne premaknete naprej. Zaradi sistema fiat valut imajo posamezniki občutek, kot da z naraščajočimi cenami nenehno tekmujejo.



V prizadevanjih pri obvladovanju naraščajočih stroškov mnogi poiščejo rešitev v zadolževanju, kar je podobno majhnemu obližu na zelo veliki rani. Ljudje vzamejo posojila ali sprejemajo nepremišljene odločitve že samo za plačilo osnovnih življenjskih stroškov. Hitri denar postane nuja, posamezniki pa se znajdejo v krogu, kjer imajo vsakdanji stroški prednost pred načrtovanjem prihodnosti.

Nenehno tiskanje denarja v sistemu fiatnih valut ima psihološki vpliv na ljudi. Spodbuja visoko časovno preferenco – osredotočenost na kratkoročne koristi namesto na dolgoročno načrtovanje. Podobno posamezniki v svetu fiatnih valut običajno dajejo prednost kratkoročnim koristim. Gre za nagon po preživetju, ki temelji na odvisnosti, kjer posamezniki iščejo sredstva za pridobitev hitrega denarja, tudi če to na dolgi rok ni trajnostno ali izvedljivo.

Vpliv sistema fiat valut predstavlja za posameznike po svetu velik izziv. V takšnem sistemu se cene zvišujejo, dohodki stagnirajo, boj za preživetje pa postaja vsakdanja bitka. Medtem ko nekatere skupine še naprej kopičijo bogastvo, pa je večina ljudi po svetu odvisna od sistema, ki jih dela vedno bolj revne.

### 5.2.2 Vpliv na družbo – večanje premoženjske neenakosti

V družbi, ki temelji na stabilnem denarju, je sprejemanje odločitev vlade na področju financ povezano z odobritvijo ljudi. V sistemu fiat valut pa se lahko vlade neomejeno zadolžujejo na račun svojih državljanov.

Možnost tiskanja denarja po lastni presoji pogosto vodi v politično centralizacijo. V sistemu fiat valut lahko vlade kopičijo ogromne dolgove in sprejemajo odločitve, ki koristijo njim samim in ne večini. Velesile, kot so Združene države Amerike, imajo zaradi tega konkurenčno prednost. Tiskajo lahko neomejene količine denarja za financiranje svojih načrtov, vključno z vojnami. Dominantne države s tem pridobijo možnost nadzorovanja, vplivanja in sodelovanja v geopolitičnih konfliktih, česar posledica je globalno neravnovesje moči. Vojne in večji ukrepi za izvajanje nadzora nad drugimi so za velesile finančno izvedljivi cilji, medtem ko se druge, finančno manj vplivne države, soočajo z omejitvami.

V sistemu fiat valut bogastvo ni porazdeljeno enakomerno. Običajno je v rokah nekaj izbrancev. To spominja na igro Monopoli, kjer ima peščica igralcev v lasti skoraj vse hotele in nepremičnine, medtem ko se jih večina prizadeva, da ne izgubi vsega. Takšen sistem je postal orodje, s katerim nekatere skupine kopičijo bogastvo. Vlade s tiskanjem denarja in tesnim sodelovanjem s centralnimi bankami v gospodarstvo vnašajo več denarja, prejemniki tega novo ustvarjenega denarja pa so tisti z že obstoječim bogastvom in statusom – vplivne organizacije in vplivni posamezniki. Te skupine se okoristijo s sveže natisnjenim denarjem, še preden se v gospodarstvu pokažejo njegovi negativni vplivi, kot je zmanjšanje kupne moči.

# Kako težave vodijo do rešitev

Premoženjska neenakost ne izkazuje zgolj razmerja v količini pridobljenega imetja, temveč zaviranje gospodarske mobilnosti. Ljudje iz manj privilegiranih okolij se soočajo z zahtevnim izzivom vzpenjanja po ekonomski lestvici, kar je podobno teku s težkim nahrbtnikom. Vedno večji razkorak med bogatimi in revnimi povzroča težave vsem, saj bogati narekujejo oblikovanje politik v svojo korist. To otežuje življenje običajnih ljudi, povzroča socialne nemire, pomanjkanje zaupanja v ustanove in razpadanje skupnosti kot hišic iz kart. Nestabilnost sistema fiatnih valut se kaže v gospodarski negotovosti, političnih nemirih in globalnih posledicah, ko se zahodni svet sooča z gospodarsko krizo.

Gre za globalni fenomen, ki vpliva na družbe v razvitih državah kot tudi v državah v razvoju. Bogati, ki pogosto delujejo na transnacionalni ravni, izkoriščajo globalni finančni sistem sebi v prid in tako še povečujejo razlike med višjimi in nižjimi sloji.

V sistemu fiatnih valut postaja zadolževanje ljudi stalna praksa. Vlade, ustanove, podjetja in posamezniki po svetu se utapljajo v morju dolgov.



Psihološki vidik sprejemljivosti dolgov temelji na zasnovi takšnega sistema. V zadnjih desetletjih so se podjetja čedalje lažje zadolževala, zaradi naraščajočih cen in življenjskih stroškov pa je zadolževanje pogosto postalo celo nuja za običajne ljudi.

Potrošništvo – stalna želja po nakupovanju in trošenju – ljudi sili k nakupu več dobrin, kot jih potrebujejo, kar vodi v prekomerno potrošnjo in kopičenje odpadkov. Čeprav je morda videti kot nenehna nakupovalna mrzlica, pa dejanski stroški presegajo ceno ter vplivajo na psihološko zdravje in dobrobit ljudi.

Sistem fiatnih valut ni le gospodarski mehanizem. Je sistem, ki oblikuje človeško družbo kot celoto. Od kopičenja moči do globalne dinamike, premoženjskih razlik in družbenih norm – sistem fiatnih valut neposredno vpliva na delovanje držav in način življenja običajnih državljanov.

## Dejavnost: posledice sistema fiatnih valut

1. Ali obstajajo kakršne koli druge posledice sistema fiatnih valut za posameznike in celotno družbo?
2. Kakšne so posledice sistema fiat valut v vaši državi? Kaj se je dogajalo tekom zgodovine in kako je to vplivalo na ljudi v vaši državi?
  - a. Osebni primeri: interaktivna seja

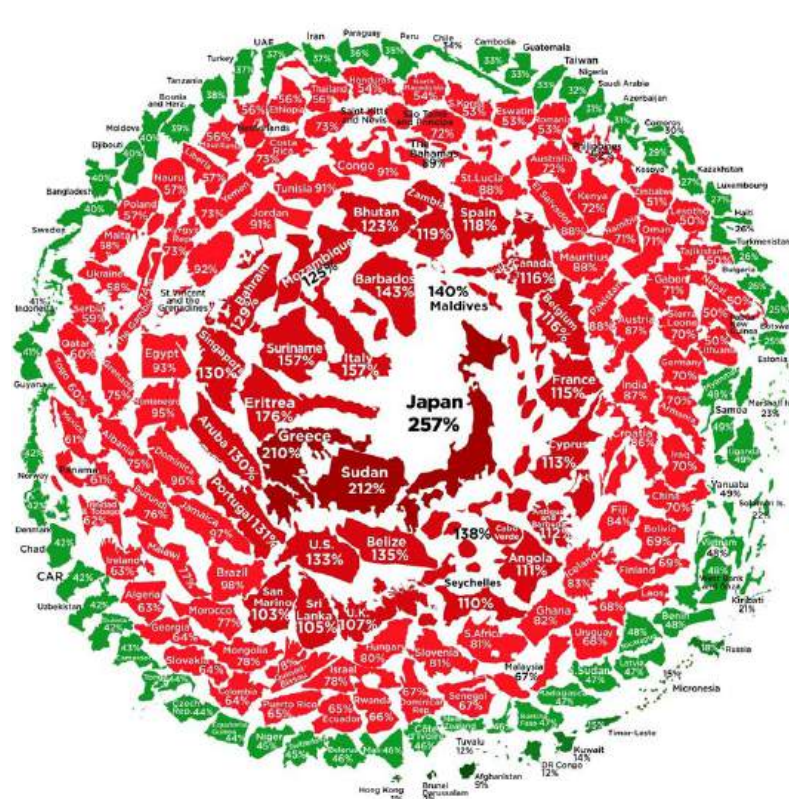
### 5.2.3 Breme globalnega dolga

Zaradi sistema fiatnih valut so vlade po svetu ujete v ogromni mreži dolgov, imenovani »globalna dolžniška spirala«. Zamislite si, da si izposodite več denarja, kot ga lahko kdaj koli vrnete. Ta scenarij postaja stalnica po vsem svetu. Vlade, ki se utapljajo v dolgovih, so ujete v nevarni igri kopičenja večjega dolga, kot ga lahko kdaj koli povrnejo. To je zgodba o nepremišljenem trošenju, zadolževanju in pomanjkanju vpogleda v prihodnost, ki države po svetu potiska na rob finančne katastrofe.



Dolg ameriške zvezne vlade se je od leta 2019 do danes povečal za neverjetnih 10 bilijonov dolarjev. Skupni dolg se je s približno 23 bilijonov dolarjev v četrtem četrtletju 2019 skokovito zvišal na današnjih astronomskih 34 bilijonov dolarjev. Hitrost novega zadolževanja vlad po svetu se ne upočasnjuje, temveč celo pospešuje. Po napovedih naj bi bilo v letu 2023 ustvarjenega največ dolga po burnem letu 2021, ki ga je zaznamovala pandemija covida.

Stanje svetovnega javnega dolga



Kaj to pomeni za posameznike in družbe, ki se morajo že zdaj spopadati s posledicami sistema fiatnih valut? Dolžniška spirala, v katero so ujete, je kot snežna kepa, ki se vali po hribu navzdol – nenehno se veča, mi pa ne vemo, kako naj jo ustavimo.

Prej omenjene posledice – od premoženjske neenakosti do družbenih nemirov – ne bodo izginile. Nasprotno, breme globalnega dolga je doseglo točko brez povratka, kar pomeni, da se bo stanje samo še poslabšalo.

Delež dolga v BDP 2021 (%)

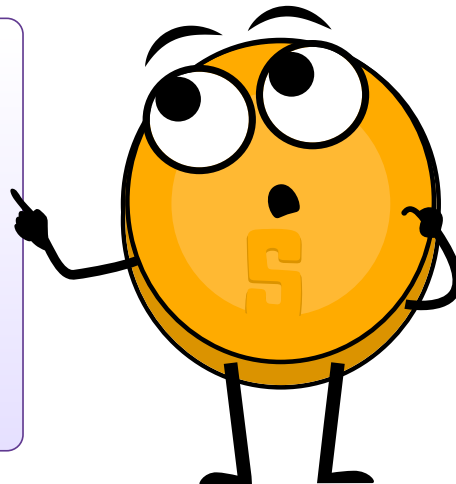


# Kako težave vodijo do rešitev



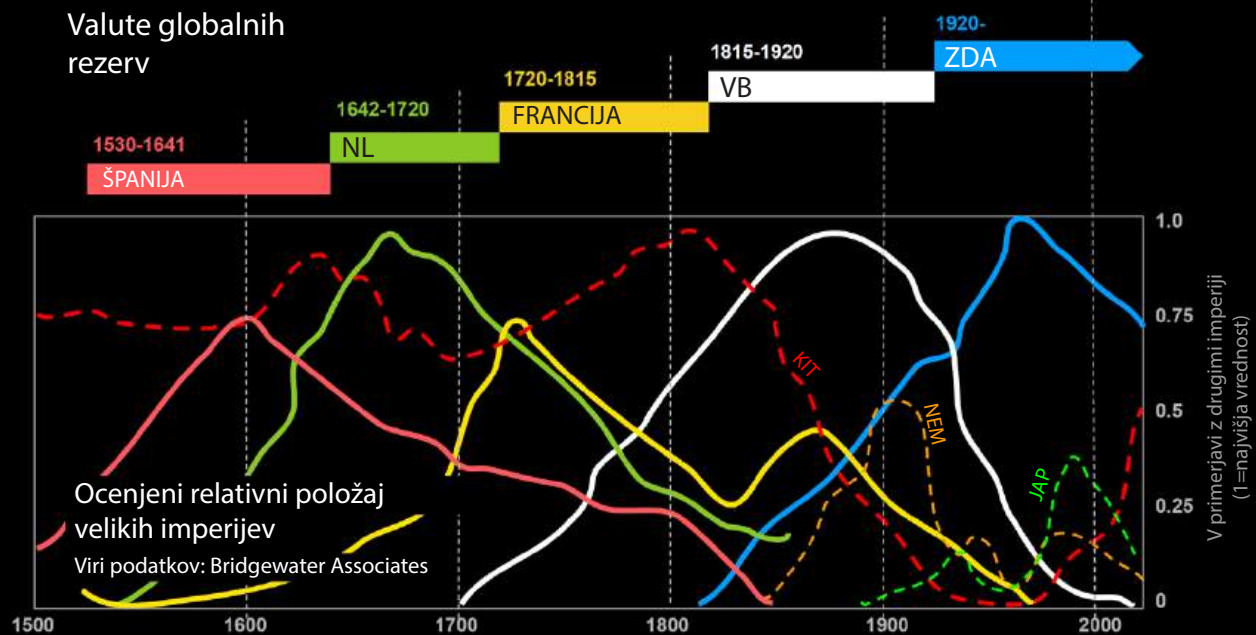
Dokler denarja ne bomo vzeli iz rok države, ne bomo imeli več dobrega denarja. Vse, kar lahko storimo, je, da na prebrisan način uvedemo nekaj, česar ne bodo mogli ustaviti.

Friedrich Hayek  
Nobelov nagrajenec za ekonomijo



@anilsaidso

## Valute globalnih rezerv



## 5.3 Cypherpunksi in iskanje decentralizirane valute

Skozi zgodovino lahko opazujemo postopno kopičenje denarja s strani bank in vlad, kar je privedlo do uvedbe sistema fiat valut, kot ga poznamo danes, in njegovih uničujočih posledic za družbo. Vendar pa so se z razvojem novih tehnologij, kot sta šifriranje in internet, oblikovale tudi nove zamisli, kot je neodvisni digitalni denar – neodvisen od vladnih posegov, odprt in dostopen vsem. Spoznajmo ljudi, ki vodijo to revolucionarno gibanje – cypherpunkovce.



### 5.3.1 Cypherpunksi



Računalnik lahko uporabljamo kot orodje za osvoboditev in zaščito ljudi, ne pa za njihov nadzor.

Hal Finney



V drugi polovici 20. stoletja smo bili priča številnim tehnološkim dosežkom, kot sta računalnik in internet, ki so utrli pot novi digitalni dobi.


Skupina ljudi je spoznala, da bodo te obsežne inovacije kmalu spremenile način delovanja družbe. Predvideli so tako pozitivne kot tudi negativne vplive osebnega računalnika – lahko je orodje za zagotavljanje svobode posameznikov ali pa orodje za doseganje popolnega nadzora in spremljanja.

To so bili Cypherpunksi. Gre za ne tesno povezano skupino aktivistov, kriptografov, programerjev in zagovornikov varstva zasebnosti z eno skupno vizijo – prizadevati si za zagotovitev zasebnosti, varnosti in decentralizirane digitalne prihodnosti. Izraz »cypherpunk« je zveza besed »cypher«, ki se nanaša na kriptografsko kodo, in »punk«, ki predstavlja protikulturni etos upornišva.

Cypherpunksi so verjeli, da lahko zmogljivosti kriptografije zaščitijo svoboščine posameznikov. Njihovi cilji so vključevali razvoj orodij za zaščito spletnih komunikacij, anonimizacijo internetnih dejavnosti in uvedbo digitalnih valut, ki bi jih lahko uporabljali zunaj nadzora centraliziranih organov.

Cypherpunksi so razumeli posledice sistema fiatnih valut in videli grožnjo »orwellovske prihodnosti«. Menili so, da je njihovo poslanstvo zagotoviti osebni računalnik in internet kot skupno dobro in ne kot orodje za krepitev nadzora države nad ljudmi.

#### DEFINICIJA ORWELLOVSKE PRIHODNOSTI:



Orwellovska prihodnost se nanaša na distopično vizijo, ki jo navdihujejo dela Georgea Orwella. Izraz je povezan z morasto in totalitarno družbo, za katero so značilni zatiralska vladna oblast, obsežen nadzor, propaganda in manipulacija z informacijami. Izraz »orwellovski« pogosto opisuje scenarij, kjer so svoboščine in avtonomija državljanov močno omejene, nesoglasja zatrta, resničnost pa popačena za namene služenja interesom vplivnega in avtoritarnega režima. Ta pojem nosi ime po Georgeu Orwellu, ki je v svojih delih opozarjal na potencialne nevarnosti nenadzorovane moči vlade in krčenja temeljnih človekovih pravic.

# Kako težave vodijo do rešitev

Ključne osebe gibanja cypherpunksov so bili Eric Hughes, Timothy C. May in John Gilmore. Leta 1992 je Eric Hughes napisal »Manifest cypherpunksov«, v katerem je predstavil načela skupine. Manifest poudarja pomen zasebnosti, šifriranja in potrebe po tem, da posamezniki prevzamejo nadzor nad svojo digitalno identiteto.



Oglejte si ta videoposnetek in spoznajte zgodbo cypherpunkovcev.

Ena od najpomembnejših inovacij cypherpunksov je bila izdelava kriptografskih orodij in protokolov. Leta 1991 je Phil Zimmermann predstavil programsko opremo za šifriranje e-pošte PGP (Pretty Good Privacy – Precej dobra zasebnost), ki je postala vodilni projekt. PGP je uporabnikom omogočal pošiljanje šifriranih sporočil prek interneta, ki jih ni mogel dešifrirati nihče razen predvidenega prejemnika. Pred tem so lahko vsa sporočila, poslana prek interneta, prestregli in prebrali drugi, na primer vlade.

Cypherpunksi so bili mnenja, da učinkovitost šifriranja, skupaj z internetom in računalnikom, zagotavlja trdne temelje za vzpostavitev decentraliziranih omrežij v digitalnem okolju, kar lahko posamezniki zasebno komunicirajo in opravljajo transakcije v internetu brez vmešavanja osrednjih organov.

Bili so na pravi poti ustvarjanja svetlejše prihodnosti za ljudi, kjer bi bila tehnologija orodje za povečanje svobode in ne nadzora. Manjkala sta le še decentralizirano omrežje in digitalna valuta.

## 5.3.2 Centralizirani in decentralizirani sistemi

### Centralizirani sistemi: en vladar, številne težave

V centraliziranem sistemu se vse vrti okoli enega glavnega organa, kot je na primer visoka stavba v mestu. Ta organ nadzoruje delovanje celotnega sistema. Kot primer lahko vzamemo tradicionalne banke, kjer vse odločitve sprejema majhna skupina.



Primer iz resničnega sveta: leta 2022 so med mirnimi protesti v Kanadi banke zamrzile račune protestnikov, kar je odraz dejstva, da lahko osrednji organ posreduje in nadzoruje dostop do finančnih storitev.



### Težave centraliziranih sistemov

- ☀ Osrednja točka odpovedi: če pride do težav pri osrednjem organu, se lahko celoten sistem zruši.
- ☀ Nadzor: majhna vplivna skupina ima ves nadzor in vso moč ter pogosto sprejema odločitve sebi v korist.
- ☀ Neučinkovitost in posredniki: centralizirani sistemi so lahko počasni in dragi zaradi nepotrebnih posrednikov, podobno kot prometni zastoji v mestu.
- ☀ Pomanjkanje avtonomije: ljudje morda ne bodo mogli sprejemati lastnih finančnih odločitev – o vsem odloča najvišji organ.
- ☀ Cenzura in omejitve: podobno kot lahko blokiramo nekatere dele mesta, lahko centralizirani sistemi blokirajo ali omejijo dostop do določenih finančnih virov.
- ☀ Izzivi glede prilagodljivosti: ko finančne storitve potrebuje več ljudi, centralizirani sistemi morda ne morejo slediti tej zahtevi.
- ☀ Varnostna tveganja: težave osrednjega organa lahko zaradi kibernetских napadov ogrozijo celoten sistem.
- ☀ Pomanjkanje preglednosti in zaupanja: notranje delovanje centraliziranih sistemov je zapleteno, zato jim ljudje težko zaupajo.

### Decentralizirani sistemi: moč ljudem

Predstavljajte si decentralizirani sistem kot velik gozd. Vsako drevo predstavlja posamezen del, ves gozd pa predstavlja celoten sistem. V nasprotju z mestom z eno samo osrednjo točko je decentralizirani sistem bolj podoben odpornemu gozdu, ki raste naprej, tudi če se en del sooča s težavami.

- ☀ Primer iz resničnega sveta: omrežje Tor in njegov brskalnik sta ustvarila decentralizirani sistem, ki zagotavlja ohranjanje anonimnosti ljudi v internetu, kjer je omrežje težko ustaviti ali cenzurirati.



### Prednosti decentraliziranih sistemov

- ☀ Izboljšana odpornost in zanesljivost: ni ene same točke odpovedi, zato je sistem zanesljiv, tudi v primeru morebitnih težav.
- ☀ Večja varnost: z ustreznim šifriranjem/zaščito se decentralizirani sistem učinkoviteje upira nadzoru enega organa.

# Kako težave vodijo do rešitev

- ✿ Večja samostojnost: ljudje imajo večji nadzor nad svojim denarjem, podatki in odločitvami.
- ✿ Izboljšana preglednost: vsi vidijo iste informacije, zato je sistem bolj zaupanja vreden.
- ✿ Okolje brez dovoljenj in omejitev: vsak se lahko pridruži ali sodeluje, zato je to vključujoč finančni sistem.
- ✿ Enake možnosti: vsi imajo na voljo enake priložnosti, da prispevajo in izrazijo svoje mnenje.
- ✿ Izboljšana zasebnost: podatki so razdeljeni med več udeležencev, ki večinoma uporabljajo psevdonime, zato decentralizirani sistemi zagotavljajo večjo zasebnost.

Decentralizirani sistemi imajo številne prednosti, vendar pa je skupno sprejemanje odločitev lahko težavno. Za to je potrebno sodelovanje vseh.

## Spreminjanje načina uporabe moči

V svetu centraliziranih in decentraliziranih sistemov je pomembno, kdo ima moč. Centralizirani sistemi dajejo moč majhni skupini, decentralizirani sistemi pa jo porazdelijo in omogočijo vključenost vsakega posameznika. Ta sprememba moči pomeni pravičnejšo in bolj demokratično prihodnost, kjer lahko množica ljudi vpliva na sistem, ki oblikuje njihova življenja.

## 5.3.3 Kratka zgodovina digitalnih valut

Ena od najpomembnejših tem, o katerih so razpravljali cypherpunksi, je bil digitalni denar. Spoznali so, da je treba ločiti državo in denar za zagotovitev prihodnosti, ki temelji na skupnem dobrem. David Chaum je s svojim pionirskim delom na področju kriptografskih protokolov za varne in zasebne transakcije postavil temelje za uresničitev tega spoznanja. Slaba stran tega protokola je bila, da je bil za njegovo delovanje potreben osrednji organ, kar je vzbudilo pomisleke glede ene same točke odpovedi in morebitne cenzure.

V naslednjih letih so številni cypherpunksi poskušali nadgraditi zamisli drug drugega, da bi ustvarili učinkovito rešitev za digitalno valuto brez vladnega nadzora. V spodnji tabeli so predstavljene pomembne inovacije, ki so jih razvili na poti ustvarjanja digitalnega denarja:

Ime in datum	Opis	Omejitve
E-Cash (1982)	Valuta E-Cash, ki jo je ustvaril David Chaum, je bila zgodnji koncept elektronskega denarja, osredotočenega na zasebnost s kriptografskimi tehnikami.	Valuta je zahtevala osrednji organ, zaradi česar so se pojavili pomisleki glede ene same točke odpovedi in morebitne cenzure.
DigiCash (1990)	Valuta DigiCash, ki jo je ustvaril David Chaum, je bila zasnovana kot digitalna oblika valute s poudarkom na zasebnosti.	Centralizirani model je bil razlog za njen stečaj leta 1998.



## 5. poglavje

B-Money (1996)	Valuta B-Money, ki jo je predlagal Wei Dai, je bila teoretični predlog anonimnega, distribuiranega sistema elektronskega denarja.	Valuta ni bila nikoli uvedena in je ostala zgolj konceptualna zamisel. Ni bilo izvedeno njeno praktično uvajanje.
HashCash (1998)	Valuta HashCash, ki jo je ustvaril Adam Back, je bila sistem dokaza o delu, zasnovan za omejevanje neželene e-pošte in napadov za zavrnitev storitve.	Valuta ni neposredno obravnavala težave dvojne porabe, povezane z digitalnimi valutami.
Bit Gold (1998)	Valuta Bit Gold, ki jo je predlagal Nick Szabo, je predstavljala decentraliziran sistem digitalne valute z elementi dokaza o delu.	Valuta ni bila nikoli uvedena in je ostala samo teoretični koncept.
e-Gold (2004)	e-Gold je bila centralizirana digitalna valuta, podprta s fizičnim zlatom, ki je uporabnikom omogočala nakup in prenos enot e-Gold.	Zaradi pravnih težav je bila leta 2009 ukinjena, kar je opozorilo na izzive, povezane s centraliziranimi digitalnimi valutami.

Cypherpunkovski so se v preteklih desetletjih kljub številnim poskusom, da bi ustvarili digitalno valuto brez nadzora katere koli skupine ali vlade, soočali s praktičnimi izzivi, zaradi česar se njihova prizadevanja niso mogla v celoti uresničiti v resničnem svetu. Ugotovili so, da ni tako preprosto ustvariti digitalne oblike gotovine, ki bi bila varna, skalabilna in široko sprejeta.

Zgodba pa se je spremenila, ko je oseba, ki se je učila iz izkušenj cypherpunksov, dvignila koncept decentralizirane digitalne valute na novo raven. V naslednjih poglavjih je predstavljeno, kako je ta oseba nadgradila predhodno 40-letno delo in ustvarila funkcionalni sistem.



## 6. poglavje

# *Uvod v Bitcoin*

### 6.0 Satoshi Nakamoto in vzpostavitev Bitcoina

#### 6.1 Kako deluje Bitcoin?

##### 6.1.1 Mehanizem Nakamotovega soglasja

##### 6.1.2 Glavni akterji

Dejavnost: doseganje soglasja v omrežju enakovrednih udeležencev

#### 6.2 Bitcoin kot stabilni digitalni denar

##### 6.2.1 Uvod

##### 6.2.2 Značilnosti Bitcoina

Dejavnost: razprava v razredu – ali je Bitcoin stabilni denar?

##### 6.2.3 Sprejemanje osebne odgovornosti

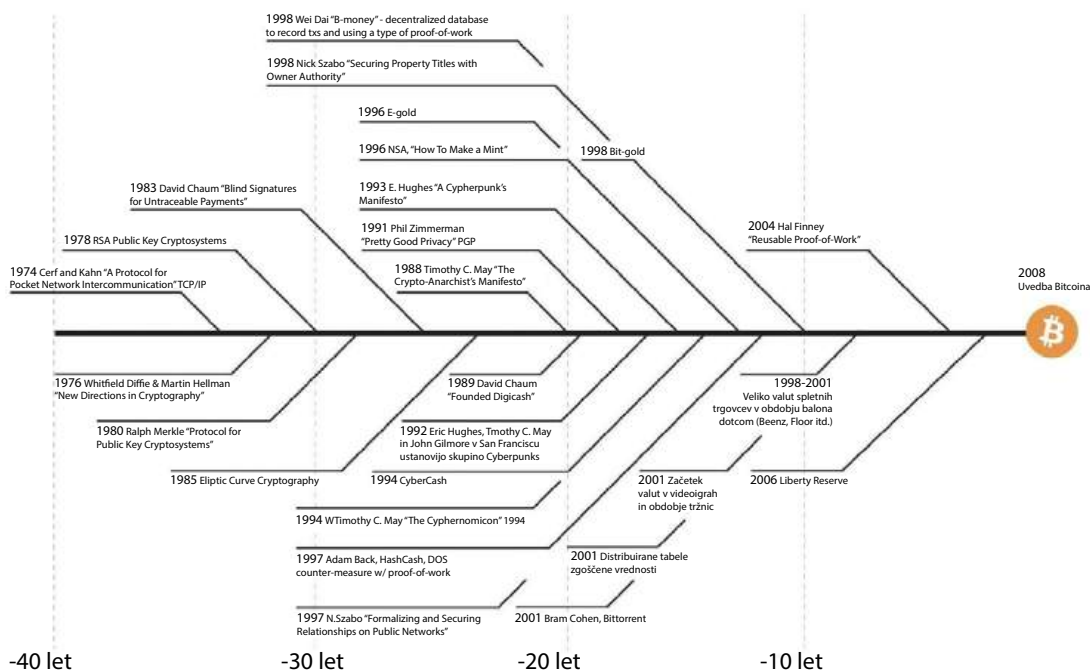
# Uvod v Bitcoin

## 6.0 Satoshi Nakamoto in vzpostavitev Bitcoina

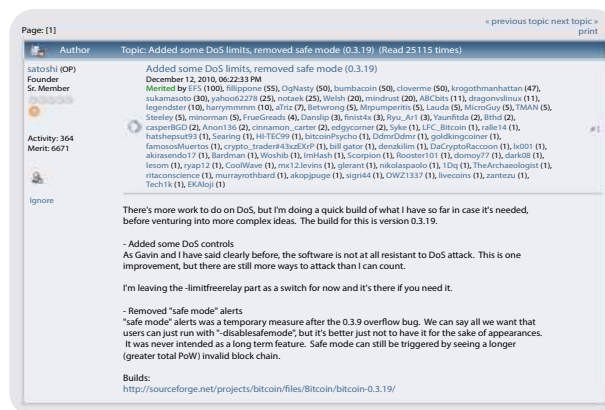
Veliko ljudi samodejno zavrača elektronsko valuto kot izgubljen primer zaradi vseh podjetij, ki so propadla v devetdesetih letih prejšnjega stoletja. Upam, da je jasno, da jih je uničila le centralno nadzorovana narava teh sistemov. To je prvi poskus uvedbe decentraliziranega sistema, ki ne temelji na zaupanju.

# Satoshi Nakamoto

## Predzgodovina Bitcoina - je rezultat 40 let raziskav, razvoja in povpraševanja

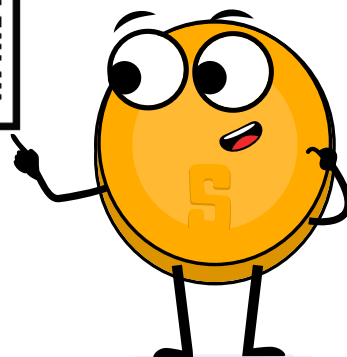


Kot je bilo predstavljeno v prejšnjem poglavju, je več cypherpunksov poskušalo ustvariti alternativni denarni sistem. V tem poglavju se nadaljuje zgodbo o enem od njih – vizionarju z imenom Satoshi Nakamoto. Ta anonimna oseba (moški, ženska ali skupina) je bila že dolgo pred vzpostavitvijo Bitcoina ena od kriptografskih navdušencev, kot so računalničarji in hekerji, ki so sodelovali v razpravah glede iskanja učinkovitih rešitev za zamenjavo sistema fiatnih valut.



Oktobra 2008 je Nakamoto predstavil revolucionarno belo knjigo z naslovom »Bitcoin: A Peer-to-Peer Electronic Cash System« (Bitcoin: elektronski gotovinski sistem enakovrednih partnerjev) na kriptografskem e-poštnem seznamu. Ta dokument je postavil temelje decentraliziranega protokola enakovrednih udeležencev, namenjenega opravljanju varnih spletnih transakcij brez posrednikov.

Nakamotova vizija je bila jasna – ustvariti različico elektronskega denarja izključno enakovrednih udeležencev, ki ne bi bila nadzorovana s strani vplivnih vlad in finančnih ustanov.



Nakamoto je 3. januarja 2009 izvedel rudarjenje prvega bloka Bitcoina, znanega kot »izvirni blok« (angl. genesis block). To je bil uradni začetek vzpostavitve omrežja Bitcoin – novega denarnega sistema, ki je temeljil na zaupanju in varnosti na podlagi decentralizirane glavne knjige. V mesecih in letih, ki so sledila, se je tej ideji začelo pridruževati vedno več somišljenikov, ki so prispevali k njeni uresnitvi.

## Blok geneze Bitcoina

Surova šestnajstiška različica

```
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 ....f19z{.2c>
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....a.B.A~SQ2:Y,a
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA K.*J)*_IY...+|
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C .....YfYfM.Yf..
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....EThe Times 03/
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Jan/2009 Chancel
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D ..lor on brink of
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F second bailout f
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C or banksYfYf..o.
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 *....CA.g5YpUH'
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 .gn|q0-.A0'(A9!
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 ybâ0.ab*10k?L10K
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 óU.â.â.â\0M+0..W
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 80 39 09 A6 SLP+kh_-....
000000F0 79 42 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4
00000100 F3 55 04 B5 1E C1 12 DE 5C 38 4D F7 BA 0B BD 57
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00
```

Leta 2011, ko smo bili priča uspešnemu delovanju omrežja Bitcoin brez njegovega vplivnega ustvarjalca, je Nakamoto sporočil svojemu kolegu razvijalcu Bitcoina, da se bo umaknil iz sveta Bitcoina in prihodnost prepustil drugim »strokovnjakom«, ki delijo njegovo vizijo.

Čeprav Nakamotova identiteta še danes ostaja uganka, pa razlog za vzpostavitev Bitcoina nikoli ni bil skrivnost. Nakamoto ga je ustvaril z namenom, da bi odvezel moč peščici posameznikov in jo vrnil v roke množici z uvedbo alternativne rešitve v obliki decentraliziranega, odprtokodnega in preglednega denarnega sistema, v katerem je denar ločen od države. Vzpostavitev Bitcoina je bil Nakamotov odziv na finančno krizo leta 2008, ki je prizadela običajne ljudi po svetu, hkrati pa znova omogočila kopičenje bogastva eliti. Bil je Nakamotov odziv na korupcijo in krhkost sistema fiatnih valut. Nakamoto je postavil temelje za novo revolucijo in se od nje umaknil, namesto da bi si pripisal zasluge.

# Uvod v Bitcoin

V letih, ki so sledila, se je Bitcoin začel hitro razvijati in uveljavljati kot simbol upanja, opolnomočenja ter odpornosti, saj se je zoperstavil sistemu fiatnih valut in zagotovil varen način opravljanja finančnih transakcij, odpornih na cenzuro. Bitcoin je odprtokodni protokol, kar pomeni, da nihče ni njegov lastnik ali nadzornik. Njegova zasnova je javna in odprta za vsakogar.

Nakamotove sanje o brezmejnem, preglednem in varnem finančnem sistemu živijo naprej in spodbujajo današnjo globalno revolucijo svobode. Običajno ljudje vsakodnevno izstopajo iz sistema fiatnih valut in vstopajo v svet Bitcoina. Zagovorniki svobodnega odločanja so v regijah po vsem svetu ustanovili Bitcoinova središča – tako imenovane Bitcoinove krožne ekonomije. Tudi države, ki iščejo alternativno pot, kot je Salvador, začenjajo sprejemati Bitcoin.

## 6.1 Kako deluje Bitcoin?

### 6.1.1 Mehanizem Nakamotovega soglasja

Kako deluje Bitcoin? Bitcoin ima številne funkcije in še zdaleč nismo odkrili vseh. Na srečo pa ga lahko začnete uporabljati tudi, če ne razumete vseh podrobnosti njegovega delovanja.

Enako velja za uporabo interneta: Večina ljudi ne ve, kako deluje protokol TCP/IP, vendar kljub temu vsak dan pošiljajo e-pošto in sporočila ter objavljajo vsebine s svojimi računi v družabnih omrežjih. Enako velja za vožnjo avtomobila – večina ljudi ne ve točno, kako deluje avtomobil, vendar ga znajo voziti.



Vendar Bitcoin še ni splošno sprejet. Še vedno se smatra za dokaj novo tehnologijo, kot je bil internet v 90. letih prejšnjega stoletja. Zato želimo njegove osnove predstaviti na preprost, manj tehničen način.

Glavno misel delovanja Bitcoina lahko strnemo v enem stavku: Bitcoin je dogovor med ljudmi v spletu. Podoben je igranju družabne igre s prijatelji. Pri igri, kot je Monopoli, se z ostalimi igralci strinjate glede upoštevanja določenih pravil. Eno od pravil Monopolija je, da so sprejeti samo posebni bankovci. Če Janez (eden od igralcev) krši pravila in za nakup hiše namesto bankovcev Monopolija uporabi na primer toaletni papir, mu bodo drugi igralci rekli, da goljufa, in bodo preprosto prenehali igrati z njim. Če želite igrati igro, je potrebno doseči soglasje glede pravil in jih upoštevati, sicer ste zavrneni.

Na tak način deluje tudi Bitcoin. Bitcoin je omrežje ljudi, ki uporabljajo ista pravila. Ta pravila so matematična, zapisana v računalniški kodi in neposredno sprejeta s strani vseh, ki uporabljajo programsko opremo Bitcoin. Pravila Bitcoina veljajo za vse udeležence enako, kar pomeni, da vsi upoštevajo pravila igre ali pa ne morejo igrati, ker jih omrežje zavrne.

Eno od pravil Bitcoina je na primer to: »Nikoli ne bo na voljo več kot 21 milijonov bitcoinov.« Če bi kdo želel ustvariti milijon dodatnih bitcoinov zase, mu to ne bi koristilo, saj bi ga vsi ostali samodejno identificirali in zavrnil. Prav zaradi tega je Bitcoin tako robusten.



Ali ste vedeli, da se je Bitcoin od leta 2009 ubranil pred več kot deset tisoč poskusi vdora, ponarejanja ali spreminjanja? Bitcoin je dokazal, da ga nihče ne more ustaviti, nadzorovati ali manipulirati z njim.



Ni pomembno, kdo ste ali od kod prihajate – če vstopate v svet Bitcoina, morate upoštevati enaka pravila kot vsi drugi.

To velja tudi za vse posameznike in entitete, ki razpolagajo z veliko mero nadzora in vpliva v fiatnem sistemu. V svetu Bitcoina ni prostora za goljufije ali sabotaže – vsi so obravnavani enako in tega ne more spremeniti nihče.



# Uvod v Bitcoin

## 6.1.2 Glavni akterji

Za boljše razumevanje decentralizacije Bitcoina moramo pridobiti vpogled v različne vloge v omrežju. V Bitcoinu imajo različni udeleženci različne, a usklajene vloge, ki prispevajo k nemotenemu delovanju omrežja.

### 1. Rudarji: arhitekti varnosti

Rudarji so hrbtenica omrežja Bitcoin. To so ljudje oziroma skupine ljudi, ki v ozadju vzdržujejo in varujejo omrežje z mehanizmom, imenovanim dokaz o delu (angl. proof-of-work, PoW). Ti posamezniki uporabljajo posebne visokozmogljive računalnike. Njihova strojna oprema je na voljo v omrežju Bitcoin, kjer iščejo kompleksne kriptografske številke, preverjajo transakcije in dodajajo nove bloke informacij o transakcijah v Bitcoinovo decentralizirano glavno knjigo (imenovano blockchain oz. veriga blokov). Njihova predanost zagotavlja nespremenljivost glavne knjige in zaščito pred zlonamernimi napadi.



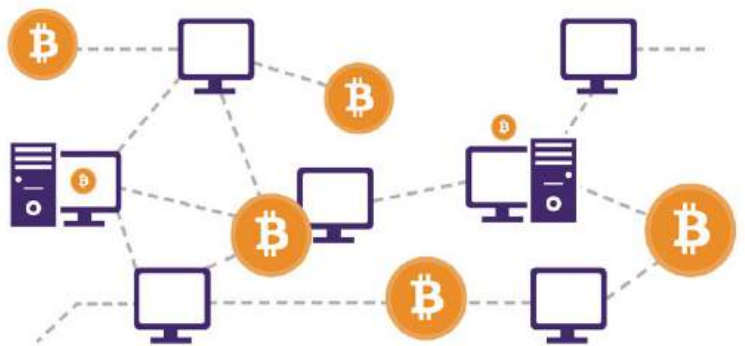
Decentralizirana narava rudarjenja omogoča sodelovanje vsakomur, ki ima na voljo ustrezne računalniške vire. Rudarji, ki najhitreje rešijo uganko, so za svoje trdo delo nagrajeni z bitcoini.

Rudarji bitcoinov delujejo po vsem svetu, s čimer varujejo omrežje pred centralizacijo ter zagotavljajo robustnost in porazdeljenost Bitcoina.

### 2. Vozlišča: varuhi preverjanja veljavnosti

Bitcoinova vozlišča so običajni ljudje tega planeta. Ti udeleženci so varuhi omrežja Bitcoin, saj v svojih računalnikih uporabljajo programsko opremo Bitcoin, v kateri hranijo kopijo celotne glavne knjige. Vozlišča potrjujejo transakcije in zagotavljajo, da vsi udeleženci delujejo v skladu s pravili soglasja.

Zaradi deljenja odgovornosti preverjanja veljavnosti v omrežju vozlišč ostaja Bitcoin odporen proti napadom in ohranja svojo naravo brez potrebe po zaupanju. Vozlišča imajo ključno vlogo pri ohranjanju integritete glavne knjige in prispevajo k decentralizaciji Bitcoina.





### 3. Uporabniki: opolnomočeni udeleženci

Uporabniki – gonilna sila omrežja Bitcoin – so posamezniki, ki izvajajo transakcije. Uporabniki so običajni ljudje, ki živijo svoja življenja, ki pa so se opolnomočili z uvedbo Bitcoina. Nekateri uporabniki na primer varčujejo svoj denar v bitcoinih, drugi, kot so državljani Salvadorja, pa ga uporabljajo kot plačilno sredstvo za nakup živil in valuto za prejemanje plače.

Bitcoin zagotavlja opolnomočenje uporabnikov, saj odpravlja potrebo po posrednikih, kot so banke in vlade, ter omogoča neposredne transakcije med enakovrednimi udeleženci. To pomeni tudi, da imajo uporabniki popoln nadzor nad svojim denarjem, kar jim omogoča nadzorovanje sredstev in transakcij.

### 4. Razvijalci in projekti: arhitekti inovacij

Denarni sistem prihodnosti ni zgrajen sam od sebe, niti ni sprejet globalno na etično ustrezen način brez truda. Tu prevzamejo vaje Bitcoinovi razvijalci in projekti.

Razvijalci s svojim tehničnim strokovnim znanjem in izkušnjami zagotavljajo izboljšave in inovacije Bitcoinovega protokola. Ti posamezniki prispevajo kodo, predlagajo izboljšave in odpravijo ranljivosti, s čimer zagotovijo razvoj omrežja kot odziv na vse vrste izzivov. Odprtokodna narava Bitcoina spodbuja sodelovanje, saj lahko vsi razvijalci po svetu prispevajo k njegovi rasti.

Sama narava decentraliziranega razvoja preprečuje, da bi en sam subjekt prevzel nadzor nad protokolom. To je mogoče le s postopkom, ki temelji na doseganju soglasja. Razvijalci predlagajo zamisli in spremembe, skupnost pa podpre le tiste z najboljšimi zamislimi, ki so v skladu s širšo vizijo boljšega sveta, kar omogoča pregleden in demokratičen razvoj Bitcoina, dokler ta ne bo pripravljen za 8 milijard ljudi.

Bitcoinovi projekti vključujejo različne skupine – od neprofitnih organizacij in korporacij s poslanstvom do skupin in posameznikov, ki ustvarjajo dragoceno vsebino. Ti ljudje sodelujejo pri doseganju določenega cilja ali pa se na poti do kolektivne svobode osredotočajo na večje Bitcoinovo poslanstvo.

Bitcoinovi projekti imajo ključno vlogo pri oblikovanju in spodbujanju sprejetja Bitcoina ter si prizadevajo za zagotovitev prihodnosti, ki v ospredje postavlja opolnomočenje in svobodo človeške rase.

### Simfonija

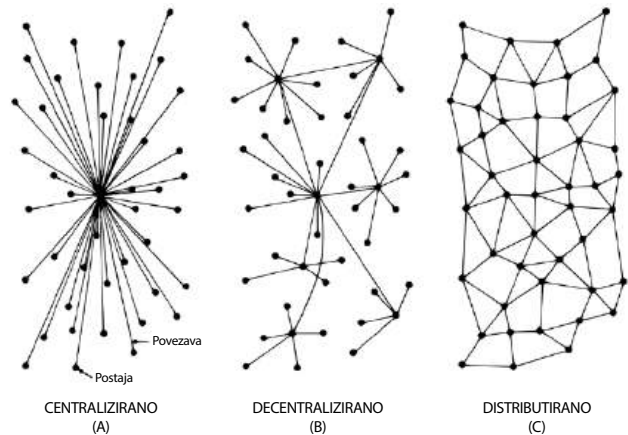
Decentralizacijo Bitcoina si lahko predstavljamo kot sinergijo glasbenega orkestra, v katerem posamezni različni glasbeniki skupaj ustvarjajo najlepšo glasbo. V omrežju Bitcoin ni vodje, temveč rudarji, vozlišča, uporabniki, razvijalci in projekti, ki opravljajo svoje vloge avtonomno in v sodelovanju.

Decentralizirana glavna knjiga, ki jo vzdržujejo vozlišča, zagotavlja preglednost, mehanizem dokaza o delu pa omogoča varnost in preprečuje centralizacijo rudarjenja. Uporabniki so finančno neodvisni in opolnomočeni ter osvobojeni okov nadzora sistema fiatnih valut. Razvijalci v skladu z doseganjem soglasja zagotavljajo prilagajanje protokola razvijajočim se potrebam človeštva. Bitcoinovi projekti s svojimi enoličnimi načini prispevajo k širšemu poslanstvu kolektivne svobode.

# Uvod v Bitcoin

Vsak udeleženec ima ključno vlogo pri oblikovanju sprejemanja Bitcoina in kreptvi vloge človeštva. Vsak udeleženec tega decentraliziranega sistema prispeva k zagotavljanju odpornosti in trajnosti Bitcoina ter ustvarjanju brezmejnega in opolnomočenega ekosistema, ki za delovanje ne potrebuje zaupanja.

Decentralizacija v omrežju Bitcoin je simfonija vizije Satoshija Nakamota in neizmerne strasti globalne skupnosti, ki si prizadeva zagotoviti svobodo in opolnomočenje.



## Vaja v razredu - doseganje soglasja v omrežju enakovrednih udeležencev



### Cilj

Razumeti, kako je doseženo soglasje v skupini, ter se seznaniti s kriptografijo in Bitcoinovo plastjo soglasja.



### Materiali

Sporočilo s šifriranimi in nešifriranimi navodili za dejanja (»napadi« ali »ne napadi«).



### Priprava vaje

Učitelj pred začetkom predavanja izbere skupino treh ali štirih učencev, ki bodo pri naslednji dejavnosti prevzeli vlogo zlonamernih vozlišč. Njihova domača naloga je, da do začetka predavanja rešijo kriptografsko uganko.

### Koraki vaje:

1

Učitelj bo izbral učenca »avtorja«, ki bo prejel sporočilo na listu papirja z besedo »NAPAD« in niz števil »4-16-14-21-1-21-21-1-3-11«.

2

Učenci se bodo postavili v krog, pri čemer mora učitelj zagotoviti, da so izbrani učenci, ki predstavljajo zlonamerna vozlišča, ločeni od ostalih zaradi zagotovitve večje učinkovitosti vaje.



3

Ko je skupina postavljena, avtor poda listek osebi na desni strani kroga.

4

Ko bodo vsi prebrali sporočilo, bo avtor dal znak skupini z besedo »zdaj«, skupina pa se bo hkrati odzvala na sporočilo. Če je v sporočilu zapisano »NAPAD«, bodo vsi udeleženci naredili korak naprej.

5

Po začetnem odzivu bodo nekateri učenci (tisti, ki so prejeli šifrirano sporočilo in ga pravilno interpretirali) ostali pri miru, medtem ko bodo drugi sledili prvotnim navodilom, kar nakazuje pomanjkanje soglasja.

### Zaključek:

Razpravljajte o tem, zakaj soglasje ni bilo doseženo, in predstavite koncept problema bizantinskih generalov, kako je povezan s potrebo po skupnem cilju, nato pa razpravljajte o tem, kako Bitcoin zagotavlja rešitev za to težavo.

# Uvod v Bitcoin

## 6.2 Bitcoin kot stabilni digitalni denar

### 6.2.1 Uvod

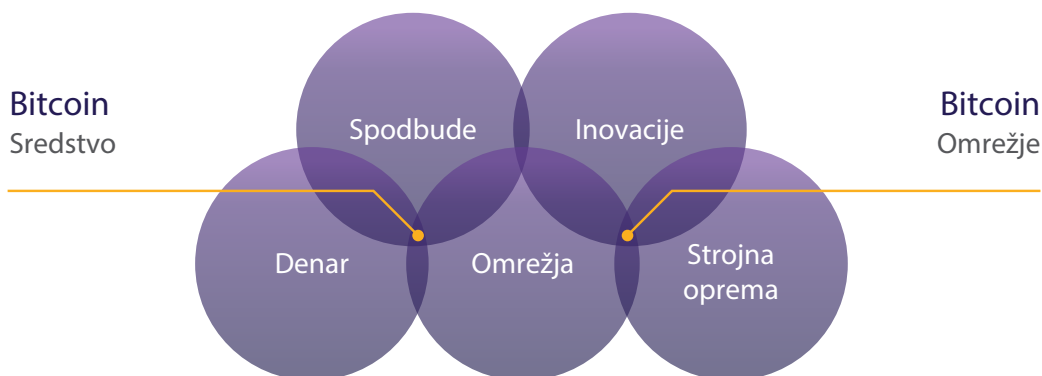
#### Dejavnost:

Oglejte si  
1,5-minutni  
video »What  
is Bitcoin?«  
(Kaj je  
Bitcoin?)



Preprosto povedano – Bitcoin je denar. Bitcoin ni naložba, temveč varen in učinkovit način varčevanja težko prisluženega denarja.

Z bitcoini ne boste obogateli, saj vam ne zagotavljajo donosa v obliki več bitcoinov. Vrednost bitcoina se v primerjavi s fiatno valuto povečuje zaradi njegovega obsežnega sprejemanja in razvrednotenja fiatnih valut.



Bitcoin je nova oblika denarja. Je internet denarja, kar pomeni, da se mu lahko pridruži kdor koli in začne izmenjevati vrednost z drugimi uporabniki. Tudi najbolj izolirane in revne skupnosti na svetu lahko dostopajo do denarnega sistema. Tako kot lahko vsak, ki ima telefon in internetno povezavo, uporablja mehanizem za iskanje, tudi Bitcoin omogoča dostop do novega globalnega denarnega sistema vsem, ki imajo telefon in internetno povezavo.



Hitrejša in  
cenejša  
plačila

Denar lahko pošljete kamor koli že v nekaj minutah in po izjemno nizkih provizijah.



Finančna  
vključenost

2,5 milijarde ljudi, ki nimajo bančnega računa, lahko dostopa do denarja prek telefona ali računalnika.



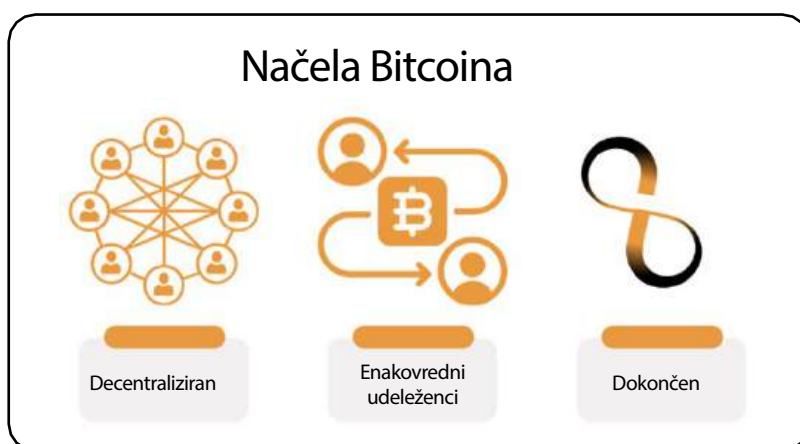
Večja  
zasebnost

Bitcoinove transakcije so javne, vaša identiteta pa je zasebna.

Bitcoin je popolnoma digitalna in brezmejna valuta. Ni pomembno, kje živite, saj je na voljo v računalnikih in pametnih telefonih po vsem svetu. Veliko uporabnikov po svetu uporablja programsko opremo Bitcoin in kopijo njene glavne knjige.

Verjetnost, da bi ta programska oprema in evidenca vseh transakcij izginila, je zelo majhna, saj obstaja nešteto njenih kopij. Če bi ju želeli izklopiti, bi morali za vedno izklopiti celoten internet, kar pa je zelo malo verjetno.

Bitcoin je redek, kar pomeni, da je razpoložljiva količina žetonov Bitcoin omejena. Ne more ga ponarediti nihče – niti najvplivnejše vlade in finančne ustanove.



### 6.2.2 Značilnosti Bitcoina

#### Razvoj stabilnega denarja

Kot je bilo predstavljeno v 2. poglavju, življenjski cikel stabilnega denarja vključuje tri faze, da je doseženo končno, splošno sprejetje s strani družbe: od začetnega hranilca vrednosti do menjalnega sredstva in nazadnje obračunske enote.

Prva faza denarja – hranilec vrednosti – je, ko se valuta začne skozi čas uveljavljati kot stabilno sredstvo (oziroma sredstvo, katerega vrednost se povečuje). Ljudje, ki zgodaj prepoznajo to fazo, poskušajo zaščititi svoje premoženje tako, da ga shranijo v tej obliki denarja, zlasti v času geopolitične in makroekonomske negotovosti.

Nekatere skupine, kot so mediji, Bitcoin opredeljujejo kot obliko »digitalnega zlata«. Bitcoin se je namreč v zadnjem desetletju uspešno uveljavil kot hranilec vrednosti. Vsak dan vse več ljudi dojema Bitcoin kot varovalo pred inflacijo, podobno, kot je bilo v preteklosti zlato.

Naslednja faza je utrditev prepričanja o stabilnosti valute. Takrat se valuta preoblikuje v menjalno sredstvo, ki omogoča transakcije v vsakdanjem življenju ljudi. V tej fazi postaja valuta splošno sprejeta za namene izmenjave blaga in storitev.

Bitcoin postopoma postaja menjalno sredstvo. S sprejemanjem valute s strani trgovcev in razvojem protokola postajajo njegove transakcije vse bolj učinkovito in vsakdanje sredstvo poslovanja. Primer tega je Salvador, kjer je Bitcoin uradno priznan kot zakonito plačilno sredstvo. Vsak dan ga vse več običajnih državljanov in podjetij uporablja kot menjalno sredstvo.

# Uvod v Bitcoin



V končni fazi valuta pridobi status obračunske enote, ki služi kot skupno merilo za določanje cen blaga in storitev. Na tej stopnji prevzame vlogo standardne metrike za merjenje vseh drugih vrednosti.

Pot do uveljavitve kot obračunske enote pa je dolgoročnejši proces. Blago in storitve so po svetu trenutno merjeni samo v fiatnih valutah, zato mora biti Bitcoin sprejet s strani širše javnosti ter biti vključen v različne finančne sisteme. So pa temelji že postavljeni, saj podjetja in posamezniki že razmišljajo o uporabi in denominiranju vrednosti v Bitcoinu.



Kot lahko vidite, je Bitcoin na dobri poti v tem evlucijskem ciklu stabilnega denarja. Ko bo Bitcoin v celoti integriran v globalni finančni sistem, lahko postane standardna obračunska enota in preoblikuje celoten globalni denarni sistem.

### Lastnosti denarja

Kot je bilo opisano v 2. poglavju, je človeštvo sčasoma prišlo do spoznanja, da mora imeti pravi stabilni denar določene lastnosti, da je lahko učinkovit. Te lastnosti so trajnost, deljivost, prenosljivost, sprejemljivost, redkost in zamenljivost.

Oglejmo si lastnosti Bitcoina.

**Trajnost:** Bitcoin je v celoti digitalna valuta in je zato popolnoma trajna.

**Deljivost:** fiatna valuta euro je deljiva na cente (0,01). Bitcoin pa je deljiv na tako imenovane satoshije ali satse (0,00000001). Ker pa je Bitcoin digitalen, ga bo mogoče v prihodnosti še dodatno razdeliti, če bo to potrebno. Trenutno je najbolj deljivo denarno sredstvo na svetu.

**Prenosljivost:** aprila 2020 je bilo v zgolj nekaj minutah prenesena 1,1 milijarda dolarjev, stroški transakcije pa so znašali le 68 centov. Noben drug način plačevanja ne omogoča tako hitrega, samostojnega in nizkostroškovnega prenosa tako velikih količin denarja. Zato je Bitcoin najlažje prenosljiva oblika denarja na svetu.

**Sprejemljivost:** Bitcoin je še vedno v zgodnji fazi svojega uveljavljanja kot menjalno sredstvo in v primerjavi s fiatnimi valutami je trenutno njegova sprejemljivost nizka.

**Redkost:** na voljo bo le 21 milijonov bitcoinov. V skladu s kodo je nemogoče, da se ta vrednost kadar koli poveča, kar pomeni, da Bitcoin ni le redek, ampak tudi najbolj redko denarno sredstvo na svetu.

**Zamenljivost:** vsaka enota bitcoina je enaka kateri koli drugi enoti in jo je mogoče zamenjati ter prenesti prek Bitcoinovega protokola na podlagi enakih vrednosti, zato je zamenljiva valuta.

# Uvod v Bitcoin

## Bitcoin, zlato in USD

Lastnosti denarja	Zlato	Fiatna valuta	Bitcoin
Trajnost	Visoka	Zmerna	Visoka
Prenosljivost	Zmerna	Visoka	Visoka
Deljivost	Zmerna	Zmerna	Visoka
Zamenljivost	Visoka	Visoka	Visoka
Redkost	Zmerna	Nizka	Visoka
Redkost	Zmerna	Zmerna	Visoka
Zgodovinska uveljavljenost	Visoka	Zmerna	Nizka
Odpornost na cenzuro	Zmerna	Zmerna	Visoka
Pametnost/programabilnost	Nizka	Zmerna	Visoka

»Bitcoin, zlato in dolar«, revija Bitcoin Magazine, <https://bitcoinmagazine.com>

Bitcoin je vrsta pametnega denarja, ki je programabilen, ga ni mogoče odvzeti in ima vse lastnosti, zaradi katerih je odličen za varčevanje ter preprost za trgovce, ki želijo opravljati hitre transakcije.






Ker gre za pregledno glavno knjigo, je Bitcoin lahko zelo učinkovito sredstvo za odkrivanje goljufij in prepoznavanje tveganj v svojih storitvah. Ima dobre lastnosti zlata, kot je omejena količina, hkrati pa tudi prednosti fiatnih valut, saj je deljiv in preprosto prenosljiv. Poleg tega se ponaša z novimi funkcijami, ki so izjemno učinkovite v digitalnem svetu.

Kaj menite vi? Bitcoin še ni splošno priznan in sprejet – vendar ali je stabilni denar?



Dejavnost: razprava v razredu – ali je Bitcoin stabilni denar?

Zdaj, ko smo si podrobneje ogledali Bitcoin, si ponovno oglejmo primerjalno tabelo denarja iz 2. poglavja, kjer je na voljo primerjava Bitcoina z drugimi oblikami denarja:

Značilnosti dobrega denarja	 Krave	 Cigarete	 Diamanti	 Evri	 Bitcoin
Trajnost					
Prenosljivost					
Zamenjljivost					
Sprejemljivost					
Redkost					
Deljivost					
Skupaj					

### 6.2.3 Sprejemanje osebne odgovornosti

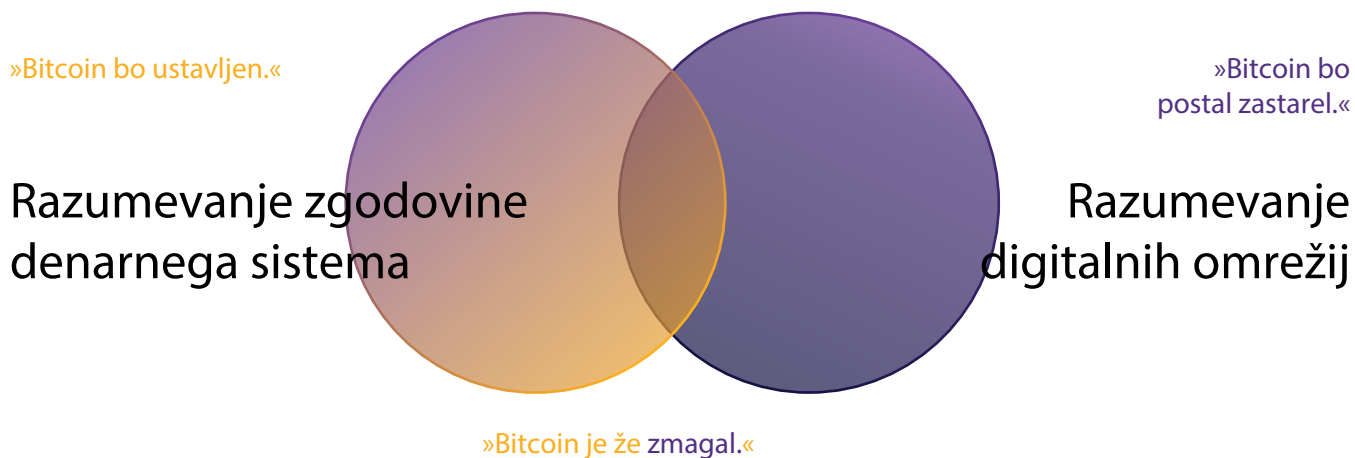
Rezultat je porazdeljen sistem brez osrednje točke, kjer bi lahko prišlo do napake. Uporabniki imajo kriptografske ključe za dostop do svojega denarja in opravljajo transakcije neposredno drug z drugim, pri čemer je s pomočjo omrežja enakovrednih udeležencev preverjana morebitna dvojna poraba.

Satoshi Nakamoto

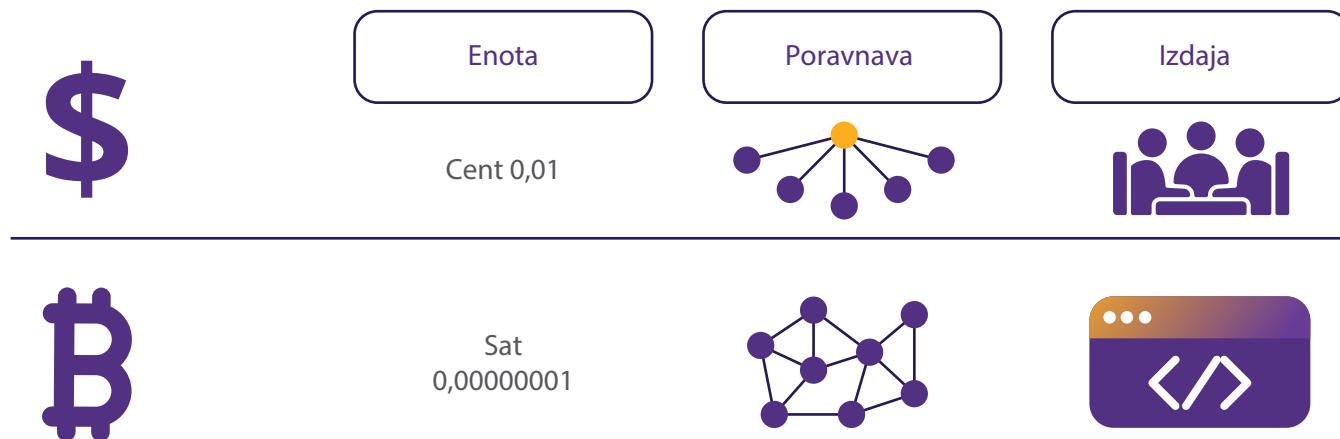
# Uvod v Bitcoin

V svetu fiatnih valut se ljudje zanašajo na vlade, banke in uveljavljene ponudnike plačilnih storitev. Vodje teh (finančnih) ustanov določajo pravila omrežja, udeleženci – večinoma običajni državljani – pa morajo ta pravila spoštovati. Ni pomembno, kje živite – vedno obstaja nabor standardnih postopkov z navodili, kaj morate narediti. Sčasoma je to privedlo do težav, zlasti za družine, ki se spopadajo z vse večjimi izzivi vsakdanjega življenja.

Ta sistem sili ljudi k temu, da svojo finančno odgovornost prenašajo v roke drugih. Večina ljudi se na primer zanaša na pomoč drugih, zlasti v primeru težav (na primer izguba dostopa do bančnega računa).



Denarni sistem Bitcoina je zelo drugačen. Bitcoin deluje na poseben način, kjer je vodje nadomestil avtonomni sistem pravil. Ni avtokrata ali vodje, kar pomeni, da vam nihče ne narekuje, kaj morate narediti. Če želite izkoristiti novo odkrito svobodo in zmogljivost Bitcoina, morate pridobiti vpogled v njegovo delovanje in integrirati tehnologijo na način, ki vam najboljše ustreza.



Bitcoin vam omogoča popoln nadzor nad svojimi sredstvi, vendar pa ta nadzor prinaša tudi večjo odgovornost. Če na primer izgubite dostop do svojih bitcoinov, ker izgubite ključ digitalne denarnice, to pomeni, da ste trajno izgubili vse svoje prihranke. Na voljo ni linije za pomoč strankam, kamor bi lahko poklicali, ali strokovnjaka, na katerega bi se lahko obrnili – če imate težave, jih morate odpraviti sami.

Na srečo pa se to ne bo zgodilo ljudem, ki so se odločili prevzeti polno odgovornost nad svojim življenjem. Uporaba omrežja Bitcoin ni zapletena, gre le za nov koncept. Nelagodje je posledica nepoznavanja – če pa ste se pripravljene naučiti uporabljati Bitcoin in v celoti prevzeti odgovornost nad varovanjem svojega premoženja, postane Bitcoin orodje za nadzorovanje premoženja, ki vam ga nihče ne more zaseči.

Ključ do uspeha je v ukrepanju, razumevanju delovanja Bitcoina in njegovem sprejetju v skladu z vašimi enoličnimi potrebami in življenjsko filozofijo. Temu sledi uporaba bitcoinov z vzpostavitvijo Bitcoinove denarnice, pošiljanjem in prejemanjem prvih transakcij ter pregledom najboljših varnostnih praks.



## 7. poglavje

# ***Kako uporabljati Bitcoin***

### 7.0 Uvod

### 7.1 Pridobivanje in izmenjava bitcoinov

#### 7.1.1 P2P: fizično

#### 7.1.2 P2P: spletno

#### 7.1.3 Centralizirane borze

### 7.2 Uvod v Bitcoinove denarnice

#### 7.2.1 Samoskrbniške in skrbniške denarnice

#### 7.2.2 Različne vrste Bitcoinovih denarnic

#### 7.3.3 Odprta in zaprta koda

Dejavnost: ocenjevanje Bitcoinovih denarnic v razredu

### 7.3 Namestitev mobilne Bitcoinove denarnice

Dejavnost: namestitev/obnovitev Bitcoinove denarnice

### 7.4 Prejemanje in pošiljanje transakcij

Dejavnost: potek Bitcoinove transakcije

### 7.5 Varčevanje v bitcoinih

### 7.6 Ne zaupaj, preveri

# Kako uporabljati Bitcoin

## 7.0 Uvod

Zakaj bi kdo raje zaupal piflarskemu denarju namesto centralnobančnemu denarju? Internet so ustvarili piflarji. Banke pa so ustvarile veliko depresijo.

Andreas M. Antonopoulos

Zdaj, ko ste pridobili vpogled v to, kaj je Bitcoin in kakšen je njegov namen, je čas, da se ga naučite uporabljati v praksi. V tem poglavju vas bomo po korakih vodili skozi postopek pridobivanja bitcoinov, raziskali različne razpoložljive vrste denarnic, vam pomagali namestiti lastno Bitcoinovo denarnico ter celo vadili pošiljanje in sledenje Bitcoinove transakcije v omrežju. Čas je, da pridobljeno znanje uporabite v praksi!

## 7.1 Pridobivanje in izmenjava bitcoinov

Bitcoin lahko pridobite na več načinov. Naredite lahko naslednje:

- ☀ prejemanje plačila v bitcoinih v zameno za svoje delo ter plačevanje izdelkov in storitev drugih ljudi z bitcoini (več o tem v 8. poglavju),
- ☀ Rrdarjenje bitcoinov (več o tem v 9. poglavju),
- ☀ zamenjajte svojo fiat valuto za bitcoine ali pa zamenjajte svoje bitcoine za fiat valuto v spletu,



V nadaljevanju si bomo ogledali izmenjavo fiat valute za bitcoine in obratno, in sicer z najpogostejšimi možnostmi – osebnimi transakcijami ter spletnimi metodami.

### 7.1.1 Enakovredni udeleženci: osebno

Transakcije enakovrednih udeležencev (P2P) za pridobivanje in prodajo bitcoinov vključujejo neposredno izmenjavo fiatne valute (ali drugega blaga oziroma storitev) za bitcoine z drugim posameznikom, pri čemer v transakcijo ni treba vključiti banke ali drugega udeleženca.

Oba udeleženca sporazumno določita znesek in menjalni tečaj. Kupec zagotovi denar, prodajalec prenese bitcoine in transakcija je zaključena. Čeprav izmenjavo P2P lažje opravite fizično z osebnim srečanjem posameznika v resničnem svetu, pa jo lahko izvedete kjer koli prek interneta. Postopek izmenjave bitcoinov za fiatno valuto vključuje podobne korake, vendar v obratni smeri.



### 7.1.2 Enakovredni udeleženci: spletno

Vstopite v okolje platform P2P, kjer se kupci in prodajalci bitcoinov srečujejo v kibernetnem prostoru in opravljajo transakcije brez posrednikov, neposredno v internetu.

V takšnih platformah ni treba nikomur zaupati svojih podatkov ali denarja – srečujete se lahko z drugimi udeleženci in z njimi neposredno trgujete.



V večini platform P2P morajo enakovredni udeleženci del sredstev deponirati, da zagotovijo izpolnitev svojega dela dogovora. Deponirati pomeni, da denar hranite na varnem mestu, ki ga nadzoruje platforma, dokler oba udeleženca ne naredita, kar sta obljubila. Podobno, kot če bi zaupanja vreden prijatelj hranil vaše stvari, dokler vsi udeleženci ne izpolnijo dogovora.

### 7.1.3 Centralizirane borze

Uporaba centraliziranih borz je morda najlažji način za pridobivanje in prodajo bitcoinov, vendar pa vključuje tudi znatne kompromise. Centralizirane borze so podjetja, ki strankam omogočajo nakup in prodajo bitcoinov neposredno prek njih. Vendar pa ima ta priročnost tudi svojo ceno.



# CENTRALIZIRANO

#### Centralizirane borze in njeni kompromisi

Pomembno je vedeti, da morate pri nakupu bitcoinov prek centralizirane borze pogosto navesti osebne podatke in preveriti svojo identiteto. To predstavlja tveganje za krajo identitete in izpostavlja vaše osebne podatke morebitnim grožnjam. Poleg tega centralizirane borze hranijo bitcoine za vas, kar pomeni, da nimate nadzora nad svojim denarjem, dokler ga ne dvignete z njih.

Centralizirane borze lahko prav tako zlorabijo sredstva uporabnikov ali posodijo več bitcoinov, kot jih imajo na zalogi, dokler ne pride do zloma. Podobno kot banke! V svetu Bitcoina ni centralne banke, ki bi reševala goljufive banke s tiskanjem dodatne valute, saj ni mogoče natisniti več bitcoinov!

# Kako uporabljati Bitcoin

## 7.2 Uvod v Bitcoinove denarnice

V nasprotju s fizičnim denarjem bitcoini niso dejansko v Bitcoinovi denarnici. Na voljo so v distribuirani glavni knjigi, ki jo omrežje Bitcoin nenehno preverja in varuje. Kako lahko postanete lastnik bitcoinov?

Lastništvo bitcoinov lahko pridobite le, če ste lastnik zasebnih ključev, s katerimi lahko podpisujete transakcije in prenašate lastništvo bitcoinov na drugo osebo. Ta postopek imenujemo pošiljanje bitcoinov.

Oglejmo si dva pojma, ki ju uporabljamo skupaj z izrazom »denarnica«:

- ✿ Glavni zasebni ključ (kot geslo) – ključ, s katerim lahko ustvarjate javne ključe in jih posredujete drugim osebam za namene prejemanja in pošiljanja bitcoinov.
- ✿ Mobilni ali namizni vmesnik – vmesnik, kjer lahko komunicirate z omrežjem Bitcoin, dostopate do svojega stanja bitcoinov, pošiljate in prejimate transakcije ter jih oddajate v omrežje. Različne vrste denarnic, skupaj z njihovimi prednostmi in kompromisi, so opisane v naslednjem poglavju.






### 7.2.1 Samoskrbniške in skrbniške denarnice

Preden si podrobneje ogledamo različne vrste Bitcoinovih denarnic in njihove značilnosti, moramo najprej razlikovati med samoskrbniškimi in skrbniškimi denarnicami, kot je prikazano v spodnji tabeli. Predstavljene so prednosti in tveganja uporabe posameznih vrst denarnic ter kdo nadzoruje bitcoine v njih. Izraz »samoskrbniški« pomeni, da ima uporabnik zasebne ključe in je s tem tudi resnični lastnik svojih bitcoinov, medtem ko ima v skrbniški denarnici njegove bitcoine v lasti tretja oseba.

Vrsta denarnice	Kdo nadzoruje moje bitcoine?	Prednosti	Tveganja
Samo-skrbniške denarnice	Uporabnik	Popoln nadzor nad sredstvi in transakcijami, ni postopka odobritve ali zamrznitve računa, ni korporativnega ali vladnega nadzora, zaščita pred arbitrarno zaplenbo, podobno hranjenju denarja doma.	Obnovitev ni mogoča, če izgubite obnovitveno frazo, manj podpore strankam, celotna odgovornost je na strani uporabnika.
Skrbniške denarnice	Ponudnik	Preprosta obnovitev v primeru izgube dostopa, lažja podpora strankam.	Sredstva so vedno povezana z internetom, zato so te denarnice bolj ranljive za vdore in kršitve varnosti. Skrbniki nadzorujejo račune in jih lahko zamrznejo.



V samoskrbniški denarnici (imenovani tudi neskrbniška denarnica) imate ključke za dostop do denarnice samo vi, kar vam zagotavlja popoln nadzor nad vsemi sredstvi, ki pritekajo vanjo in odteka iz nje. V skrbniški denarnici pa je lastnik ključa nekdo drug, ki lahko v vašem imenu dostopa do njene vsebine in jo upravlja.

-  Samoskrbništvo je podobno lastništvu banke. Transakcij ne nadzoruje nobena vlada ali podjetje, kar pa pomeni, da ste v celoti odgovorni za varnost svojih bitcoinov.
-  Samoskrbništvo preprečuje, da bi tretje osebe zasegle bitcoine brez vašega soglasja.
-  Samoskrbništvo zagotavlja brezskrbnost v času negotovosti, saj veste, da so vaši bitcoini na varnem.

Pomembno je izbrati ustrezno vrsto denarnice za potrebe vsakega posameznika. Včasih ljudje težko prepoznajo razliko med samoskrbniško in skrbniško denarnico. V spodnji tabeli so opisane razlike v postopku namestitve.

Vrsta denarnice	1. korak: Izberite denarnico	2. korak: Namestite denarnico	3. korak: Ustvarite novo denarnico	4. korak: Zavarujte semensko frazo	5. korak: Začnite uporabljati denarnico
Samo-skrbniške denarnice	Izberite ponudnika samoskrbniške denarnice	Upoštevajte navodila ponudnika denarnice	Generirajte obnovitveno frazo in najmanj en <b>zasebni ključ</b>	Obnovitveno frazo shranite na varno mesto	Začnite uporabljati denarnico za prejemanje in pošiljanje <b>bitcoinov</b>
Skrbniške denarnice	Izberite ponudnika skrbniške denarnice	Upoštevajte navodila ponudnika denarnice	Ustvarite račun pri ponudniku denarnice	Ni na voljo ( <b>zasebne ključke</b> ima ponudnik denarnice)	Začnite uporabljati denarnico za prejemanje in pošiljanje <b>bitcoinov</b>



## NISO TVOJI KLJUČI NISO TVOJI KOVANCI

»Niso tvoji ključki, niso tvoji kovanci« je priljubljeni rek med imetniki bitcoinov. Gre za idejo, da niste resnični lastnik kovancev, če nimate neposrednega nadzora nad zasebnimi ključki.

Kdor koli dostopa do vaših zasebnih ključev, postane lastnik vaših bitcoinov. Zato je izjemno pomembno, da jih zaščitite in varujete pred radovedneži. V nadaljevanju knjige je predstavljenih nekaj načinov, kako lahko to naredite.

Ogledali si bomo samoskrbniške denarnice, kjer je uporabnik lastnik svojih ključev in ima popoln nadzor nad svojimi bitcoini.

Ne skrbite, če je videti zapleteno ali če ne razumete vsega – ko boste začeli uporabljati Bitcoin, boste pridobili tudi dodatno znanje.

# Kako uporabljati Bitcoin

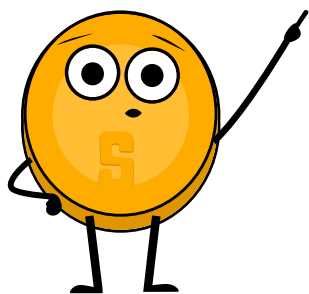
## 7.2.2 Različne vrste Bitcoinovih denarnic

Za Bitcoinove denarnice običajno uporabljamo različna imena, odvisno od tega, kje ustvarite oziroma hranite zasebni ključ. Če so ključi shranjeni v pametnem telefonu, to imenujemo mobilna denarnica. Če so ključi varno shranjeni v namenski napravi, to imenujemo strojna denarnica. Če je ključ shranjen samo kot zapis na papirju, to imenujemo papirnata denarnica.

Različna imena za Bitcoinove denarnice,  
glede na njihovo strukturo:

Vrsta denarnice	Opis	Prednosti	Slabosti	Predvideni uporabniki
Spletna denarnica	Denarnica, dostopana prek spletnega brskalnika.	Dostopno v kateri koli napravi z internetno povezavo. Preprosto za uporabo.	Manj varna. Lahko pride do vdora ali ogroženosti.	Osebe, ki morajo pogosto dostopati do svoje denarnice in nimajo veliko sredstev za hranjenje.
Mobilna denarnica	Denarnica, nameščena v mobilni napravi.	Priročna. Do nje lahko dostopate kjer koli.	Če izgubite napravo, jo nekdo ukrade ali vdre vanjo, lahko izgubite denarnico.	Osebe, ki želijo opravljati transakcije na poti in nimajo veliko sredstev za hranjenje.
Namizna denarnica	Denarnica, nameščena v namiznem računalniku.	Bolj varna kot spletne denarnice. Lahko jo uporabljate brez povezave.	Če je računalnik okužen z zlonamerno programsko opremo, lahko pride do vdora v denarnico.	Osebe, ki želijo hraniti večjo količino <b>bitcoinov</b> in uporabljajo namizni računalnik.
Strojna denarnica	Fizična naprava za hranjenje <b>bitcoinov</b> brez povezave.	Zelo varna. Lahko jo uporabljate brez povezave.	Če izgubite napravo ali jo nekdo ukrade, sredstev morda ne boste mogli povrniti.	Osebe, ki želijo hraniti večjo količino <b>bitcoinov</b> in so pripravljene plačati za dodatno varnost strojne denarnice.
Papirnata denarnica	Fizični zapis zasebnih in javnih ključev Bitcoinove denarnice.	Zelo varna. Lahko jo uporabljate brez povezave.	Če je fizični zapis ukraden ali izgubljen, lahko izgubite denarnico oziroma vam jo nekdo ukrade.	Osebe, ki želijo hraniti večjo količino <b>bitcoinov</b> in so pripravljene sprejeti dodatne previdnostne ukrepe za zagotovitev varnosti.








Ker lahko ključne prenašate iz ene naprave v drugo, »stanje« Bitcoinove denarnice ni dokončno. Če na primer ustvarite ključne Bitcoinove denarnice v računalniku in jih pozneje prenesete v telefon, postane »namizna denarnica« »mobilna denarnica«.



Ko govorimo o hranjenju bitcoinov, ne govorimo le o tem, kdo jih nadzoruje, ampak moramo upoštevati tudi številna druga tveganja. Zato je pomembno izbrati varno in priročno rešitev za hranjenje.

Ko boste analizirali kompromise različnih vrst denarnic, boste prišli do spoznanja, da ni na voljo popolne denarnice, ki bi zadovoljila vse potrebe.

### Pri izbiri Bitcoinove denarnice morate upoštevati več dejavnikov

-  **Varnost:** prepričajte se, da ima denarnica vzpostavljene zmogljive varnostne ukrepe, kot so dvojno preverjanje pristnosti in pravilniki o varnih geslih.
-  **Zasebnost:** upoštevajte, ali denarnica omogoča anonimnost ali pa za nastavitev računa zahteva osebne podatke.
-  **Preprosta uporaba:** izberite denarnico, ki je preprosta za uporabo in krmarjenje, zlasti če šele vstopate v svet Bitcoina.
-  **Združljivost:** prepričajte se, da je denarnica združljiva z vašo napravo in operacijskim sistemom.
-  **Provizije:** primerjajte provizije različnih denarnic, da si zagotovite najboljšo ponudbo.
-  **Ugled:** raziščite ugled denarnice in njene ekipe ter se prepričajte, da je zaupanja vredna.
-  **Nadzor:** nekatere denarnice omogočajo večji nadzor nad zasebnimi ključi, kar je lahko varnostna prednost.

Razmislite o tem, ali želite namestiti denarnico, ki omogoča popoln nadzor, ali pa denarnico, ki je uporabniku prijaznejša, vendar vam zagotavlja manjši nadzor.

### 7.2.3 Odprta in zaprta koda

Še en pomemben dejavnik, ki ga morate upoštevati pri izbiri Bitcoinove denarnice, je, ali gre za odprtokodno aplikacijo oziroma programsko opremo.

Odprta koda je zelo pomembna, saj omogoča skupnosti pregledovanje kode in nadaljevanje razvoja projekta, če ekipa neha delati na njem.

# Kako uporabljati Bitcoin



Tako kot je Bitcoinova koda popolnoma odprta, da jo lahko vsak pregleduje, uporablja in spreminja, mora biti odprta tudi koda denarnice, ki jo uporabljate za hranjenje svojih bitcoinov.

Dejavnost: razprava v razredu in ocenjevanje  
Bitcoinovih denarnic na spletnem mestu  
[bitcoin.org](https://bitcoin.org)

Obiščite to spletno mesto:

<https://bitcoin.org/en/choose-your-wallet> in uporabite novo pridobljeno znanje o  
Bitcoinovih denarnicah, da izberete najboljšo denarnico na podlagi danes  
obravnavanih meril.

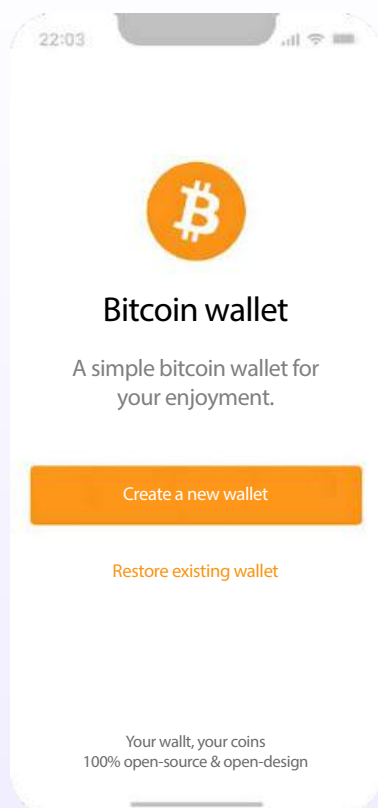


## 7.3 Namestitev mobilne Bitcoinove denarnice

Zdaj, ko smo pridobili vpogled v Bitcoinove denarnice in razlike med njimi, si bomo ogledali njihovo uporabo v praksi. Ustvarili bomo mobilno denarnico v pametnem telefonu.

### Dejavnost: namestitev/obnovitev Bitcoinove denarnice

Če učenci nimajo mobilnih telefonov, naj jim jih zagotovi učitelj. Za to dejavnost sta na voljo dve možnosti.



### Vaša semenska fraza

Vaša semenska fraza se uporablja za generiranje in obnovo računa.

- |             |           |           |
|-------------|-----------|-----------|
| 1. issue    | 2. flame  | 3. sample |
| 4. lyrics   | 5. find   | 6. vault  |
| 7. announce | 8. banner | 9. cute   |
| 10. damage  | 11. civil | 12. goat  |

Teh 12 besed si zapišite na list papirja. Vrstni red je pomemben. S tem semenom boste lahko obnovili svoj račun.

### Vaja v razredu: 1. možnost – prenesite novo denarnico.

Kako ustvariti in uporabljati Bitcoinovo denarnico:

- 1 Aplikacijo poiščite v trgovini App Store (iOS) ali Google Play Store (Android).
- 2 Odprite aplikacijo in vnesite oziroma generirajte 12- ali 24-besedno obnovitveno frazo (včasih imenovana tudi semenska fraza). Ne pozabite si jo zapisati in shraniti na varnem mestu! S to obnovitveno frazo lahko po potrebi obnovite popoln dostop do svojih sredstev.

Če je dostop do denarnice onemogočen in izgubite ali pozabite to zaporedje besed, ne morete dostopati do svojih bitcoinov.

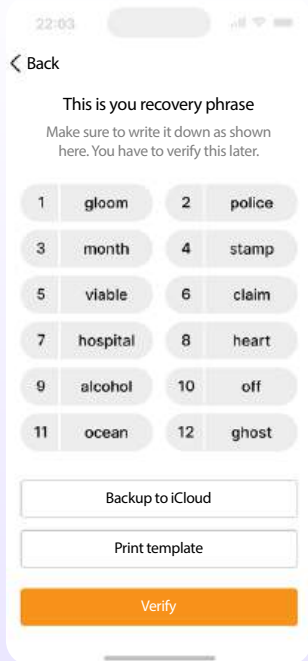
- 3 Nato morate potrditi, da ste shranili obnovitveno ali semensko frazo. Pri tem morate v enakem vrstnem redu vnesti besede semenskega fraze.
- 4 Nekatere denarnice vam omogočajo, da izberete varno geslo kot dodaten varnostni ukrep. Denarnica samodejno ustvari vaš zasebni ključ in prvi Bitcoinov naslov.

Predstavljajte si, da je javni ključ vaš e-poštni naslov, ki ga želite posredovati drugim, da vam lahko pošljejo bitcoine, oziroma v tem primeru, da je e-poštni naslov vaša e-pošta.

Predstavljajte si, da je zasebni ključ vaše geslo za e-pošto, ki pa ga ne želite deliti z nobeno osebo, saj bi ji s tem omogočili dostop do vaše e-pošte.

- 5 Za prejemanje bitcoinov uporabite naslov za prejemanje. Prenesite bitcoine v denarnico. S samoskrbniško denarnico ne morete vedno kupiti bitcoinov s fiatno valuto, zato jih boste morda morali najprej kupiti in prenesti z borze.

# Kako uporabljati Bitcoin



Vaja v razredu: 2. možnost – obnovite denarnico (časovno omejeno).

Prenesite Bitcoinovo denarnico in vsakemu učencu dodajte nekaj satoshijev.

Vsakemu učencu dajte list s semensko frazo za prevzem denarnice.

Učence vodite korak za korakom

- 1 Ob prvem zagonu denarnice so na voljo trije načini ustvarjanja denarnice – pritisnite [Import an existing wallet] (Uvozi obstoječo denarnico). Ko se prikaže pozdravni zaslon, pritisnite [Restore with recovery phrase] (Obnovi z obnovitveno frazo).
- 2 Vnesite 12/18/24-besedno obnovitveno frazo v pravilnem vrstnem redu.
- 3 Ko končate, se dotaknite možnosti [Restore] (Obnovi).
- 4 Ko je postopek uvoza denarnice uspešno dokončan, se prikaže sporočilo »Import Successful« (Uvoz je bil uspešen).

## 7.4 Prejemanje in pošiljanje transakcij

Bitcoinova transakcija je prenos lastništva obstoječih bitcoinov na novega lastnika. Vendar pa namesto prenosa dejanskih kovancev vsa vozlišča v omrežju posodobijo svojo lokalno kopijo javne knjige s spremembo lastništva.

Pri pošiljanju Bitcoinove transakcije pošiljatelj s svojim enoličnim zasebnim ključem podpiše sporočilo, s čimer omrežju sporoči, da je lastništvo bitcoinov spremenjeno na naslov prejemnika.

Bitcoin so zdaj vezani na naslov, s katerega lahko pošilja le novi lastnik, s čimer postane lastnik bitcoinov.

GLAVNA KNJIGA

Lastnik računa	Vrednost
Peter	2.50
Anže	3.00
Maks	6.00
Matej	1.50
Robert	2.00
Helena	1.75
David	5.25

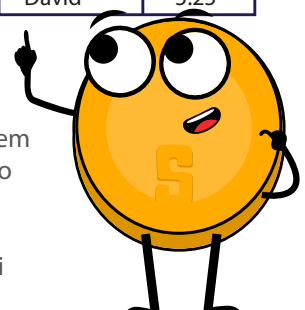
Sporočilo o zahtevi za izvedbo Bitcoinove transakcije  
Matej pošlje 0,50 BTC Heleni  
Matej → Helena 0.50 BTC

GLAVNA KNJIGA

Lastnik računa	Vrednost
Peter	2.50
Anže	3.00
Maks	6.00
Matej	1.00
Robert	2.00
Helena	2.25
David	5.25

Nove Bitcoinove transakcije so inicializirane v denarnicah po svetu, vendar ni osrednjega plačilnega procesorja. Namesto tega rudarji po vsem svetu tekmujejo pri zapisovanju transakcij v glavno knjigo.

Matej na primer dolguje Nini 0,5 BTC in ji želi vrniti denar. Oba imata digitalni denarnici.



- 1 Nina posreduje Mateju svoj naslov.
- 2 Matej s programsko opremo denarnice ustvari transakcijo, ki vključuje Ninin naslov, znesek za prenos (0,5 BTC) in provizijo za rudarja.
- 3 Po podpisu transakcije, je ta oddana v omrežje, kjer jo preverijo vozlišča. Vozlišča preverijo veljavnost transakcije in zagotovijo, da ima Matej na voljo zadosti sredstev. Če jih nima, je transakcija takoj zavrnjena.
- 4 Ko je transakcija preverjena, jo rudarji dodajo v verigo blokov, sredstva pa so prenesena na Ninin naslov.
- 5 Nina lahko nato s svojim zasebnim ključem dostopa do prenesenih sredstev v svoji denarnici.

Pomembno je vedeti, da transakcije ni mogoče razveljaviti, ko je enkrat zaključena.

### Kako poteka Bitcoinova transakcija



### Prejemanje Bitcoinovih transakcij:



Če želite prejeti bitcoine, morate pošiljatelju posredovati naslov Bitcoinove denarnice. To je enoličen niz črk in števil, ki predstavlja vašo denarnico in se uporablja za njeno identifikacijo v omrežju Bitcoin. Naslov denarnice najdete tako, da se prijavite v Bitcoinovo denarnico in poiščete možnost za »prejem« ali »depozit« bitcoinov.

Bitcoinov naslov lahko pošiljatelju posredujete na več načinov:

- 1 Kopirajte in prilepite naslov: naslov lahko kopirate tako, da ga označite in na tipkovnici pritisnete »Copy« (Kopiraj), nato pa ga prilepite v e-pošto ali sporočilo pošiljatelju.
- 2 Posredujte povezavo do svoje Bitcoinove denarnice: nekatere omogočajo ustvarjanje povezave do denarnice, ki jo lahko posredujete pošiljatelju. S klikom povezave lahko pošiljatelj dostopa do vaše denarnice in pošlje bitcoine.
- 3 Posredujte kodo QR: če ima pošiljatelj pametni telefon z aplikacijo Bitcoinove denarnice, lahko skenira kodo QR in pridobi vaš Bitcoinov naslov.

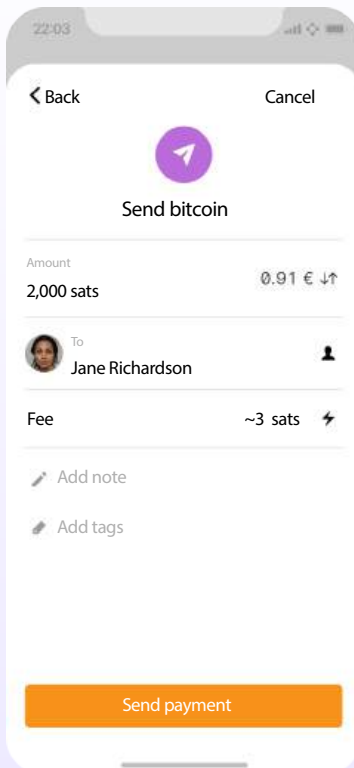


# Kako uporabljati Bitcoin

Ko pošiljatelj pridobi vaš Bitcoinov naslov, lahko pošlje bitcoine tako, da vnese vaš naslov in znesek, ki vam ga želi poslati, ter inicializira transakcijo. Bitcoini so nato poslani v vašo denarnico in so prikazani, ko je transakcija potrjena v omrežju Bitcoin. Ta postopek običajno traja nekaj minut.

Spodaj je predstavljen postopek pošiljanja Bitcoinovih transakcij.

## Pošiljanje Bitcoinovih transakcij:



Za pošiljanje bitcoinov potrebujete Bitcoinovo denarnico, Bitcoinov naslov prejemnika in znesek bitcoinov, ki ga želite poslati.

- 1 Odprite Bitcoinovo denarnico. Na vašo telefonsko številko bo preko SMS poslana koda, ki jo morate vnesti v pogovorno okno. Če ste omogočili Googlovo dvojno preverjanje pristnosti, morate vnesti šestmestno kodo iz aplikacije Google Authenticator.
- 2 Pomaknite se do funkcije »Send« (Pošlji) ali »Withdraw« (Dvigni) in kopirajte naslov prejemnika.
- 3 Vpišite Bitcoinov naslov prejemnika tako, da ga prilepite v polje »To« (Za).
- 4 V polje »Amount« (Znesek) vnesite znesek bitcoinov, ki ga želite poslati.
- 5 Preverite naslov prejemnika in znesek, ki ga želite poslati.
- 6 Preden kliknete »Confirm and Send« (Potrdi in pošlji), znova preverite podrobnosti transakcije in se prepričate, da pošiljate ustrezen znesek bitcoinov na pravi naslov denarnice.
- 7 Potrdite transakcijo in počakajte, da je transakcija potrjena tudi v omrežju.

Zdaj veste, kako ocenite, izberete in nastavite samoskrbniško Bitcoinovo denarnico. Pošiljanje bitcoinov iz ene denarnice v drugo v omrežju Bitcoin se imenuje pošiljanje transakcije v verigi. Transakcija namreč poteka v glavni verigi blokov omrežja Bitcoin. Tiste, ki so del verige so najvarnejši način poslovanja z bitcoini, vendar so dražje in počasnejše od drugih možnosti, ki so predstavljene v 8. poglavju.

## Dejavnost: potek Bitcoinove transakcije





Cilj: razumevanje osnovnih konceptov in mehanizmov Bitcoinove transakcije med enakovrednimi udeleženci.

Preden začnemo, si oglejmo glavne udeležence v Bitcoinovi transakciji:

- pošiljatelji in prejemniki so udeleženci, ki želijo med seboj opravljati transakcije,
- vozlišča potrdijo transakcije in shranijo celotno kopijo verige blokov. \*Lahka vozlišča omogočajo potrjevanje transakcij, pri tem pa uporabljajo manj prostora za shranjevanje in manj računalniških virov,
- rudarji so odgovorni za dodajanje novih transakcij v verigo blokov.



Preučite svojo vlogo. Dodeljena vam je bila ena od teh vlog: pošiljatelj, prejemnik, vozlišče ali rudar.




-  pošiljatelji bodo odgovorni za ustvarjanje in oddajanje transakcij,
-  prejemnik bodo odgovorni za prejemanje in preverjanje transakcij,
-  vozlišča bodo odgovorna za potrjevanje transakcij,
-  rudarji bodo odgovorni za dodajanje transakcij v verigo blokov.

**Vozlišča in prejemniki morajo preveriti transakcije**

 **1** Kot pošiljatelj: ustvarite transakcijo.



Če želite ustvariti transakcijo, upoštevajte naslednje korake: vzemite potrdilo o transakciji in zapišite število kovancev, ki jih želite poslati, ter ime oziroma začetnice prejemnika. Potrdilo podpišite s svojim imenom ali začetnicami, kar predstavlja vaš zasebni ključ. Prejemniku izročite potrdilo o transakciji in ustrezno število kovancev.

 **2** Kot prejemnik: za preverjanje transakcij ste odgovorni sami. Izvedite te korake:

-  preverite, ali je na potrdilu o transakciji zapisano pravilno število kovancev in prejemnikovo ime oziroma njegove začetnice,
-  preštete prejete kovance in jih primerjate s številom kovancev, navedenih na potrdilu,
-  če se število kovancev ujema, potrdite polje za odobritev. Če se število kovancev ne ujema oziroma imate pomisleke, transakcijo zavrnite.

Poslanih kovancev	Pošiljatelj	Podpis pošiljatelja	Prejemnik	Datum in ura	Odobritev prejemnika

 **3** Kot vozlišče: preverite in potrdite transakcije. Za preverjanje veljavnosti transakcije ste odgovorni sami.

-  Preverite veljavnost naslova pošiljatelja in prejemnika.
-  Preverite, ali ima pošiljatelj na voljo dovolj sredstev za dokončanje transakcije in da transakcija ne vključuje dvojne porabe kovancev.

Poslanih kovancev	Pošiljatelj	Podpis pošiljatelja	Prejemnik	Datum in ura	Odobritev prejemnika

# Kako uporabljati Bitcoin

**4** Kot rudar: odgovorni ste za dodajanje transakcij v verigo blokov. Izvedite naslednje korake:

- preverite transakcije, ki so jih odobrili prejemniki in potrdila vozlišča,
- vrzite kocko in primerjajte številke z drugim rudarjem. Transakcija rudarja z manjšo številko bo dodana v verigo blokov,
- za svoj čas, energijo in trud boste prejeli točko. Ob koncu dejavnosti bo zmagal rudar z največjim številom točk.

Ko je transakcija dodana v verigo blokov, je ni mogoče spremeniti ali razveljaviti.

**5** Spremljajte stanje kovancev: med dejavnostjo spremljajte stanje kovancev tako, da štejete kovanec v digitalni denarnici.

Poslani kovanci	Pošiljatelj	Podpis pošiljatelja	Prejemnik	Datum in ura	Odobritev

**6** Z razredom razpravljajte o ugotovitvah.

## 7.5 Varčevanje v bitcoinih

Bitcoin zagotavlja zaščito denarja pred inflacijo in nadzorom kogar koli, vendar morate to izvesti pravilno. Varčevanje v bitcoinih je sredstvo za hranjenje, kopičenje in ustvarjanje bogastva skozi čas. Kot je bilo že povedano, je vrsta denarja, ki ga želite prihraniti, ena najpomembnejših odločitev v življenju. S pametno izbiro si lahko zagotovite boljšo prihodnost zase in za svojo družino.



**Brezskrbnost:** če bitcoine hranite pravilno, je to edina oblika lastnine, ki vam je nihče ne more vzeti.

### 7.6 Ne zaupajte, ampak preverite

Pri izvajanju kakršnih koli opravil v Bitcoinu si zapomnite naslednje: »Ne zaupaj, preveri.« V Bitcoinu ni vodij. Nikoli ne sledite slepo trditvam drugih. Vedno bodite dvomljivi glede besed drugih in raje preverite sami. Z upoštevanjem tega načela se boste zaščitili pred izgubo svojih bitcoinov. To velja za trditev, kot je »naslednji Bitcoin« ali »naložbene priložnosti«, oziroma obljube o »hitrih in preprostih zasluških«.

V 7. poglavju ste pridobili pomembne informacije o uporabi Bitcoina v vsakdanjem življenju. Naučili ste se, kako na različne načine pridobiti in zamenjati bitcoine ter kako jih hraniti na varnem z uporabo različnih denarnic.

Z namestitvijo mobilne Bitcoinove denarnice in opravljanjem medsebojnih transakcij ste pridobili praktične izkušnje za samozavestno, vsakodnevno uporabo Bitcoina. Z razumevanjem Bitcoina kot načina varčevanja denarja ter širjenjem ideje »razišči sam (DYOR)« – »ne zaupaj, preveri« lahko zdaj nadzorujete svoj denar.

V naslednjem poglavju bomo raziskali omrežje Lightning Network. Ogledali si bomo, kako ta inovativna tehnologija spreminja način, kako ljudje po svetu dostopajo do denarja in ga uporabljajo. Izvedeli boste, kako ta omrežja posameznikom, skupnostim in podjetjem omogoča dostop do finančnih storitev – od vsakodnevnih transakcij do naprednejših aplikacij.



## 8. poglavje

# ***Lightning Network: vsakodnevna uporaba Bitcoina***

### 8.0 Uvod

**Dejavnost:** oglejte si videoposnetek »Bitcoin Lightning Network Explained«: How it Actually Works« (Vpogled v v Bitcoin Lightning Network: kako dejansko deluje)

### 8.1 Omrežje Lightning Network

### 8.2 Različne vrste denarnic Lightning

#### 8.2.1 Samoskrbniške in skrbniške denarnice

#### 8.2.2 Odprta in zaprta koda

### 8.3 Namestitev denarnice Bitcoin Lightning

### 8.4 Pošiljanje in prejemanje transakcij Lightning

**Dejavnost:** štafeta v denarnici Lightning

### 8.5 Nakup kave in živil z bitcoini

#### 8.5.1 V spletu: vtičniki za plačila – elektronsko poslovanje

#### 8.5.2 Osebno: poiščite trgovca v svojem območju

#### 8.5.3 Prehodna orodja: darilne kartice in plačilne kartice

#### 8.5.4 Krožne ekonomije in Bitcoin kot menjalno sredstvo

***Delovni zvezek za učence***

Slovenska različica | 2024

# Lightning Network: vsakodnevna uporaba Bitcoina

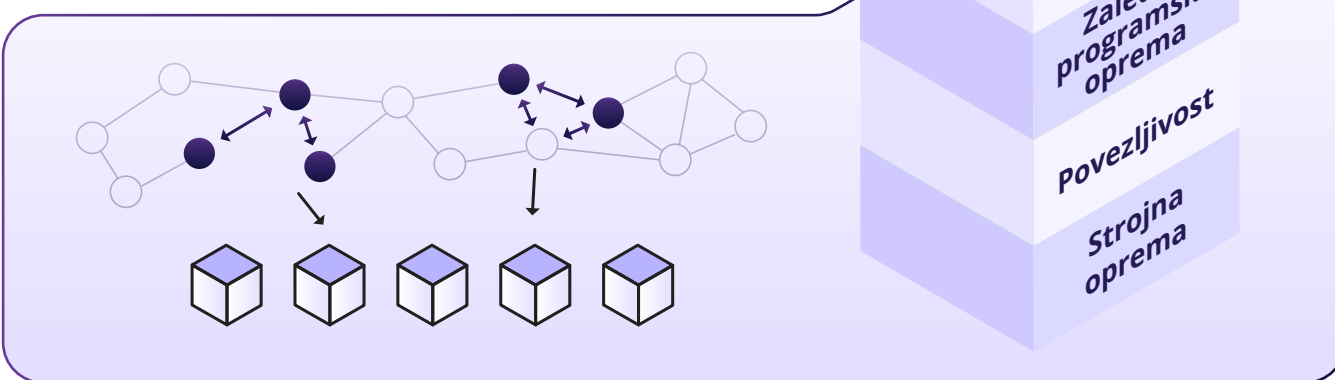
## 8.0 Uvod

Gradimo omrežje Visa za bitcoin. Vendar menim, da je za razliko od Vise zelo pomembno, da lahko na njem gradi vsakdo.

**Elizabeth Stark**

Tehnologije običajno rastejo in se širijo v plasteh, podobno kot skladovalnica. Pomislite na svoje najljubše spletno mesto, e-pošto ali družabna omrežja – zgrajeni so bili na podlagi internetnega protokola, ki je bil zgrajen na podlagi računalnikov, ki so bili zgrajeni na podlagi elektrike itd. Te tehnologije so se začele z zelo preprosto zasnovo in se sčasoma izboljšale.

Bitcoin ni izjema. Kot je dejal Andreas Antonopoulos: »Bitcoin je internet denarja.« To je osnovna plast stabilnega digitalnega denarja, ki predstavlja trdno podlago za graditev nove tehnologije.

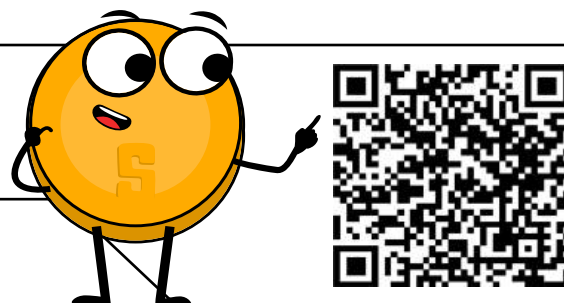


Ena od teh plasti se imenuje Lightning Network. To je kot superhitra avtocesta za bitcoine, ki omogoča hitro pošiljanje in prejemanje bitcoinov z zelo nizkimi provizijami. Uporabnikom omogoča takojšnje opravljanje majhnih transakcij v običajnem omrežju Bitcoin. Tako lahko preprosto in hitro kupite kavo ali pa izvedete plačilo prijatelju.

Ne pozabite: satoshi je kot najmanjši bitcoinov kovanec. Tako kot lahko evro razdelimo na cente, lahko en bitcoin razdelimo na manjše enote, imenovane satoshiji. En bitcoin je enakovreden 100 milijonom satoshijem, zato so satoshiji najmanjši delci vrednosti v sistemu Bitcoin. Ko bomo v tem poglavju govorili o pošiljanju bitcoinov prek omrežja Lightning Network, bomo to imenovali »pošiljanje satsov«, ki so manjši

Satoshi	Bitcoin
1	0,00000001
10	0,00000010
100	0,00000100
1.000	0,00001000
10.000	0,00010000
100.000	0,00100000
1.000.000	0,01000000
10.000.000	0,10000000
100.000.000	1,00000000

**Dejavnost:** oglejte si videoposnetek o omrežju Lightning Network



## 8.1 Omrežje Lightning Network

Lightning Network služi kot plačilni sistem, ki omogoča hitre in stroškovno učinkovite Bitcoinove transakcije. Deluje z vzpostavitvijo skupne denarnice, v kateri imata oba udeleženca nekaj bitcoinov. Opravljata lahko številne medsebojne transakcije, ne da bi morala posamezne transakcije zabeležiti v glavno knjigo. Ko so transakcije zaključene, je v glavno knjigo zabeležen končni saldo.



Omrežje Lightning Network je plačilni sistem, ki uporabnikom omogoča hitro ter cenovno ugodno pošiljanje in prejemanje plačil z bitcoin. Deluje na podlagi vzpostavitve skupne denarnice, v kateri oba udeleženca hranita svoje bitcoine, nato pa med seboj opravljata neomejene transakcije brez vključitve glavne verige blokov. Ko končata, je končno stanje zabeleženo v glavno verigo blokov.

Predstavljajte si, da morate izvesti nekaj opravil in za delovno mesto izberete kavarno. Ker veste, da boste tam preživeli cel dan, odprete račun in vnaprej plačate določen znesek, namesto da bi plačevali vsako naročilo posebej. Ko ste ob koncu dneva pripravljeni oditi, z lastnikom kavarne pregledate račun in poravnate končni znesek. Če ste plačali več, kot ste dejansko porabili, dobite nekaj denarja nazaj.

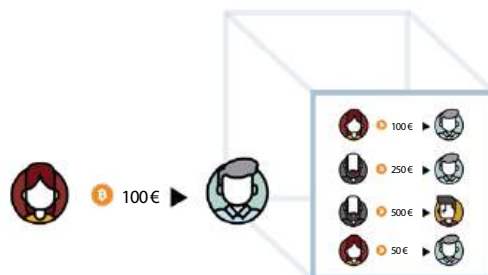
Zdaj pa si predstavljajte, da več tisoč ljudi hkrati počne isto stvar in omogoča drugim, da uporabljajo njihove račune za povezovanje z več ljudmi. To je omrežje Lightning Network.

Z omrežjem Lightning lahko izvajate plačila z vsemi ljudmi v omrežju in ne le z osebo, s katero imate skupni račun. Vaše plačilo lahko potuje po omrežju, dokler ne doseže cilja, tudi če s prejemnikom nimate odprtega kanala.

Oglejmo si razliko med transakcijami, ki so del verige (transakcije, opisane v 7. poglavju) in transakcijami, ki niso del verige (omrežje Lightning Network).

### Transakcije v verigi:

To so transakcije, ki se izvajajo neposredno v Bitcoinovi verigi blokov. Postopek njihovega izvajanja traja približno 10 minut, provizije pa so odvisne od velikosti transakcije v bajtih. So varnejše, vendar počasnejše.

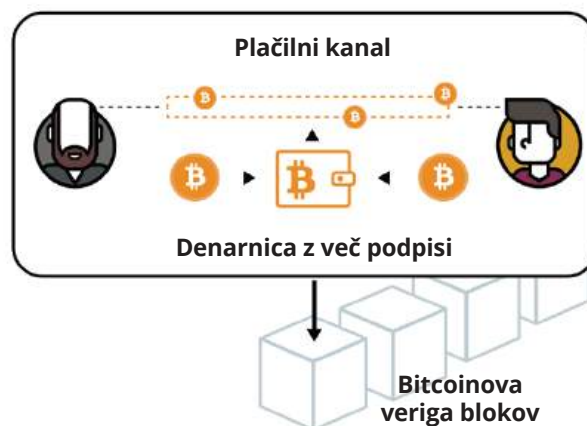


# Lightning Network: vsakodnevna uporaba Bitcoina

## Transakcije izven verige (omrežje Lightning Network)

Te transakcije potekajo v ločenem omrežju, ki je zgrajeno na Bitcoinovi verigi blokov. Transakcije so poravnane hitreje in z nižjimi provizijami.

Običajno se uporabljajo tam, kjer so podprte s predpisi in z zakoni ter kjer sta pomembnejša hitrost in stroški transakcij. V primerjavi s transakcijami v verigi so te transakcije manj varne.



Plačilno omrežje	Omrežje Bitcoin	Omrežje Lightning Network
Definicija	Decentralizirano digitalno omrežje, ki uporablja kriptografijo za zaščito finančnih transakcij.	Plačilni protokol druge plasti, ki temelji na Bitcoinovi verigi blokov in omogoča hitrejša ter cenejša transakcije.
Prednosti	Decentralizirano in varno. Brez povratnih plačil ali goljufij. Omogoča anonimno uporabo. Globalno sprejetje.	Hitrejša in cenejša transakcije. Večja skalabilnost. Transakcije izven verige ne zamašijo verige blokov.
Slabosti	Počasno izvajanje transakcij. Visoke provizije za nekatere vrste transakcij. Zapleteno za začetnike.	Zahteva zaupanje v upravitelja kanalov. Še vedno eksperimentalno in ni splošno sprejeto. Za odpiranje in zapiranje kanalov je potrebna transakcija v verigi.



## 8.2 Različne vrste denarnic Lightning

Denarnica Lightning se nekoliko razlikuje od Bitcoinove denarnice, čeprav ima enako funkcijo: prejemanja in pošiljanja bitcoinov. Razlika je v tem, da denarnica Lightning omogoča pošiljanje bitcoinov v omrežju Lightning Network, ki je druga plast na vrhu omrežja Bitcoin.

Podobno kot Bitcoinove denarnice, ki so bile predstavljene v prejšnjem poglavju, imajo tudi denarnice Lightning različne značilnosti, ki jih morate upoštevati, preden se odločite za eno od njih.

### 8.2.1 Samoskrbniške in skrbniške denarnice

Denarnice Lightning lahko razdelimo v zelo specifične kategorije, vendar jih bomo zaradi lažjega razumevanja razdelili v dve kategoriji: samoskrbniške in skrbniške denarnice.

Pri samoskrbniški denarnici Lightning velja, da ključne za dostop do denarnice nadzorujete vi, medtem ko pri skrbniški denarnici Lightning ključne nadzoruje nekdo drug – enako kot pri Bitcoinovih denarnicah.

Če uporabljate skrbniško denarnico, lahko dostopate samo do denarnice, vendar ste za dovoljenje za uporabo svojega denarja odvisni od nekoga drugega – zaradi priročnosti se odpovedujete lastništvu svojega denarja.

To je sprejemljivo za manjše zneske, ko pa pridobite boljše razumevanje te tehnologije, je priporočljiva uporaba samoskrbniške denarnice.

V nadaljevanju bo govora samo o samoskrbniških denarnicah Lightning.

### 8.2.2 Odprta in zaprta koda

Tako kot Bitcoinove denarnice, predstavljene v prejšnjem poglavju, so lahko tudi denarnice Lightning odprtokodne ali zaprtokodne. Vedno uporabljajte odprtokodne denarnice, saj so popolnoma odprte za pregled in jih preverja skupnost.

Odpertokodna aplikacija pomeni tudi, da lahko vsakdo prispeva k izboljšanju programske opreme, zato je za uporabnike boljša izbira.

## 8.3 Namestitev denarnice Bitcoin Lightning

Postopek namestitve samoskrbniške denarnice Bitcoin Lightning je enak kot postopek namestitve samoskrbniške denarnice v Bitcoinovi verigi.

# Lightning Network: vsakodnevna uporaba Bitcoina

Vaja v razredu – 1. možnost: prenesite novo samoskrbniško denarnico Lightning

## Kako ustvariti in uporabljati denarnico Bitcoin Lightning?

- 1 Aplikacijo poiščite v trgovini App Store (iOS) ali Google Play Store (Android).
- 2 Odprite aplikacijo in vnesite oziroma prepisite 12- ali 24-besedno obnovitveno frazo (včasih imenovana tudi semenska fraza). **Ne pozabite si jo zapisati in shraniti na varnem mestu!** S to obnovitveno frazo lahko po potrebi obnovite popoln dostop do svojih sredstev.

**Če je dostop do denarnice onemogočen in izgubite ali pozabite to zaporedje besed, ne morete dostopati do svojih bitcoinov.**

- 3 Nato morate potrditi, da ste shranili obnovitveno ali semensko frazo. Pri tem morate v enakem vrstnem redu vnesti besede semenskega fraze.
- 4 Nekatere denarnice vam omogočajo, da izberete varno geslo kot dodaten varnostni ukrep. Denarnica samodejno ustvari vaš zasebni ključ in prvi Bitcoinov naslov.
- 5 Ustvarite račun Lightning, naslov ali kodo QR za prejemanje bitcoinov. Prenesite bitcoine v denarnico. S samoskrbniško denarnico ne morete vedno kupiti bitcoinov s fiatno valuto, zato jih boste morda morali najprej kupiti in prenesti z borze.

**Vaša semenska fraza** Semenska fraza se uporablja za generiranje in obnovitev računa.

1 Issue

2 Flame

3 Sample

4 Lyrics

5 Find

6 Vault

7 Scissors

8 Banner

9 Cute

10 Damage

11 Civil

12 Goat

Teh 12 besed si zapišite na list papirja. Vrstni red je pomemben. S tem semenom boste lahko obnovili svoj račun.

Opomba: če uporabljate skrbniško denarnico, vam nekaterih korakov v razdelku 8.3 ni treba izvesti. Uporaba skrbniške denarnice je povezana s tveganjem, saj nimate nadzora nad svojim zasebnim ključem, kar pomeni, da nimate nadzora nad denarjem, ki ga hranite v denarnici.

Zdaj, ko ste namestili denarnico Bitcoin Lightning, si oglejmo postopek prejemanja in pošiljanja transakcij v omrežju Lightning ter tako se ta postopek razlikuje od postopka pošiljanja transakcij v verigi, opisanega v 7.

## 8.4 Pošiljanje in prejemanje transakcij Lightning

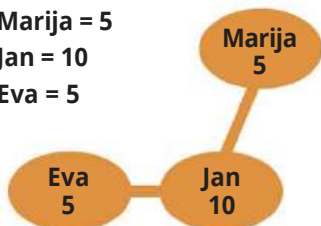
Z denarnico Lightning je uporaba Bitcoina hitra, cenovno ugodna in zasebna, kar zagotavlja preproste transakcije med dvema udeležencema. Bitcoine lahko hitro pošiljate in prejimate za vsakdanje stvari, kot je nakup kave ali drugih dobrin.

Oglejmo si nekaj primerov delovanja omrežja Lightning Network.

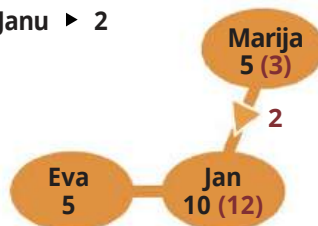
### 1. primer:

Marija in Eva imata vsaka po 5 enot valute. Marija želi poslati 2 svoji enoti Evi, zato pošlje 2 enoti Janu. Jan nato prenese 2 enoti Evi, ki ima zdaj 7 enot. Marija ima zdaj 3 enote. In to je to! Transakcija je opravljena.

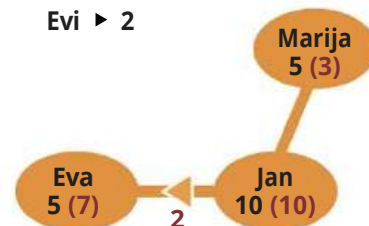
**Sprva**  
Marija = 5  
Jan = 10  
Eva = 5



**Od Marije**  
Janu ► 2



**Od Jana**  
Evi ► 2



Jan ima v tem scenariju, kjer si Marija in Eva ne zaupata neposredno, vlogo posrednika ali »zaupanja vredne tretje osebe«. Jan od Marije prejme 2 enoti in ju posreduje Evi, s čimer je transakcija zaključena. Z Janom kot posrednikom lahko Marija in Eva transakcijo opravita brez banke ali druge centralizirane ustanove, zaradi česar je transakcija hitrejša, cenejša in varnejša. Jan je ključni element v tem postopku transakcij med enakovrednimi udeleženci.



#### Transakcijske provizije

Jan za vsako transakcijo, ki gre skozi njegovo vozlišče, prejme majhno provizijo, kot nadomestilo za čas in trud, ki ju je vložil v vzdrževanje in vzpostavljanje vozlišča.



#### Sodelovanje v omrežju

Z vzpostavitev vozlišča Lightning Jan sodeluje v omrežju in pomaga povečati njegovo decentralizacijo, varnost in stabilnost. To lahko poveča ugled in verodostojnost Jana kot zanesljivega upravljalca vozlišča, s čimer postane bolj vabljen posrednik za prihodnje transakcije.

# Lightning Network: vsakodnevna uporaba Bitcoina



## Rast omrežja

Z rastjo omrežja Lightning Network in večanjem števila uporabnikov se bo število transakcij, ki potekajo skozi Janovo vozlišče, verjetno povečalo, kar lahko privede do večjega prihodka iz transakcijskih provizij.



## Večja varnost omrežja

Janova vloga posrednika pripomore k večji varnosti omrežja, saj vnese dodatno plast zaščite med Marijo in Evo. To lahko poveča zaupanje uporabnikov v omrežje, zaradi česar postane privlačnejše za nove uporabnike in pripomore k njegovi rasti. Na splošno lahko vloga upravljavca vozlišča v omrežju Lightning Network Janu zagotovi stalen vir dohodka in priložnost, da prispeva k rasti in razvoju omrežja.

Če povzamemo – **transakcije v verigi so počasnejše, vendar varnejše, medtem ko so transakcije izven verige (omrežje Lightning Network) hitrejše, vendar manj varne.** Glede na svoje potrebe morate razmisliti o kompromisu med varnostjo in hitrostjo.

## 2. primer:

Mina je ljubiteljica restavracije McDonald's – vsak dan gre tja na zajtrk, kosilo in večerjo. Vendar zaradi številnih različnih možnosti plačila, ki so na voljo, ni prepričana, katera je najboljša izbira. Na srečo se je naučila nekaj malega o Bitcoinu in omrežju Lightning Network. Po primerjavi spodnjih tabel je Mina prepričana, da je najboljša izbira plačilo v omrežju Lightning.

### Lightning Network in tradicionalni bančni sistem

Prednosti	Lightning	Tradicionalni bančni sistem
Hitrost	Hitro	Počasno
Preglednost	Pregledno	Nepregledno
Varnost	Varno	Ranljivo
Transakcijske provizije	Nizko	Visoko
Finančna vključenost	Visoko	Omejeno

Prednosti	Lightning	Tradicionalni bančni sistem
Skalabilnost	Visoko	Nizko
Zasebnost	Visoko	Zmerno
Interoperabilnost	Visoko	Nizko
Skladnost s predpisi	Zmerno	Visoko
Stroškovna učinkovitost	Visoko	Zmerno

Visa, Inc.



V povprečju 1.700 transakcij na sekundo.

Zmogljivost 65.000 transakcij na sekundo.

Bitcoin v verigi



Zmogljivost 7 transakcij na sekundo.

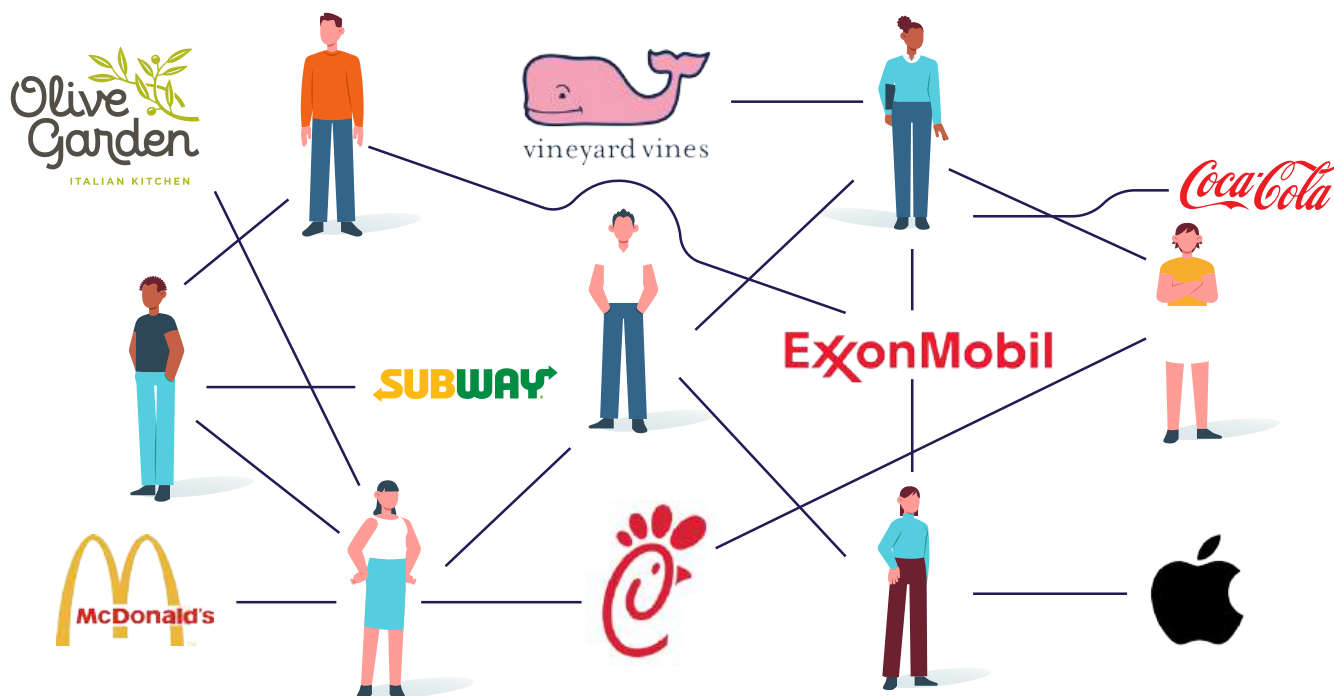
Bitcoin Lightning Network



Več milijonov transakcij na sekundo.

Mini so prav tako vseč hitre, varne in stroškovno učinkovite transakcije, zato se je odločila, da bo storitev v McDonaldsu plačala v omrežju Lightning. Z omrežjem Lightning lahko še bolj uživa v svojih obrokih, saj ve, da so njena plačila obdelana takoj, varno in z nizkimi provizijami. Ker Lightning Network zagotavlja finančno vključenost, lahko Mina zdaj plačuje obroke tudi, če je na primer na odročnem območju v Salvadorju.

Če želi Mina začeti uporabljati omrežje Lightning, najprej v svoj telefon prenese denarnico Lightning. Svojo denarnico nato napolni tako, da nanjo pošlje nekaj bitcoinov iz svoje običajne Bitcoinove denarnice. Ta postopek se imenuje »polnjenje denarnice« ali »polnjenje plačilnega kanala«. Mina lahko svojo denarnico napolni z želenim zneskom bitcoinov, vendar mora vedeti, da zneska bitcoinov, ki ga zaklene v denarnici Lightning, ne more uporabljati pri transakcijah v verigi.



Ko je njena denarnica Lightning napolnjena, jo lahko uporablja za plačevanje storitev v McDonaldsu.

McDonald's ima vozlišče Lightning, zato lahko Mina v njem odpre plačilni kanal tako, da nekaj svojih bitcoinov iz denarnice Lightning pošlje na poseben McDonaldsov naslov. S tem dejanjem prenese svoje bitcoine iz Bitcoinove verige blokov v transakcijo izven verige v omrežju Lightning.

Z odprtim plačilnim kanalom lahko Mina zdaj kupuje v McDonaldsu, ne da bi morala odpreti nov kanal ali vsakokrat plačati visoke provizije. Kanal je odprt, dokler ga Mina in McDonald's uporabljata. Če Mina na primer kupi hamburger za 0,0005 bitcoina, kanal spremlja Minino stanje, ki je zdaj 0,9995 bitcoina. Če naslednji dan kupi mlečni napitek za 0,0003 bitcoina, kanal zabeleži, da ima Mina zdaj na voljo 0,9992 bitcoina.

# Lightning Network: vsakodnevna uporaba Bitcoina

Ko se Mina odloči, da želi stanje svojih bitcoinov uporabiti za kaj drugega, zapre kanal tako, da v Bitcoinovo verigo blokov odda zaključno transakcijo. To naredi tako, da v svoji denarnici Lightning inicializira zaključno transakcijo, ki vsebuje končno stanje kanala, o katerem sta se dogovorila oba udeleženca. Transakcija je nato prenesena v Bitcoinovo verigo blokov, kjer jo potrdi rudar. Ko je transakcija potrjena, se kanal zapre, preostali bitcoini v kanalu pa so vrnjeni Mini in McDonaldsu.

Postopek zapiranja kanala lahko traja nekaj časa, saj mora biti potrjen v verigi blokov. V tem obdobju čakanja so sredstva še vedno zaklenjena v kanalu in jih ni mogoče uporabljati za izvajanje transakcij v verigi. Mina prejme obvestilo, ko je zaključna transakcija potrjena.

Zdaj, ko ste namestili denarnico Lightning in prebrali, kako uporabljate omrežje Lightning za pošiljanje transakcij, bomo izvedli dejavnost, kjer boste drugim učencem v razredu prek omrežja Lightning pošiljali satoshije (najmanjše enote bitcoina).



To je zemljevid celotnega sveta. V omrežju Lightning pošiljate satoshije kateremu koli uporabniku z denarnico Bitcoin Lightning. Plačilo je preneseno v nekaj sekundah in stane zgolj nekaj centov.

Preverite sami:





**Dejavnost: Vaja v razredu – štafeta v denarnici Lightning**

- 1** Najprej morate v telefon ali računalnik prenesti denarnico Lightning.
- 2** Sledite navodilom za namestitev denarnice v napravo v razdelku 8.3 tega poglavja.
- 3** Ko je denarnica nameščena, jo odprite in sledite navodilom za nastavitve. Morda boste morali ustvariti novo denarnico ali obnoviti obstoječo in jo zaščititi z geslom oziroma drugo obliko preverjanja pristnosti.
- 4** Ustvarite račun Lightning, naslov ali kodo QR za prejemanje bitcoinov.
- 5** Ko je vaša denarnica nameščena in lahko začnete prejemati satoshije, učitelj vam in vaši skupini nameni začetno količino satoshijev tako, da jih pošlje v vašo denarnico.



- A** Cilj vaše skupine je, da z uporabo omrežja Lightning Network prenašate satoshije iz denarnice ene osebe v denarnico druge osebe, dokler teh ne dobi zadnja oseba v skupini.
- B** Če želite poslati satoshije drugi osebi, odprite denarnico in sledite navodilom za izvedbo plačila. Zagotoviti morate prejemnikov račun Lightning ali skenirati kodo QR in vnesti znesek satoshijev, ki ga želite poslati.
- C** Če vaša skupina prva uspešno pošlje satoshije zadnji osebi, ste zmagali. (In lahko obdržite satse.)

**Pogovorite se o morebitnih težavah, ki jih je imela vaša skupina pri tej dejavnosti. Ali je bilo pošiljanje transakcije preprosto, hitro in cenovno ugodno? Ali menite, da je omrežje Lightning Network preprosto za uporabo in razumevanje?**

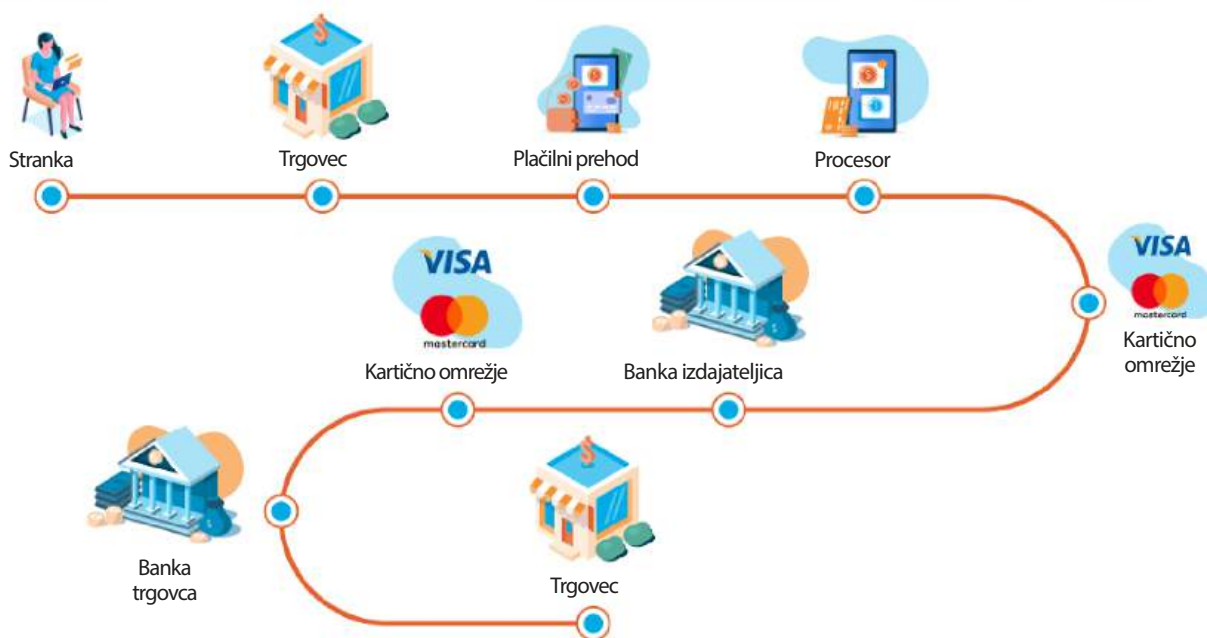
# Lightning Network: vsakodnevna uporaba Bitcoina

## 8.5 Nakup kave in živil z bitcoini

Ste se kdaj vprašali, ali bi lahko z bitcoini kupili jutranjo kavo oziroma vsakdanja živila? Odgovor je pritrdilen. Na voljo je veliko spletnih in osebnih storitev, ki omogočajo plačevanje z bitcoini. Raziskali bomo nekaj teh možnosti in orodij za lažje iskanje lokalnih trgovin, kjer lahko plačujete z bitcoini.

Čeprav se plačevanje s kreditno kartico ali aplikacijo zdi plačniku preprosto, pa je obdelava plačila v resnici zelo zapletena in vključuje več različnih udeležencev.

### Kako deluje procesiranje plačil



Pri nakupu dobrin sodeluje več udeležencev in vsak udeleženec zaračuna provizijo. Za lastnike trgovin so te provizije lahko zelo visoke – več kot 3 % cene, kar je zanje visok znesek.

Da niti ne omenjamo provizij za menjavo valut!



## Provizije za obdelavo plačil s kreditno kartico



Z Bitcoinom in omrežjem Lightning Network lahko podjetja prejemajo takojšnja plačila z vsega sveta prek odprtega, varnega, izvirno internetnega, brezmejnega in proti cenzuri odpornega denarnega sistema.

V nadaljevanju si bomo ogledali nekaj načinov, kako lahko trgovci preprosto prejemajo plačila v bitcoinih.

### 8.5.1 V spletu: vtičniki za plačila – elektronsko poslovanje

Strežnik BTCPay Server je odprtokodni plačilni procesor, ki trgovcem omogoča prejetje plačil v bitcoinih z malo tehničnega znanja. Je popolnoma brezplačen in ne zaračuna provizije.

**Spletna podjetja lahko strežnik BTCPay nemoteno integrirajo tako, da na svoje spletno mesto dodajo vtičnik BTCPay.**

#### Postanite lastni plačilni procesor.

The screenshot shows the BTCPay Server web interface. At the top, there are navigation tabs: SERVER SETTINGS, STORES, APPS, WALLETS, INVOICES, and PAY. The 'INVOICES' tab is selected, displaying a table of invoices.

Date	Orderid	Invoiceid	Status	Amount
4/12/2020 11:57:47 AM	M6QcV5Bh4pW7HJZC5q1tp		paid	\$2.00 (USD)
4/12/2020 11:57:37 AM	GGz21TH2mCwouUSWEN32		paid	0.01000000 BTC
4/12/2020 11:57:26 AM	KJwGou4Pv9gH8BvwhmgHf		new	120.00 € (EUR)
4/12/2020 11:57:15 AM	YU3W8LWUJdP3BjymSehof		new	\$5.00 (USD)
4/10/2020 11:52:52 AM	VYH4E7QWQ3K3N2mUTGf		expired	\$50.00 (USD)
4/6/2020 12:15:48 PM	5VhK3Ndyx2ZyPQ8hVQj84b		expired	\$10.00 (USD)



# Lightning Network: vsakodnevna uporaba Bitcoina

Ker je BTCPay Server odprtokodni projekt in ne podjetje, lahko k projektu prispevate, ko pridobite podrobnejše znanje o njem in računalniškem programiranju.

**Več informacij o uporabi plačilnega sistema BTCPay Server za osebno ali spletno poslovanje je na voljo na spletnem mestu <https://btcpayserver.org/>**



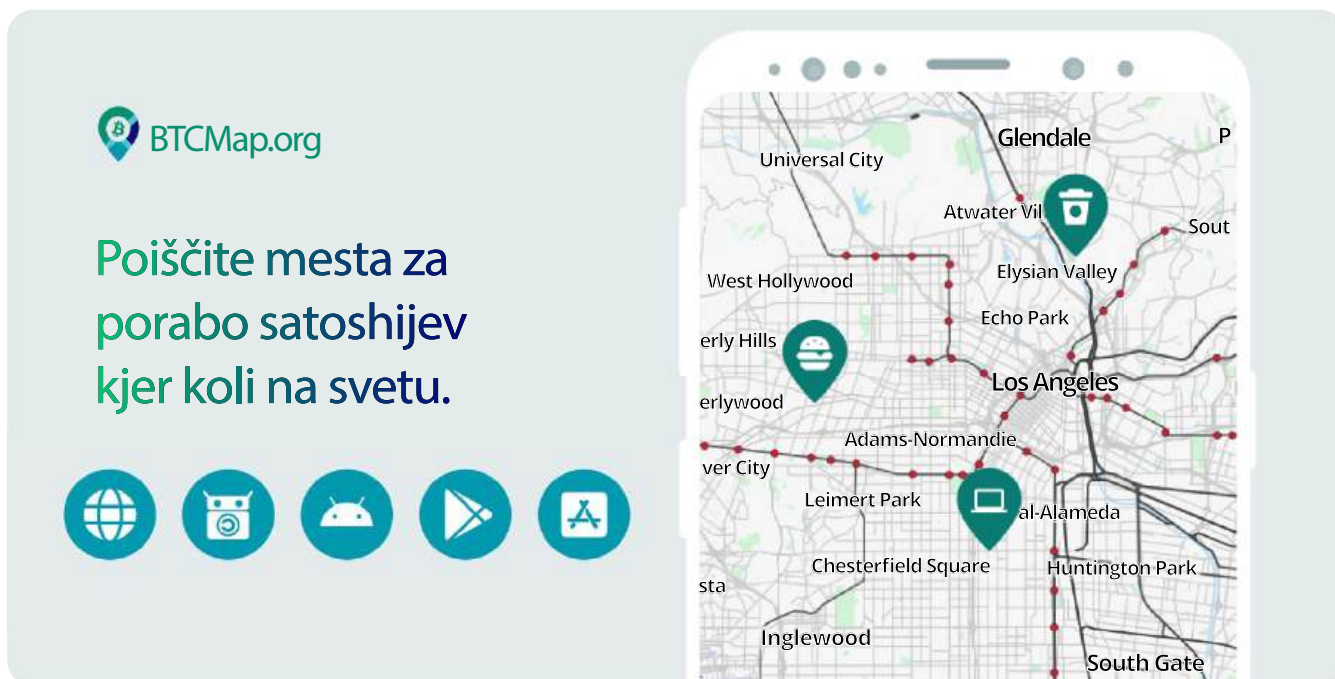
## 8.5.2 Osebno: poiščite trgovca na svojem območju

Fizične trgovine lahko za sprejemanje plačil uporabljajo strežnik BTCPay Server ali pa preprosto prenesejo Bitcoinovo denarnico in sprejmejo Bitcoinova plačila prek telefona.



Če želite najti trgovca, ki sprejema bitcoine v vašem območju, obiščite spletno mesto BTCMap.org in poiščite svoje območje.

BTCMap.org je odprtokodni zemljevid, kjer lahko trgovci, ki sprejemajo bitcoine, navedejo svoja podjetja. To je zmožljiva rešitev za ljudi, ki želijo porabiti svoje bitcoine.



### 8.5.3 Prehodna orodja: boni, darilne kartice in plačilne kartice

Za nakup izdelkov ali storitev v podjetjih, ki še ne sprejemajo bitcoinov, lahko uporabite posredniško orodje – darilne kartice.

Nekatera podjetja se osredotočajo na nakup in prodajo darilnih kartic v zameno za bitcoine. To pomeni, da lahko v zameno za bitcoine pridobite darilno kartico za želeno trgovino in jo tam unovčite.

Z bitcoini in darilnimi karticami lahko kupite skoraj vse – letalske vozovnice, hotele, igre, kartice SIM.

### 8.5.4 Krožne ekonomije in Bitcoin kot menjalno sredstvo

Koncept krožne ekonomije izhaja iz zamisli o zmanjšanju količine odpadkov v gospodarstvu s ponovno uporabo in recikliranjem čim večjega števila izdelkov in stranskih proizvodov.

Bitcoinova krožna ekonomija je koncept gospodarstva, kjer se transakcije izvajajo v bitcoinih, denar v obliki bitcoinov pa ostaja in raste v gospodarstvu ter koristi posameznikom in podjetjem.





# Lightning Network: vsakodnevna uporaba Bitcoina

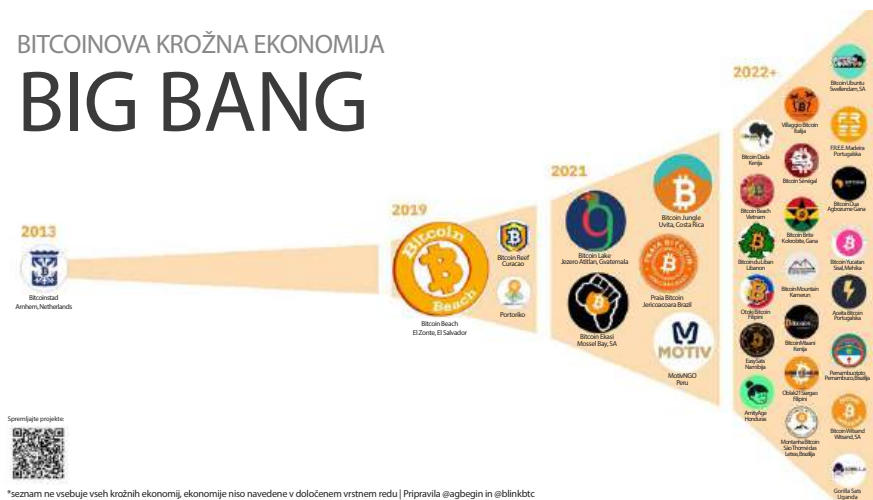
Omrežje Lightning Network omogoča razcvet Bitcoinove krožne ekonomije po svetu zahvaljujoč skoraj takojšnjim Bitcoinovim transakcijam z nizkimi provizijami.

V Arnhemu na Nizozemskem je bila ustvarjena prva Bitcoinova krožna ekonomija. Ustvarjena je bila veliko pred vzpostavitvijo omrežja Lightning Network, vendar so bile takrat provizije v verigi zelo nizke!



## BITCOINOVA KROŽNA EKONOMIJA

# BIG BANG



Druha krožna ekonomija je bila Bitcoin Beach v mestu El Zonte v Salvadorju. Izkoristila je zmogljivost omrežja Lightning Network, da je skupnosti, katere člani večinoma niso imeli bančnih računov, omogočila takojšnja digitalna plačila neposredno z njihovimi pametnimi telefoni.

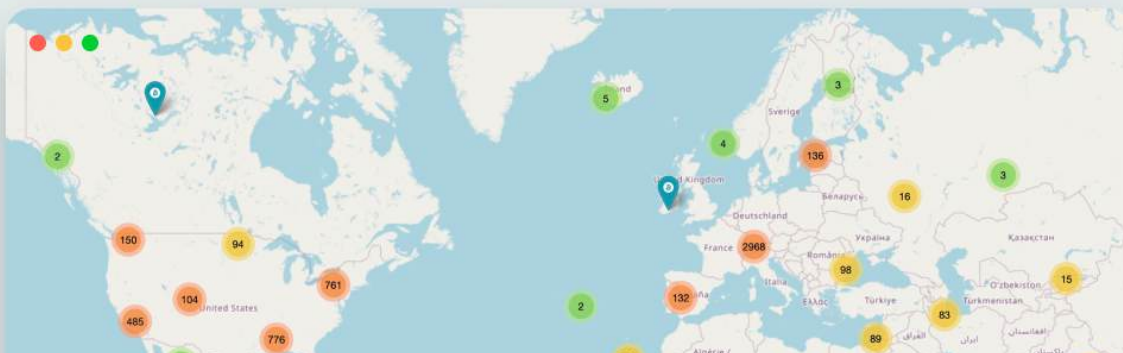
Danes so Bitcoin in Lightning Network ter izobraževalni viri vzpostavili več sto krožnih ekonomij po vsem svetu.



Na spletnem mestu BTCMap.org lahko poiščete tudi Bitcoinove skupnosti, kjer boste spoznali druge uporabnike Bitcoina in podjetja, ki sprejemajo bitcoin. Nekateri naši učitelji in učenci so na BTCmap.org celo dodali podjetja in krožne ekonomije – ko boste pripravljeni, lahko to naredite tudi vi!



**Poiščite mesta za porabo satoshijev  
kjer koli na svetu.**



**Vir:** [btcmap.org/communities](https://btcmap.org/communities)

Na koncu 8. poglavja ste dobili vpogled v vsakdanjo uporabo Bitcoina v omrežju Lightning Network. Omrežje Lightning Network omogoča hitrejšje in dostopnejše transakcije ter vpoglede v načine spreminjanja in večplastnega razvoja Bitcoina.

V 9. poglavju bomo raziskali tehnično stran Bitcoina. Od kriptografije do vozlišč, rudarjev in drugega – pripravite se na podrobnejši vpogled v delovanje Bitcoina.



## 9. poglavje

# ***Uvod v tehnično plat Bitcoina***

### 9.0 Uvod

Dejavnost: Oglejte si »How Bitcoin Works Under the Hood«  
(Vpogled v delovanje Bitcoina)

### 9.1 Javni in zasebni ključi: Varnost s kriptografijo

9.1.1 Kriptografija – javni/zasebni ključi

9.1.2 Razlaga zgoščevanja

Dejavnost: Generiranje zgoščene vrednosti SHA256

### 9.2 Model UTXO

### 9.3 Bitcoinova vozlišča in rudarji

9.3.1 Kaj je Bitcoinovo vozlišče in kako ga vzpostavim?

Dejavnost: Oglejte si videoposnetek o Bitcoinovih vozliščih

9.3.2 Kaj je rudar bitcoinov in kako deluje rudarjenje?

### 9.4 Kaj je bazen transakcij?

Dejavnost: Bazen transakcij

### 9.5 Kako potekajo Bitcoinove transakcije od začetka do konca

Dejavnost: potek Bitcoinove transakcije

***Delovni zvezek za učence***

Slovenska različica | 2024

# Uvod v tehnično plat Bitcoin

## 9.0 Uvod

Bitcoin ni »reguliran«. Namesto da bi ga regulirala vladna birokracija, ga regulira algoritem. Brez korupcije.

**Andreas M. Antonopoulos**

V tem poglavju si bomo podrobneje ogledali tehnologijo, ki Bitcoinovem omrežju omogoča popolnoma decentralizirano delovanje. Na preprost način bomo razložili, kaj se zgodi, ko pošljete transakcijo z bitcoin, kako se te transakcije obdelajo ter kakšno funkcijo imajo v Bitcoinovem omrežju rudarji in vozlišča. V tem poglavju bomo obravnavali nekaj zahtevnih in tehničnih konceptov. Ne pozabite, da veliko ljudi ne razume, kako deluje internet, vendar ga vsak dan uporabljajo za pošiljanje e-pošte, stike s prijatelji na družabnih omrežjih in celo plačevanje računov. Spoznavanje tehnične plati delovanja Bitcoin je dolga pot, ki je morda ne bo želel opraviti vsak, tudi če se bo odločil, da bo Bitcoin uporabljal kot obliko denarja. Čeprav vas spodbujamo, da se še naprej učite o tehničnih vidikih Bitcoin, se bomo v tem poglavju osredotočili na osnovne ključne koncepte.

### Mehanizem Bitcoinovega protokola

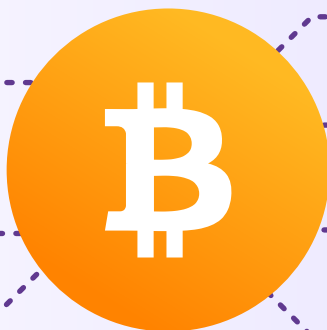
Dokaz o delu (PoW)



Kriptografski časovni žigi



Prilagoditev težavnosti



Omrežna arhitektura enakovrednih udeležencev



Zgostitvena funkcija in Merklovo drevo



Kriptografija javnih ključev



Razpolavljanje blokovnih nadomestil

Če želite več tehničnih informacij o delovanju Bitcoin, smo na koncu tega delovnega zvezka vključili vire do dodatnih informacij. Na našem spletnem mestu se lahko prijavite tudi za Diplomno Bitcoin – tehnična različica. Ko bo ta bolj tehnični tečaj pripravljen, boste o tem obveščeni.

Oglejmo si videoposnetek, ki prikazuje delovanje Bitcoinovega omrežja.

**Dejavnost: Oglejte si »How Bitcoin Works Under the Hood« (Vpogled v delovanje Bitcoin)**



Kot ste videli v videoposnetku, je Bitcoinovo omrežje le glavna knjiga ali zapis transakcij, shranjenih v več računalnikih, imenovanih vozlišča. Bitcoinova glavna knjiga je psevdonimna, kar pomeni, da ne vsebuje osebnih podatkov, temveč le podatke o transakcijah in naslovih. V njej so prikazani vsi bitcoini in njihovo premikanje od začetka delovanja omrežja 3. januarja 2009.



V nadaljevanju si bomo podrobneje ogledali tehnologijo, ki omogoča ta sistem.

## 9.1 Javni in zasebni ključi: Varnost s kriptografijo

Bitcoin nam daje trdno obljubo: program bo izveden točno tako, kot je določeno.

**Andreas M. Antonopoulos**

### 9.1.1 Kriptografija – javni/zasebni ključi

Kriptografija je način zaščite tajnosti informacij z zakrinkanjem informacij v kodo.



- Šifriranje je postopek pretvorbe informacij v posebno kodo, tako da jih ne more prebrati nihče, ki nima pravilne metode dešifriranja. To je podobno kot pri zaklepanju sefa, ki ga lahko odpre le oseba z ustreznim ključem ali kombinacijo.
- Dešifriranje pa je postopek, pri katerem šifrirane informacije ponovno postanejo berljive, podobno kot če bi odklenili sef in bi lahko prebrali informacije v njem.

Recimo, da želi Gregor poslati Alanu skrivno sporočilo, ki ga ne sme prebrati nihče drug. Dogovorita se, da bosta za prikrivanje sporočila pred pošiljanjem uporabila metodo šifriranja s prostozidarsko kodo. Sporočilo lahko dešifrirajo samo tisti, ki imajo kodo, tako da ga nihče drug ne more prebrati. Čeprav ta metoda danes ne velja za varno, ponazarja načelo kriptografije zasebnih ključev za pošiljanje sporočil.

#### Kako rešiti

prostozidarsko kodo

Pri reševanju prostozidarske kode igralec dobi šifrirano sporočilo in kodo. Če želi igralec dešifrirati sporočilo, mora poiskati simbol v šifriranem sporočilu na kodi in najti dešifrirano črko.

Primer šifriranega sporočila:



A	B	C	J	K	L	S	W
D	E	F	M	N	F	T	X
G	H	I	P	Q	R	U	Y
						V	Z

#### Kako kriptografija deluje pri transakcijah z bitcoini?

Pri tradicionalni kriptografiji z zasebnim ključem bi si morala Gregor in Alan najprej deliti skrivni ključ, na primer geslo ali prostozidarsko kodo. Gregor bi nato s tem ključem šifriral svoje sporočilo, preden bi ga poslal Alanu. Alan, ki prav tako pozna skrivni ključ, bi nato z istim ključem dešifriral sporočilo in ga prebral.

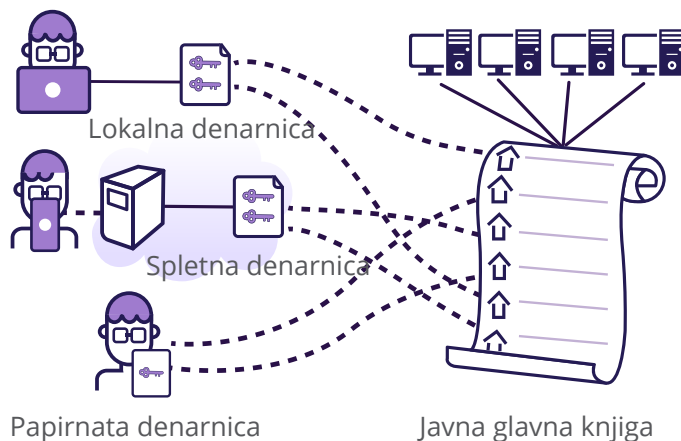
Če bi imel ključ še kdo drug in bi prestregel sporočilo, bi ga lahko dešifriral in prebral.

# Uvod v tehnično plat Bitcoina

Kriptografija z javnim ključem, ki je uporabljena pri transakcijah z bitcoini, je to težavo rešila. Pri kriptografiji z javnim ključem Gregorju in Alanu ni treba deliti gesla ali medsebojnega načina šifriranja. Namesto tega imata dva različna ključa: javni ključ (ki ga lahko varno delite s komer koli) in zasebni ključ (ki mora ostati zaupen).

Ko želi Gregor poslati sporočilo Alanu, uporabi Alanov javni ključ za šifriranje svojega sporočila, preden ga pošlje Alanu. Ko Alan prejme sporočilo, ga lahko s svojim zasebnim ključem dešifrira samo on. Sporočila ne bi mogel prebrati nihče drug, tudi če bi prestregel sporočilo. Možnosti za krajo ključa so tudi

## Uporabniki Bitcoinovega omrežja Bitcoinovo omrežje



Glavna prednost kriptografije z javnim ključem pred zasebnim je torej ta, da omogoča varno komunikacijo, ne da bi si morala pošiljatelj in prejemnik najprej deliti skrivni ključ (ali drugo metodo šifriranja, kot je prostoziidarska koda), ki bi ga lahko prestregla tretja oseba.

V Bitcoinu za pošiljanje šifriranih sporočil ni uporabljena kriptografija z javnim ključem. Namesto tega je uporabljena za ustvarjanje enoličnih digitalnih podpisov, zaradi katerih transakcij z bitcoini ni mogoče spreminjati. Digitalni podpis je način dokazovanja pristnosti transakcije z bitcoini, ki je na neki način podoben podpisu na fizičnem dokumentu.



### Kriptografija z javnim ključem (za vsako transakcijo med dvema uporabnikoma):

Vsak uporabnik ima dva ključa: zasebni ključ, ki je tajen, in javni ključ, ki ga lahko deli z drugimi.

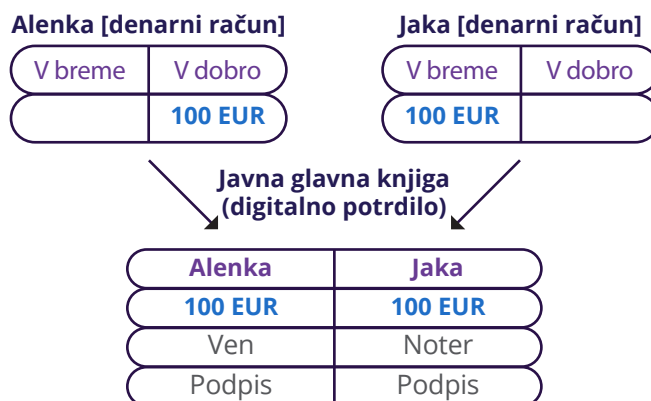
Zasebni ključ je oblika identifikacije in dokazilo o lastništvu ter potrjuje: »Ta naslov pripada meni in imam nadzor nad njim.«

Digitalni podpisi so ustvarjeni za prepoznavanje enoličnih transakcij.

## Digitalni podpis



- Transakcije z bitcoini vključujejo prenos določenega zneska bitcoinov neposredno na račun druge osebe.
- Le pravi imetnik bitcoinov lahko nadzoruje, ali bo svoj denar poslal nekomu drugemu. Zagotavlja, da je lastnina zaščitena pred zlonamernimi akterji.
- Kot dodatni zaščitni ukrep je vsaka transakcija, ki jo pošljete v Bitcoinu, samodejno podpisana z ENOLIČNIM podpisom. Ta enolični podpis je podprt s tehnologijo, odporno na spreminjanje. Ta omrežju pomaga preveriti, ali je bitcoine poslal pravi lastnik in ne kdo drug.



Kako to deluje v resnični transakciji z bitcoini, povedano na preprost način.

- 1 Ustvarjanje transakcije:**  
Uporabnik sproži transakcijo z bitcoini tako, da navede podrobnosti, kot sta naslov prejemnika in znesek bitcoinov, ki ga je treba poslati.
- 2 Ustvarjanje digitalnega podpisa:**  
Pošiljatelj s svojim zasebnim ključem ustvari enoličen digitalni podpis. Ta podpis je enolična kriptografska koda, ki potrjuje pristnost transakcije.
- 3 Oddajanje transakcije:**  
Podpisana transakcija je poslana v Bitcoinovo omrežje, kar pomeni, da namerava pošiljatelj prenesti lastništvo bitcoinov na prejemnika.
- 4 Preverjanje v omrežju:**  
Vozlišča v Bitcoinovem omrežju prejmejo transakcijo in uporabijo javni ključ prejemnika za dešifriranje in preverjanje celovitosti transakcije. Hkrati uporabijo pošiljateljev javni ključ za preverjanje digitalnega podpisa.
- 5 Potrditev v Bitcoinovem omrežju:**  
Če je preverjanje uspešno, je transakcija dodana v glavno knjigo, ki služi kot varen in pregleden zapis vseh transakcij. Po potrditvi se lastništvo bitcoinov uradno prenese s pošiljatelja na prejemnika.



Digitalni podpis, ustvarjen s pošiljateljevim zasebnim ključem, služi kot kriptografski dokaz pristnosti in lastništva ter decentraliziranemu Bitcoinovemu omrežju omogoča, da potrdi in zabeleži transakcijo v glavni knjigi.

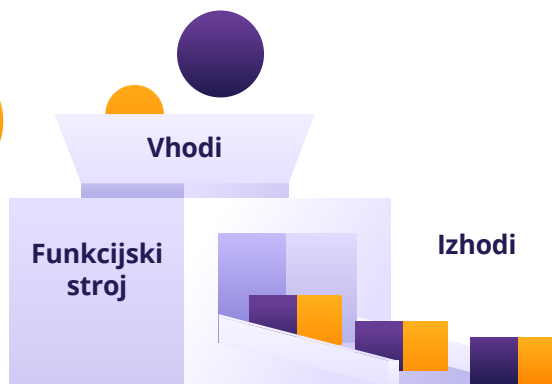
# Uvod v tehnično plat Bitcoina

## 9.1.2 Razlaga zgoščevanja

Ne ustrašite se tehničnih izrazov in matematičnih pojmov. Razumemo, da ni vsakdo navdušen nad matematiko, vendar boste morda presenečeni in ugotovili, da lahko z malo truda dojamete tudi najbolj zapletene ideje.

### Kaj je funkcija?

Funkcija je kot stroj, ki prevzame neko informacijo in jo spremeni v nekaj novega. Informacije, ki jih posredujete funkciji, se imenujejo vhod. Nova informacija, ki jo ustvari funkcija, se imenuje izhod. Funkcije pomagajo računalnikom opravljati naloge in reševati težave.



Predstavljajte si ga kot recept za pripravo solate. Recept (ali funkcija) vam pove, katere sestavine uporabiti in kako jih zmešati, da pripravite solato. V recept lahko vstavite različne sestavine, vendar bo rezultat vedno solata. Funkcije lahko uporabite, da bo delo lažje in bolj učinkovito.

Ta recept je funkcija, ki za vhod vzame sestavine in kot izhod ustvari mešano solato.

V Bitcoinu so za izvajanje transakcij uporabljene funkcije. Vemo že, da so transakcije z bitcoini v bistvu prenos vrednosti (denarja) z enega naslova na drugega. Za izvedbo transakcije so uporabljene številne kriptografske funkcije, s katerimi je potrjena transakcija in posodobljeno stanje Bitcoinove glavne knjige.



Funkcije, ki se uporabljajo pri transakciji z bitcoini, vključujejo preverjanje pristnosti vhodnih podatkov transakcije, preverjanje, ali ima pošiljatelj dovolj sredstev, in posodabljanje stanja ustreznih naslovov. Ko je transakcija preverjena in dodana v blok v glavni knjigi, postane del trajnega zapisa vseh transakcij v omrežju.

### Kaj je enosmerna funkcija?

Enosmerna funkcija uporablja niz navodil za obdelavo informacij in jih spremeni v nekaj novega, tako kot recept za smoothie spremeni sestavine v nov napitek. Toda tako kot ne morete razmešati smoothija, da bi dobili nazaj prvotne sestavine, ne morete obrniti enosmerne funkcije, da bi dobili nazaj prvotne informacije.



Kriptografija z javnim ključem, katere del je tudi javni ključ, temelji na uporabi enosmernih funkcij, ki otežujejo določanje zasebnega ključa iz javnega ključa. Teoretično ni povsem »nemogoče« najti zasebni ključ iz javnega ključa, vendar je to izredno težko in bi za to nalogo potrebovali ogromno časa in računske zmogljivosti.

Iskanje zasebnega ključa v javnem ključu v Bitcoinu je podobno iskanju igle v kupu sena, velikem kot nogometno igrišče. Igla predstavlja zasebni ključ, kopica sena pa vse možne zasebne ključe.

Prav tako so enosmerne funkcije zasnovane tako, da so nepovratne in jih ni mogoče dešifrirati.



## Kaj je funkcija zgoščevanja?

Zgoščevanje je kot prstni odtis za digitalne podatke. Gre za postopek, pri katerem je digitalno sporočilo pretvorjeno v kodo fiksne dolžine, ki služi kot enolični identifikator.



Tako kot lahko s prstnim odtisom identificiramo osebo, lahko z zgoščeno vrednostjo identificiramo digitalno sporočilo. Gesla so uporabljena v številnih aplikacijah, vključno s transakcijami z bitcoini.

Kako je pri transakcijah z bitcoini uporabljeno zgoščevanje

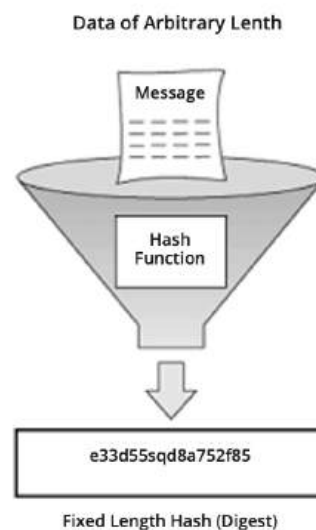
Preden je transakcija dodana v blok v Bitcoinovi glavni knjigi, je zgoščena. To zgoščevanje deluje kot podpis transakcije in preverja, ali je transakcija veljavna in ni bila spremenjena. Če nekdo poskuša spremeniti eno samo črko v transakciji, bo zgoščena popolnoma drugačna, kar bo druge opozorilo na spremembo.

Vloga zgoščevanja pri zagotavljanju varnosti

Zgoščevanje je bistvenega pomena za varnost Bitcoinovega omrežja. Z uporabo gesel za identifikacijo transakcij lahko omrežje odkrije vsak poskus spremembe ali manipulacije transakcije. To pomaga preprečevati goljufije in zagotavlja, da so vse transakcije natančno zabeležene v glavni knjigi.

Funkcija zgoščevanja je vrsta enosmerne funkcije, ki sprejme vhod (imenovan sporočilo ali podatek) in ga pretvori v številčno predstavitev, imenovano »zgoščena vrednost«. Izhodna zgoščena vrednost je enolična glede na vhodne podatke, zato že majhna

Text	Hash Value
Some text	20c9ad97c081d63397d
Some text	7b685a412227a40e23c
Some text	8bdc6688c6f37e97cfbc2
Some text	2d2b4d1db1510d8f61e
Some text	6a8866ad7f0e17c02b14
Some text	182d37ea7c3c8b9c2683
Some text	aeb6b733a1



Funkcija zgoščevanja je podobna stroju za tajno šifriranje. Prevzame sporočilo in ga pretvori v kodo.





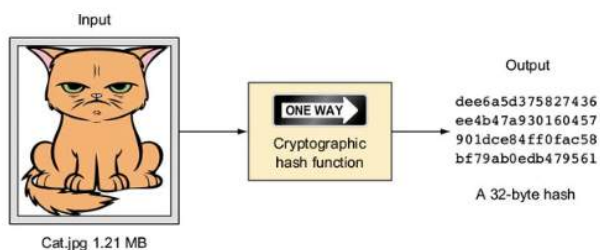
# Uvod v tehnično plat Bitcoina

Koda je za isto sporočilo vedno enaka. Če sporočilo le malo spremenite, bo koda popolnoma drugačna. Tako si računalniki lažje zapomnijo stvari in preverijo, ali je bilo kaj spremenjeno.

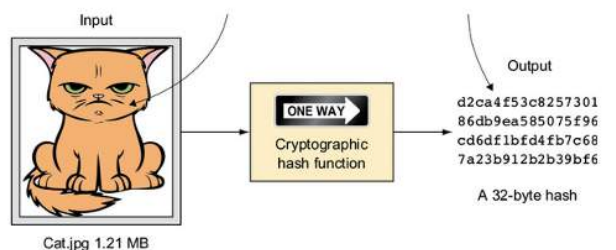


Takoj ustvarite zgoščeno vrednost SHA256 poljubnega niza ali vhodne vrednosti. Funkcije zgoščevanja so

## Dejavnost – generiranje zgoščene vrednosti SHA 256



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



Rezultat ali zgoščena vrednost je vedno enako dolg, ne glede na to, kako dolga je bila prvotna informacija.

Bitcoin uporablja nekaj posebnih vrst funkcij zgoščevanja, imenovanih SHA-256 in RIPEMD160. Nekaj primerov je v nadaljevanju:

videli boste, da majhna sprememba drugega vhoda popolnoma spremeni izhod v

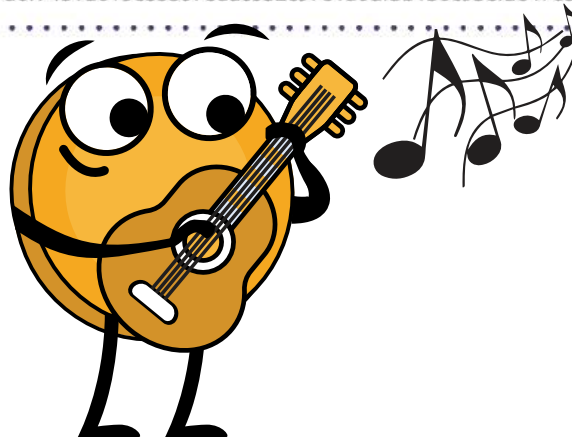
tretji vhod je ogromna datoteka, vendar je izhod še vedno enake fiksne dolžine kot druga dva.

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

Zgoščevanje si lahko predstavljamo tudi kot glasbeno partituro, ki zajame bistvo glasbenega dela. Tako kot je glasbena partitura edinstvena predstavitev melodije, je zgoščena vrednost edinstvena predstavitev dela podatkov. Glasbenik lahko primerja partituro glasbenega dela z dejansko izvedbo in tako ugotovi, ali je izvedba točna. Podobno lahko s primerjavo zgoščene vrednosti prejetih podatkov z izvirno zgoščeno vrednostjo ugotovimo, ali so bili podatki med prenosom spremenjeni.



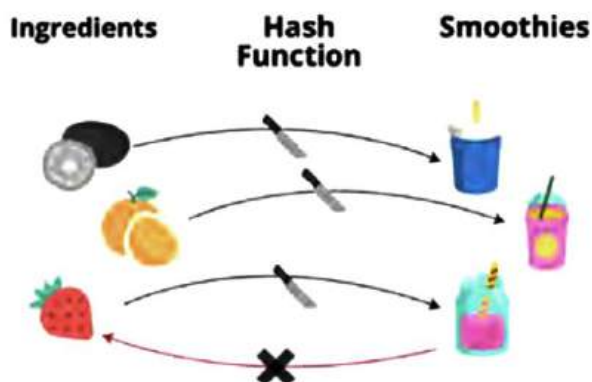
Tako kot lahko že najmanjše odstopanje v glasbeni izvedbi povzroči, da zveni drugače, bo tudi najmanjša sprememba izvirnih podatkov povzročila drugačno zgoščeno vrednost. Zaradi tega je zgoščevanje močno orodje za zagotavljanje celovitosti in pristnosti transakcije z bitcoini.

Postopek kodiranja javnega ključa s pomočjo zgoščevanja vrednosti je uporabljen za izboljšanje varnosti informacij s pretvorbo v obliko fiksne dolžine, ki je ni mogoče prebrati. Bitcoin za izdelavo javnih naslovov uporablja algoritma SHA-256 in Ripemd-160. Dobljeni rezultat je uporabljen kot enolični identifikator za javni ključ ter pomaga zagotoviti celovitost in varnost transakcij, shranjenih v glavni knjigi. S takšnim šifriranjem podatkov je nepooblaščenim osebam težje dostopati do podatkov in z njimi manipulirati.



### Hashing

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



#### Deterministično.

Iz istih sestavin vedno dobite enak smoothie.



#### Odpornost na praslike.

Ko dobite smoothie, ne morete znova sestaviti jagode.



#### Odpornost korelacije.

Z majhno spremembo sestavin dobite popolnoma drugačen smoothie.



#### Odpornost na trke.

Težko je najti različne sestavine za smoothie, iz katerih bi nastal popolnoma enak smoothie.



#### Hitrost in preverljivost.

V mešalnik vržete sadje. Mešalnik hitro zmelje sadje, vi pa dobite smoothie.

## 9.2 Model UTXO

UTXO – neporabljen izhod transakcij

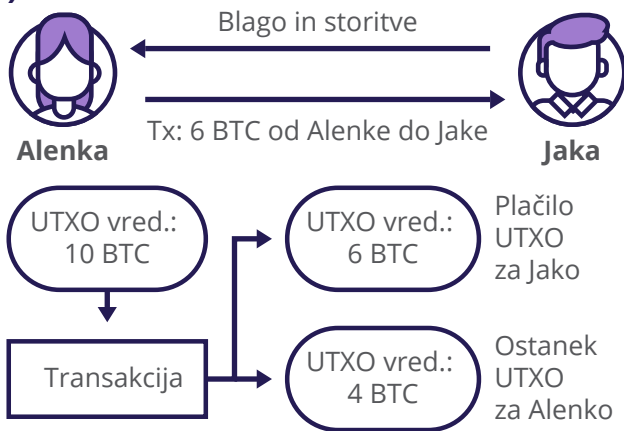


# Uvod v tehnično plat Bitcoin

## Kaj so neporabljeni izhodi transakcij (UTXO)?

V Bitcoinu transakcije potekajo tako, da večji kos zlata razbijete na manjše kose in te manjše kose pošljete drugim in sebi.

Vrednost UTXO si lahko predstavljate kot različne velikosti in dele bitcoinov ali bankovce različnih vrednosti v vaši denarnici. Ko porabite UTXO, se za prejemnika ponovno ustvari nov UTXO. Vse, kar ostane, pa prejmete nazaj v novi vrednosti UTXO, imenovani »UTXO ostanka«. To je podobno, kot če bi z bankovcem za 10 evrov kupili dve skodelici kokakole za 6 evrov. Trgovina obdrži 6 evrov, vam pa izroči 4 evre v drobižu.



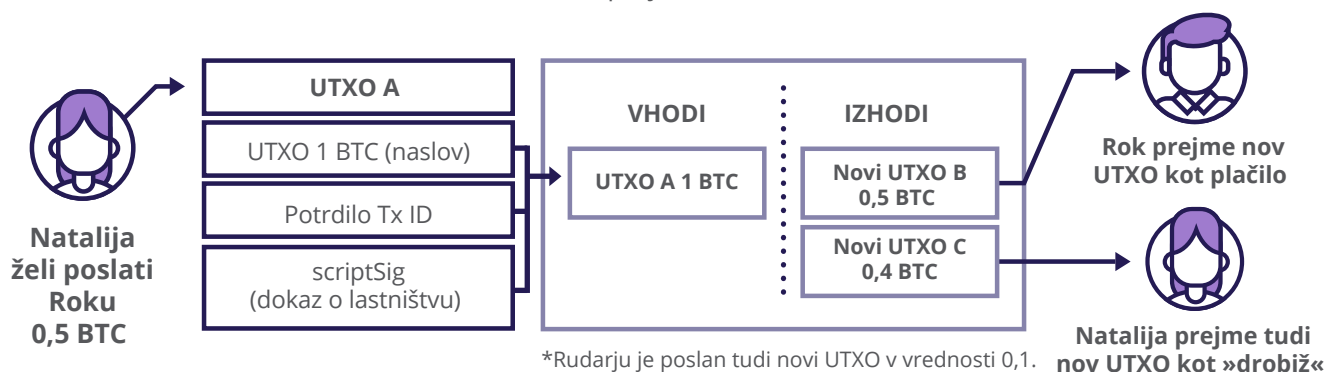
Pri pošiljanju bitcoinov vedno pošljite celoten znesek enega (ali več) svojih UTXO v Bitcoinovi denarnici. Kaj se zgodi? En del pošljete prejemniku, preostalo količino pa prejmete nazaj kot drobiž na enega od svojih novih Bitcoinovih naslovov. Razlika, ki jo prejmete, se imenuje izhod neuporabljenih transakcij ali UTXO in je lahko uporabljena kot vhod za novo prihodnjo transakcijo.

Stanje v vaši Bitcoinovi denarnici je vsota vseh vaših različnih vrednosti UTXO. Vsota vaših vrednosti UTXO je torej vsota količine bitcoinov, ki jih imate v lasti.

Pomembno je opozoriti, da drugih ne smete obveščati o svojih vrednostih UTXO, saj lahko nekdo, ki jih pozna, spremlja vaše transakcije z bitcoin v omrežju in na koncu izve, koliko denarja imate v lasti.



Vsakič, ko opravite transakcijo, uporabite enega ali več svojih obstoječih UTXO za porabo bitcoinov in ustvarite nove vrednosti UTXO (tako za vas kot za prejemnika).



Ko je transakcija izvedena, je znesek poslanih bitcoinov razdeljen na več izhodov, od katerih je vsak povezan z novim Bitcoinovim naslovom (novo vrednostjo UTXO).

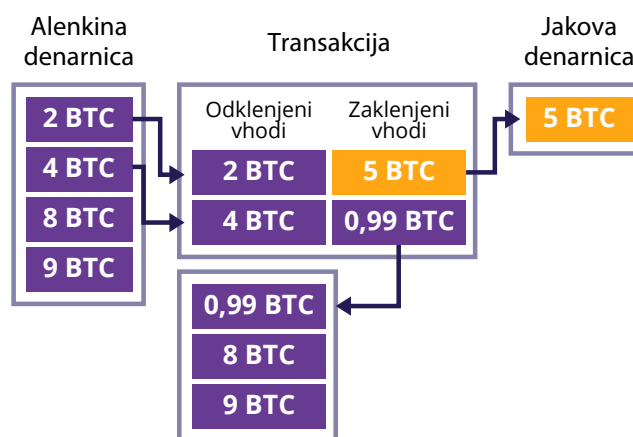


Ko nekomu pošiljate bitcoine, uporabite eno ali več vrednosti UTXO kot vir sredstev (vhod). Te vrednosti UTXO bodo po potrebi združene, da bodo ustvarjeni novi izhodi, ki pripadajo prejemniku transakcije in vam. Ti novi izhodi ali UTXO postanejo last prejemnika in vaša last. Njih je nato mogoče uporabiti kot vir sredstev pri drugih prihodnjih transakcijah. Ta veriga vrednosti UTXO ustvarja pregledno in sledljivo zgodovino vseh transakcij z bitcoini v Bitcoinovi glavni knjigi, začenši s prvim blokom (3. januarja 2009).

Primer za ponazoritev delovanja: če želite poslati dva bitcoina, a imate le UTXO v vrednosti pet bitcoinov, prejmete razliko treh bitcoinov nazaj kot »drobiž«. Ta sprememba je za vas nova vrednost UTXO, ki jo lahko porabite v eni od prihodnjih transakcij.

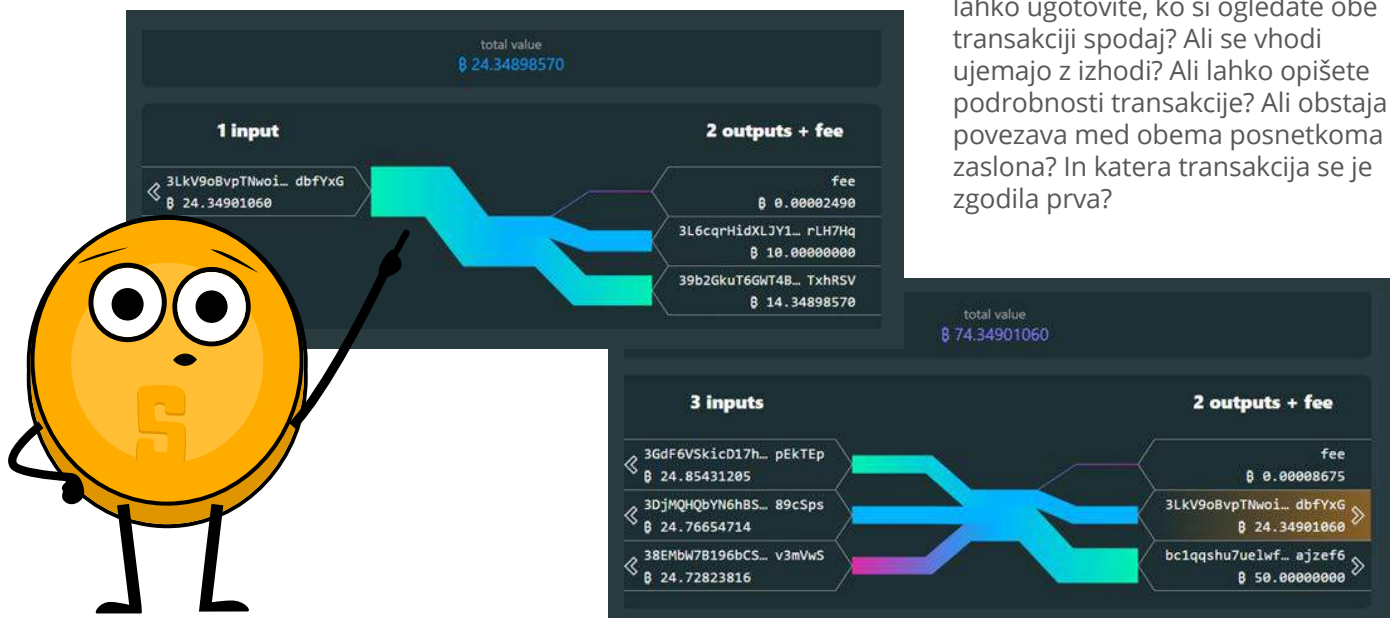
Drug primer:

- 1 Alenka želi Jaku poslati pet bitcoinov.
- 2 Združi šest bitcoinov iz dveh svojih neuporabljenih izhodov transakcij (UTXO)
- 3 Iz teh neuporabljenih izhodov transakcij pošlje Jaki pet bitcoinov, dobi nazaj 0,99 bitcoina kot drobiž in mora plačati 0,01 transakcijske provizije.
- 4 Po potrditvi je transakcija dodana v Bitcoinovo knjigo, pri tem pa so posodobljena vsa vozlišča, ki imajo kopijo knjige.



Če bi Alenka poskušala uporabiti enega od svojih že porabljenih izhodov za drugo transakcijo, bi jo vozlišča samodejno zavrnila. Vozlišča namreč hranijo kopijo Bitcoinove glavne knjige (in vseh transakcij), zato lahko preprosto preverijo stanje Aleninih vrednosti UTXO in preverijo, ali je transakcija neveljavna.

Spodaj je posnetek zaslona dejanske transakcije, v kateri je samo en vhod. V drugem primeru pa je lahko začetno stanje vsota več vrednosti UTXO (več vhodov). Kaj lahko ugotovite, ko si ogledate obe transakciji spodaj? Ali se vhodi ujemajo z izhodi? Ali lahko opišete povezavo med obema posnetkoma zaslona? In katera transakcija se je zgodila prva?



# Uvod v tehnično plat Bitcoin

## 9.3 Podrobnejši pregled Bitcoinovih vozlišč in rudarjev bitcoinov

V tem poglavju si bomo podrobneje ogledali dva zelo pomembna dela (in udeležence) Bitcoinovega omrežja, ki smo ju prvič predstavili v 6. poglavju. Ogledali si bomo:



### Bitcoinova vozlišča:

Varuhi preverjanja veljavnosti hranijo kopijo Bitcoinove glavne knjige ter skrbijo, da so vse transakcije veljavne in da vsi upoštevajo ista pravila.

Ker je to opravilo porazdeljeno med številne ljudi po vsem svetu, je Bitcoin odporen na morebitne težave. Ta vozlišča pripomorejo k temu, da je sistem vreden zaupanja in zvest svoji ideji decentraliziranega sistema, v katerem nobena oseba ali skupina nima prevelike moči.



### Rudarji bitcoinov:

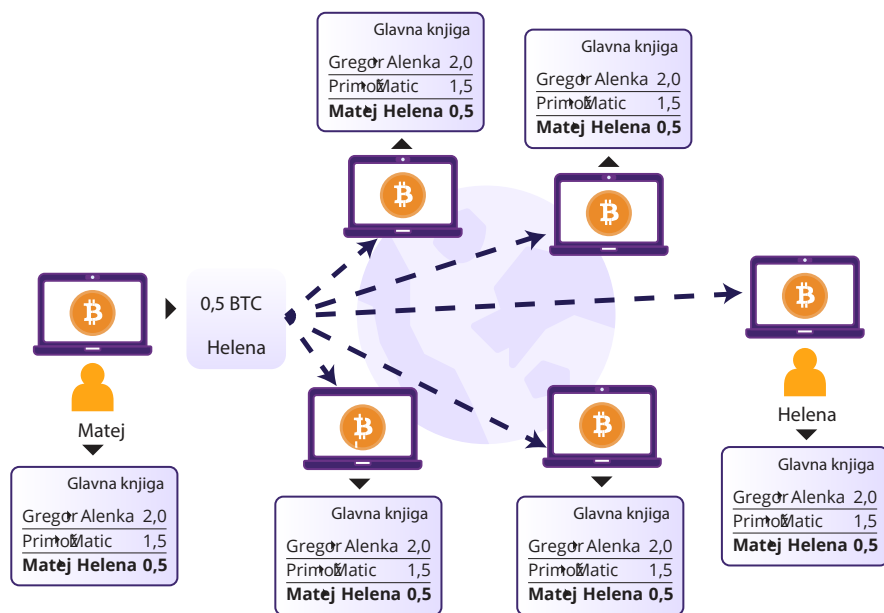
Arhitekti varnosti, ki z zmogljivimi računalniki in električnimi zmogljivostmi preverjajo in nadzorujejo transakcije ter skrbijo, da je vse varno. Na ta način je glavna knjiga ali veriga blokov odporna proti vsem zlonamernim akterjem, ki bi želeli motiti delovanje sistema.

Bitcoinova vozlišča in rudarji skupaj sodelujejo pri vzdrževanju decentraliziranega, varnega in močnega sistema – novega načina ravnanja z denarjem, na katerega se lahko zanesejo ljudje po vsem svetu. Oglejmo si te vloge bolj podrobno, da bomo razumeli, kako prispevajo k inovativnemu sistemu Bitcoin.

### 9.3.1 Kaj je Bitcoinovo vozlišče in kako ga vzpostavim?

Bitcoinovo vozlišče se morda sliši tehnično, vendar je le del programske opreme, ki upravlja kopijo Bitcoinove glavne knjige. Ko vodite svoje Bitcoinovo vozlišče, lahko sodelujete pri oblikovanju pravil omrežja Bitcoin.

Predstavljajte si naslednje: če skupina ljudi poskuša spremeniti delovanje Bitcoin, na primer tako, da spremeni skupno zalogo bitcoinov, imate možnost odločanja. Lahko se odločite, da svojega vozlišča ne boste spremenili v nov sistem, kar je kot glasovanje za



Predstavljajmo si Bitcoinovo vozlišče kot policista digitalnega prometa z nekaterimi ključnimi nalogami.

1

**Varuhi preverjanja veljavnosti:**

Bitcoinovo vozlišče hrani digitalno kopijo verige blokov, ki je neke vrste skupna glavna knjiga vseh transakcij z bitcoini. Ta isti zapis imajo številna vozlišča po vsem svetu.

2

**Komunikacijsko vozlišče:**

Vozlišča se med seboj povezujejo in ustvarjajo obsežno komunikacijsko omrežje. Med seboj si izmenjujejo informacije, zlasti o transakcijah, ki v digitalni čakalnici, imenovani »bazen transakcij«, čakajo, da bodo dodane v verigo blokov.

3

**Preverjevalnik kakovosti:**

Vsak dodatek v verigi blokov je izpostavljen natančnemu pregledu. Vozlišča skrbijo za veljavnost transakcij in zavrnejo vse, ki ne izpolnjujejo pravil Bitcoinovega omrežja.

4

**Obveščevalec o verigi blokov:**

Druga programska oprema, kot so denarnice, lahko vozlišče zaprosi za informacije o verigi blokov, na primer o stanju bitcoinov. Vozlišča služijo kot informacijska vozlišča.

5

**Dobrodošlica za nova vozlišča:**

Ko se želi pridružiti novo vozlišče, obstoječa vozlišča velikodušno posredujejo kopijo verige blokov. Novo vozlišče neodvisno preveri veljavnost vsake transakcije, kar poudarja sistem, brez potrebe po zaupanju drugim udeležencem.

Dejavnost: Oglejte si videoposnetek o Bitcoinovih vozliščih



Ena od možnosti za zagon lastnega vozlišča je, da prenesete programsko opremo Bitcoin Core in ji daste nekaj časa, da prenese celotno verigo blokov. Ko je oprema pripravljena, jo lahko pustite vklopljeno in približno vsakih 10 minut bodo prispeli novi bloki s transakcijami. Vozlišče preveri njihovo veljavnost in jih doda v lokalno kopijo verige blokov.

Viri:  
Programska oprema  
Bitcoin Core



Upravljanje vozlišča zagotavlja suverenost in neodvisnost. Ni se vam treba zanašati na druge – to je vaš lastni nadzornik prometa. V nasprotju z Bitcoinovo denarnico, ki nima kopije verige blokov, vozlišče zagotavlja samozadostnost. Namesto da bi svoje imetje bitcoinov (in stanje Bitcoinovega omrežja) zaupali drugim, vaša denarnica komunicira z vašim osebnim vozliščem, zaradi česar je vaša digitalna izkušnja bolj varna in vredna zaupanja.

### 9.3.2. Kaj je rudar bitcoinov in kako deluje rudarjenje?

Namen rudarjenja ni ustvarjanje novih bitcoinov – je sistem spodbude. Rudarjenje je mehanizem, s katerim je varnost Bitcoina decentralizirana.

**Andreas M. Antonopoulos**

# Uvod v tehnično plat Bitcoina



**Rudarji zbirajo nepotrjene transakcije, oblikujejo blok in porabijo energijo za iskanje dragocenega ključa, ki doda blok in mu zagotovi mesto v verigi blokov.**

Rudarji tekmujejo v dodajanju naslednjega bloka v verigo blokov. Želena nagrada je »veljavna zgoščena vrednost bloka«, ki je spretno skrita med milijardami drugih, odklene pa jo lahko le poseben ključ, ki ga dodeli omrežje.

Predstavljajte si ogromno kopico sena z milijoni ključev, od katerih vsak predstavlja edinstveno zgoščeno vrednost bloka. Mreža je izbrala en poseben ključ, ki odklene dragoceno nagrado. Rudarji brskajo po kupu sena in preizkušajo vsak ključ v ključavnici, a le en srečnež bo našel pravega.

Ko rudar ugotovi pravilno zgoščeno vrednost bloka, ga deli z omrežjem skupaj z ustvarjenim blokom novih transakcij. Drugi rudarji preverijo, ali se rešitev ujema. Če je vse v redu, je blok dodan v verigo blokov, s čimer se ustvari varna in javna glavna knjiga.

Rudarji so za svoj trud nagrajeni na dva načina:



Nagrade za blok



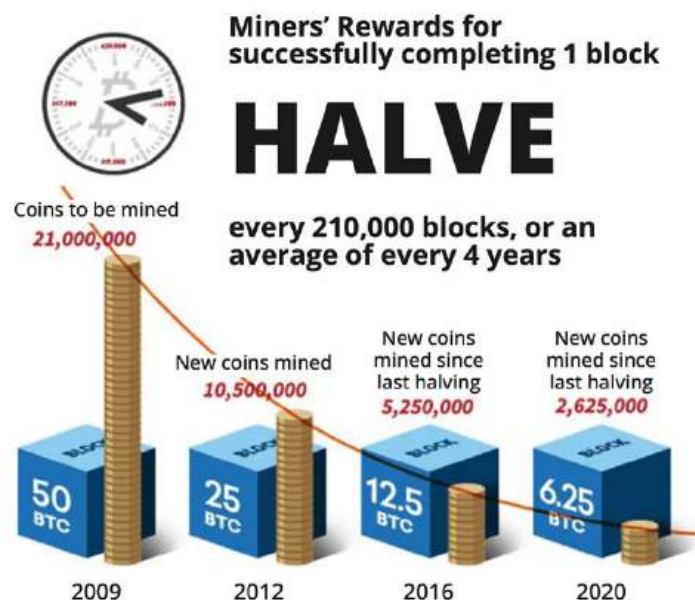
Transakcijske provizije

Nagrade za bloke so novi bitcoini, ki se sprostijo v obtok z vsakim blokom, dodanim v verigo blokov. Transakcijske provizije so majhna plačila, ki jih uporabniki bitcoinov plačajo, da bi rudar hitreje obdelal njihove transakcije in jim dal prednost. Rudarji lahko izbirajo, katere transakcije bodo vključili v blok, ki ga rudarijo, pri čemer imajo običajno prednost tiste z višjimi transakcijskimi provizijami.

## Bitcoinova prepolovitev

Bitcoinova prepolovitev je ključni del sveta bitcoinov, s katerim je ohranjena njihova redkost in vrednost skozi čas. Kot veste, je skupno na voljo 21.000.000 bitcoinov. Ta zaloga ni bila v celoti na voljo od dneva zagona Bitcoina. Ta zaloga vstopa v svet bitcoinov postopoma.

Satoshi Nakamoto je spretno zasnoval sistem nagrajevanja blokov za razdeljevanje novih bitcoinov brez osrednjega nadzornega organa. V prvih dneh Bitcoina so rudarji za vsak izkopani blok dobili nagrado 50 bitcoinov, kar jih je spodbudilo, da so vlagali v zmogljivo opremo in električno energijo za rudarjenje.



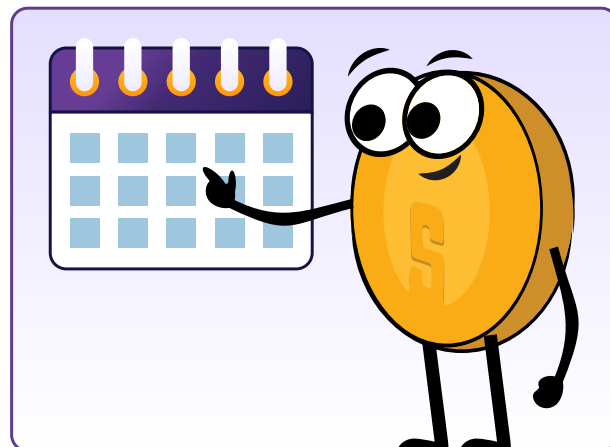
Nagrada za blok je prepolovljena približno vsakih 210.000 blokov. Na ta način je zagotovljena stabilnost omrežja in nadzor nad ponudbo novih bitcoinov. Ta dogodek, imenovan »prepolovitev«, zmanjša število novih bitcoinov, ki pridejo v obtok, in še naprej spodbuja rudarje k zaščiti omrežja in ohranjanju njegove decentralizacije. Zgodovinsko gledano so dogodki prepolovitve zaradi zmanjšane ponudbe novih bitcoinov, ki so prišli v obtok, povzročili znatno povišanje cen na trgu bitcoinov.

**Zaloga v obtoku se nanaša na skupno količino valute. Pri Bitcoinu je skupna zaloga v obtoku število kovancev, ki so bili pridobljeni z rudarjenjem in so v obtoku v danem trenutku, brez kovancev, ki so za vedno izgubljeni.**



Med vsakim dogodkom prepolovitve rudarji prejmejo manj nagrade v obliki bitcoina, kar zmanjša hitrost izdajanja novih kovancev. Posledično se zahtevnost rudarjenja bitcoinov povečuje, čas pridobivanja bloka pa ostaja nespremenjen pri približno 10 minutah. To zagotavlja, da se v verigo blokov stalno dodajajo novi bloki. Zmanjšanje nagrad za rudarjenje ne pomeni nujno, da rudarji zaslužijo manj, saj lahko zaslužijo tudi transakcijske pristojbine za preverjanje transakcij in dodajanje v verigo blokov, kar lahko izravna nižje nagrade za rudarjenje.

Dogodki prepolovitve so vnaprej programirani v Bitcoinovem protokolu, zato je urnik zaloge bitcoinov predvidljiv in pregleden.

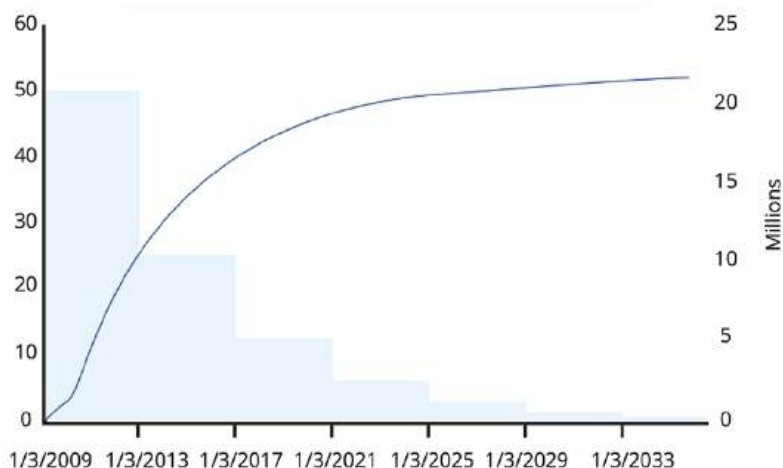


Urn timer zaloge bitcoinov je vnaprej določen in javno dostopen načrt izdajanja novih bitcoinov v obtok, ki je namenjen ohranjanju redkosti bitcoinov v daljšem časovnem obdobju.



V spodnji preglednici so opisane podrobnosti o prihajajočih dogodkih Bitcoinove prepolovitve, vključno s pričakovanim datumom naslednjega dogodka prepolovitve, številko bloka, pri katerem se bo dogodek prepolovitve izvedel, nagradami za blok (pridobljen z rudarjenjem) v času prepolovitve in odstotkom celotne zaloge, ki bo pridobljena z rudarjenjem.

**Bitcoin Supply Schedule**



Dogodek	Pričakovani datum	Blok	Nagrada za blok	Odstotek izkopanega
Četrta prepolovitev	2024	840.000	3,125	96,875 %
Peta prepolovitev	2028	1.050.000	1,5625	98,4375 %
Šesta prepolovitev	2032	1.260.000	0,78125	99,21875 %



# Uvod v tehnično plat Bitcoin

Ko je z rudarjenjem pridobljenih vse več bitcoinov, se ponudba v obtoku in odstotek celotne ponudbe, ki je bila pridobljena z rudarjenjem, povečujeta, dokler ni dosežena skupna ponudba 21.000.000 bitcoinov. Zmanjšana ponudba lahko skupaj z naraščajočim povpraševanjem poveča ceno bitcoina (merjeno v dolarjih). Od tega imajo korist zgodnji uporabniki, rudarje pa motivira, da še naprej varujejo omrežje ter prispevajo svojo računalniško moč in vire.

Bitcoin: Percent of 21M Supply Mined



## Kaj je veljavna zgoščena vrednost bloka v Bitcoinu?

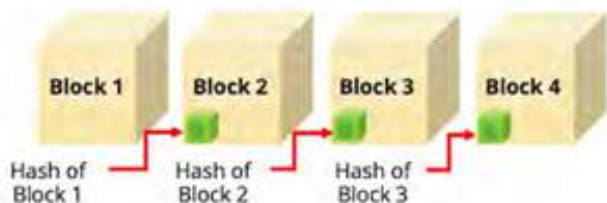
V Bitcoinu je veljavna zgoščena vrednost bloka nekakšna posebna koda, ki jo rudarji poskušajo najti. To je enolična številka, s katero je mogoče slediti vsakemu bloku v verigi blokov, v kateri so shranjene informacije o transakcijah. Bloki se povezujejo v verigo od prvega bloka (izvirnega bloka) do zadnjega, pri čemer so vse transakcije javno evidentirane. Ta zgoščena vrednost bloka je ključnega pomena, saj vsak blok povezuje s prejšnjim, kar vsakomur omogoča, da zlahka preveri zgodovino transakcij. To je nekakšen prstni odtis vsakega bloka, ki zagotavlja pravilnost in varnost podatkov. Z zgoščeno vrednostjo bloka se prepričamo, da



9ebtsznmfs7l4b876c5i7vo3bbv6kq4gem4ywzpu



The blocks are "linked" together by enforcing a specific relationship between blocks. That is, a block must contain a "fingerprint", which is a hash value of the data of the previous block. A hash function can condense arbitrary message (the block information) to a fixed size (e.g., 160 bits) and produces a fingerprint of the message.

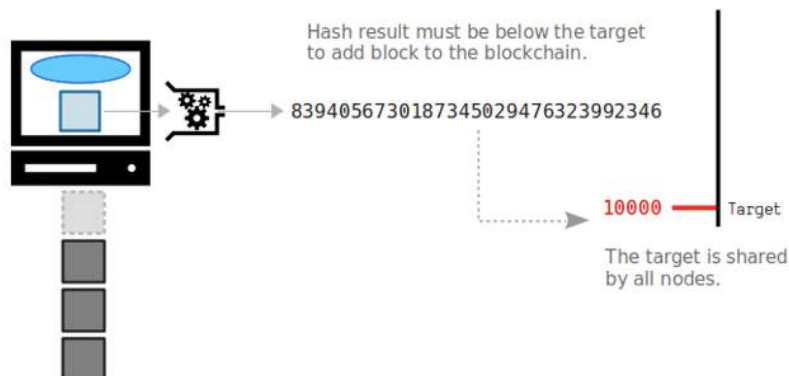


Satoshi Nakamoto, ustvarjalec Bitcoin, je z rudarjenjem pridobil začetni blok, v katerem je bilo skupaj 50 bitcoinov.

## Tekma za rudarjenje bloka

Rudarji med seboj tekmujejo, da bi odkrili zgoščeno vrednost bloka, ki ustreza cilju (posebnemu številu), ki ga določi omrežje. Rudar, ki prvi uspešno odkrije pravilno zgoščeno vrednost bloka, dobi možnost, da ta blok doda v verigo blokov in mu dodeli ustrezen ID zgoščene vrednosti. Ta rešitev deluje kot potrditev pristnosti bloka.

Rudarjenje lahko primerjamo z dirko, katere cilj je čim hitreje priti na cilj. Raven zahtevnosti iskanja zgoščene vrednosti bloka je redno prilagojena. S tem je zagotovljeno, da je za rudarjenje posameznega bloka še naprej potrebnih približno 10 minut (rudarji se pri tem pridružujejo in odhajajo). Ta mehanizem se imenuje »prilagoditev zahtevnosti«.



Vzemimo za primer, da je ciljno število, ki ga je določilo Bitcoinovo omrežje, 1000. Rudarji bi morali z zmogljivostjo računalnika in energijo najti zgoščeno vrednost bloka (specifično število), ki je manjše od 1000. Rudar, ki prvi najde zgoščeno vrednost bloka, nižjo od 1000, doda nov blok v verigo blokov in je nagrajen z bitcoini.

Raven težavnosti pri rudarjenju bitcoinov je merilo, kako težko je najti veljavno zgoščeno vrednost bloka, ki ustreza cilju, ki ga je določilo omrežje. Prilagojena je vsakih 2016 blokov ali približno vsaka dva tedna. Na ta način je zagotovljeno enakomerno dodajanje blokov v verigo blokov. Raven težavnosti je izražena s številom. Višja kot je raven težavnosti, težje je najti veljavno zgoščeno vrednost bloka.



Primerjajte na primer dve različni zgoščeni vrednosti:

 **Zgoščena vrednost 1:** 0000A1mINgF0RbL0cK5wltHth3hAy5tAcK  
**Raven težavnosti: 1**

 **Zgoščena vrednost 2:** 00000000A1mINgF0RbL0cK5wltHth3hAy5tAcK  
**Raven težavnosti: 2**

V tem primeru je raven težavnosti zgoščene vrednosti 2 višja kot pri zgoščeni vrednosti 1, ker je zgoščena vrednost daljša z več ničlami na začetku. Rudarji bi težje našli zgoščeno vrednost 2, saj bi morali njihovi računalniki opraviti več dela.

Ko rudar najde veljavno zgoščeno vrednost bloka, dokaže, da je opravil delo, potrebno za dodajanje novega bloka v verigo blokov. Za svoje delo prejme nagrado v bitcoinih ter transakcijske provizije. Dokaz o delu (PoW) je metoda, ki jo Bitcoinovo omrežje uporablja za potrjevanje transakcij in dodajanje novih blokov v verigo blokov.

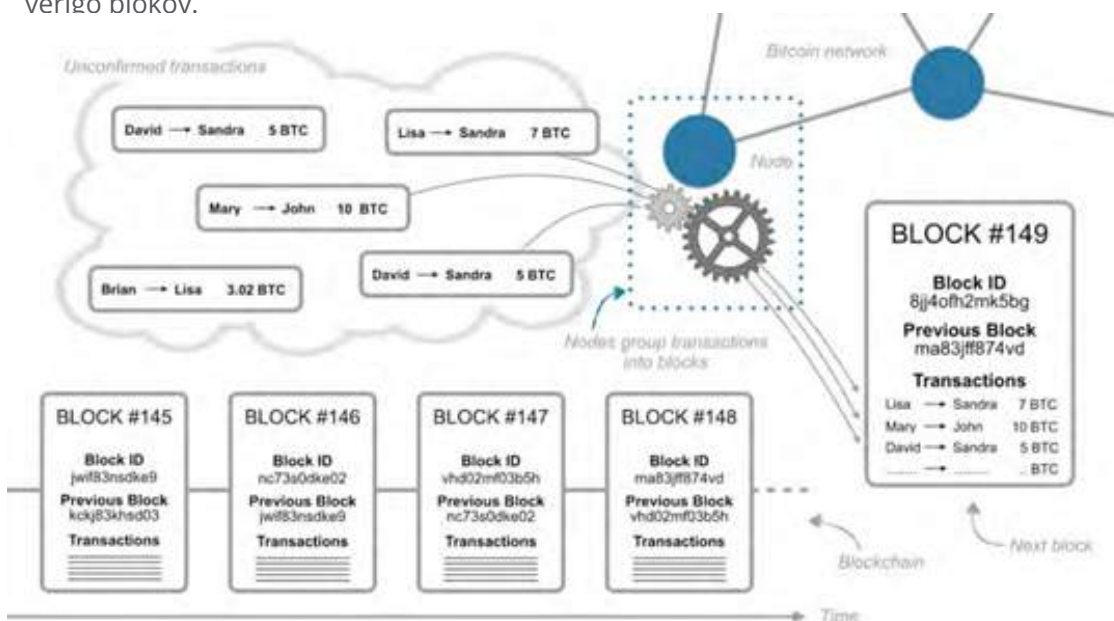


# Uvod v tehnično plat Bitcoina

Dokaz o delu (PoW) zagotavlja varnost Bitcoina, saj je težko, da bi kdo z zlonamernimi nameni prevzel nadzor nad njim.

Naloge rudarjev:

- 1 Združevanje transakcij v bloke:**  
Medtem ko vozlišča preverjajo novo ustvarjene transakcije, ki čakajo v bazenu transakcij, rudarji izberejo podmnožico teh transakcij, ki jih vključijo v svoj kandidatni blok.
- 2 Dokaz o delu (PoW):**  
Rudarji tekmujejo med seboj, da bi našli veljavno zgoščeno vrednost bloka.
- 3 Posredovanje veljavnih blokov:**  
Ko najdejo veljavno zgoščeno vrednost bloka, razširijo nov blok v omrežje.
- 4 Pridobivanje nagrad:**  
Na koncu prejmejo novo ustvarjene bitcoine in transakcijske provizije za uspešno dodan blok v verigo blokov.

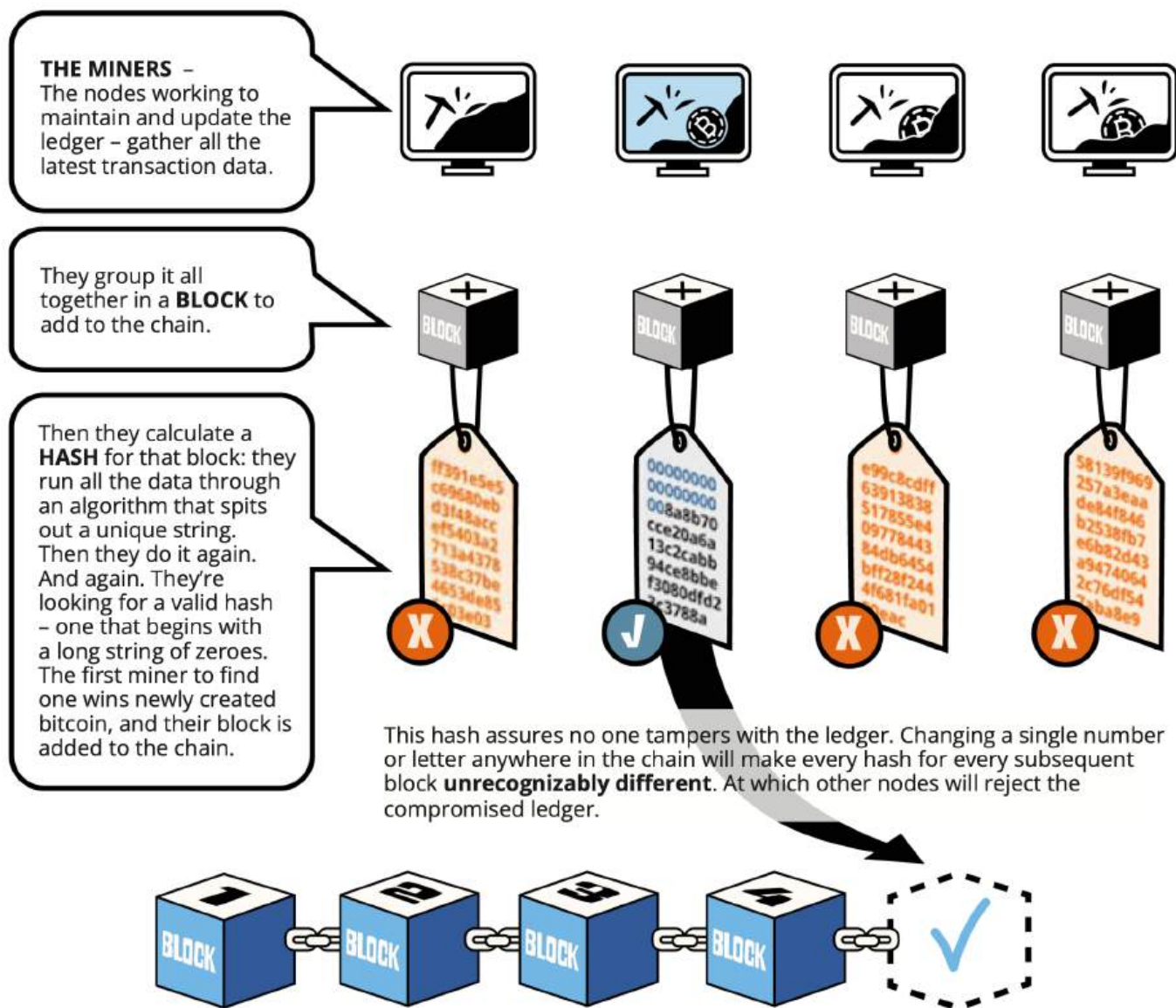


Več rudarjev lahko hkrati ustvarja nove bloke. Rudar, ki prvi odkrije zgoščeno vrednost bloka, ki ustreza cilju, ki ga je določilo omrežje, ga objavi v omrežju, drugi rudarji pa nato preverijo transakcije v kandidatnem bloku tega rudarja, da preverijo veljavnost. Če so transakcije res veljavne, je blok dodan v verigo blokov. Drugi bloki, ki so jih ustvarili drugi rudarji, niso dodani in so zavrženi. S tem postopkom je ohranjeno soglasje v omrežju in preprečena dvojna poraba.

Kandidatni blok je niz transakcij, ki so v obravnavi za dodajanje v verigo blokov, vendar še niso bile dodane.







## 9.4 Kaj je bazen transakcij?

»Bazen transakcij« ali pomnilniški bazen je kot čakalnica za transakcije v Bitcoinovem omrežju. Ko opravite transakcijo, je ta najprej posredovana v bazen transakcij, nato pa je preverjena, izbrana in dodana v verigo blokov.

Predstavljajte si, da čakate v vrsti v restavraciji. Vaše ime je dodano na seznam čakajočih za mizo. Ko je miza prosta, gostitelj pokliče vaše ime in vas posede. Podobno je transakcija z bitcoini dodana v bazen transakcij, ko jo rudar vključi v blok, pa je potrjena in dodana v verigo blokov.

# Uvod v tehnično plat Bitcoin

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

tx hsh 6053b699...  
fee rate: 3 sat/vB

tx hsh bb3b8cfc...  
fee rate: 1 sat/vB

tx hsh d7c2532a9...  
fee rate: 15 sat/vB

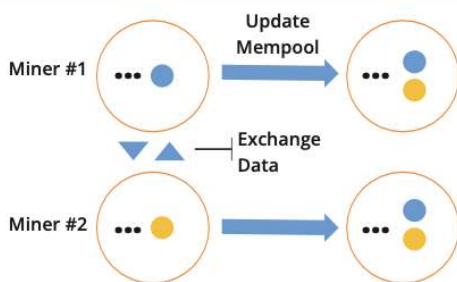
tx hsh 0ecdd9c6...  
fee rate: 2 sat/vB



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



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



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

1

Relay unconfirmed transactions.



2

Provide miners transactions to mine.



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

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

## Kako so transakcije preverjene in dodane v bazen transakcij?

Ko so v Bitcoinovo omrežje poslane nove transakcije, jih vozlišča preverijo in se prepričajo, da so veljavne in da sredstva še niso bila porabljena. Ko so te transakcije potrjene, jih vozlišča dodajo v svoj bazen transakcij. Vozlišča bodo nato transakcije delila z drugimi vozlišči, ki jih bodo še enkrat preverila. Če se večina vozlišč strinja, bodo transakcije dane na voljo rudarjem, da jih izberejo in vključijo v blok. Vendar obstaja več

1

**Nizke transakcijske provizije:**

Transakcije z nizko provizijo morda ne bodo obdelane dovolj hitro, saj bodo rudarji v svoje bloke najverjetneje vključili transakcije z višjimi provizijami.

2

**Preobremenitev omrežja:**

če je omrežje preobremenjeno, lahko pride do zamude pri potrjevanju transakcij, tudi če je njihova provizija visoka.

3

**Poskus dvojne porabe:**

če zlonamerni udeleženec poskuša podvojiti porabo, lahko omrežje njegovo transakcijo zavrne.

4

**Nepravilni ali nepopolni podatki:**

če so v transakciji napačni ali nepopolni podatki, jo lahko omrežje zavrne.

5

**Napačno oblikovana transakcija:**

če je transakcija napačno oblikovana, jo lahko omrežje zavrne.

Če se želimo izogniti zavrnitvi transakcij, je priporočljivo vključiti dovolj visoko provizijo, da je zagotovljena pravočasna obdelava transakcije, in pred pošiljanjem transakcije dvakrat preveriti, ali so vsi podatki v njej pravilni.

**Dejavnost: Bazen transakcij**









1

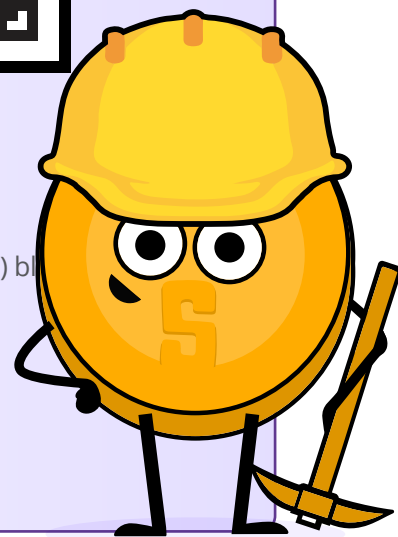
Optično preberite naslednjo kodo QR:

2

Preglejte različne elemente, prikazane na strani, vključno z zadnjimi bloki, potrjenimi transakcijami, številom transakcij, porabo pomnilnika in okvirno vrednostjo celotnega bloka. Odgovorite na vprašanja:



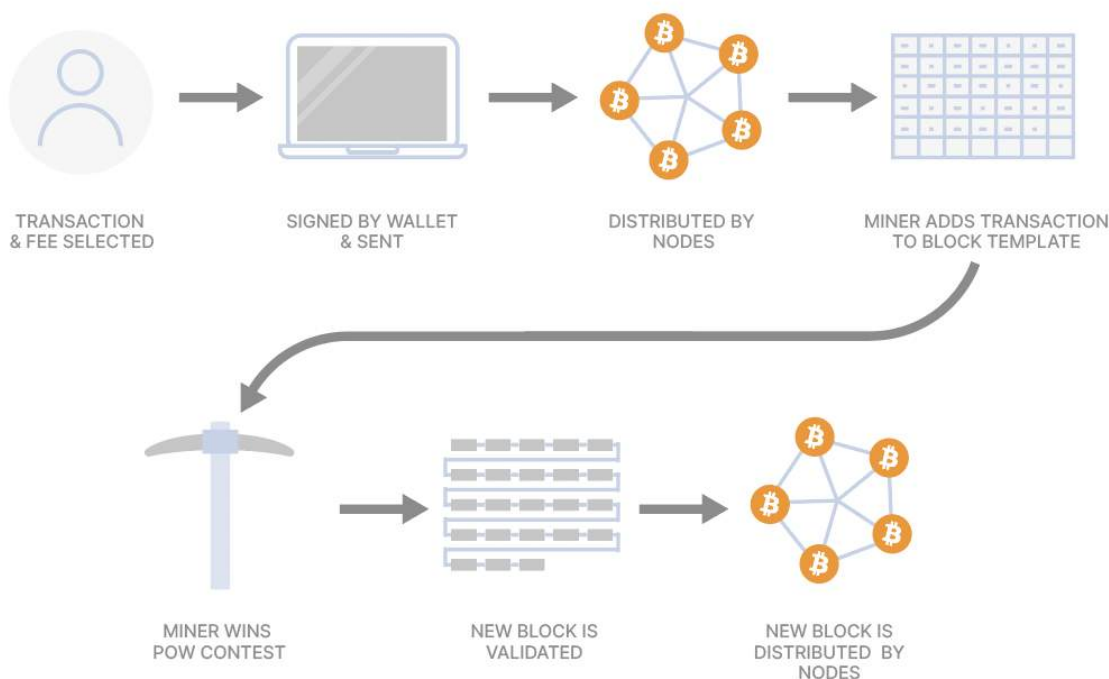
-  Kateri je bil zadnji blok, pridobljen z rudarjenjem?
-  Koliko transakcij je bilo vključenih v ta blok?
-  Kolikšna je skupna vrednost, s katero se trguje v bitcoinih?
-  Kakšna je bila velikost bloka v megabajtih?
-  S koliko ničlami se začne naključno enkratno število (angl. nonce) bloka?
-  Koliko bitcoinov je rudar skupaj zaslužil?
-  Kolikšna je bila skupna vrednost provizij, ki jih je rudar prejel za dodajanje transakcij v omrežje?
-  Izberite eno od transakcij z najvišjo vrednostjo v bloku. Na koliko Bitcoinovih naslovov je bil znesek razdeljen?



# Uvod v tehnično plat Bitcoina





## 9.5 Kako potekajo Bitcoinove transakcije od začetka do konca

- 1 Anže želi Goranu poslati bitcoine. Izbere enega od svojih neuporabljenih izhodov transakcij, ustvari transakcijo in doda vse potrebne podrobnosti, vključno z zneskom bitcoinov, ki jih želi poslati, Goranovim naslovom za prejemanje in nadpovprečno visokim zneskom transakcijskih provizij.
- 2 Po končnem preverjanju veljavnosti vseh podatkov Anže s svojim zasebnim ključem podpiše transakcijo.
- 3 Anže transakcijo objavi v omrežju Bitcoin.



Avtor: Stevenot, Ted: »Kaj je Bitcoinovo vozlišče in kako deluje?«. *Unchained Capital*, 17. januar, 2023, <https://unchained.com/blog/what-is-a-bitcoin-node/>

- 4 Vozlišča v omrežju prejmejo transakcijo in preverijo njeno veljavnost v skladu s pravili soglasja (na primer preverijo, ali je Jakobov podpis veljaven in ali ima dovolj sredstev za izvedbo transakcije).
- 5 Transakcija je označena kot veljavna, vozlišča jo razširijo na druga vozlišča v omrežju in jo dodajo v bazen transakcij.
- 6 Ker je Jakob izbral dovolj visoko transakcijsko provizijo, skoraj vsi rudarji njegovo transakcijo vključijo v svoje bloke.

-  7 Dokaz o delu (PoW): rudarji tekmujejo in skušajo z rudarjenjem pridobiti svoj blok tako, da najdejo veljavno zgoščeno vrednost bloka. Eden od rudarjev jo najde in svoj blok posreduje v omrežje.
-  8 Vozlišča prejmejo novo izkopani blok in preverijo njegovo veljavnost. To vključuje preverjanje vseh transakcij v bloku in zagotavljanje, da je izpolnjena zahteva za dokaz o delu (PoW).
-  9 Večina vozlišč se strinja, da je blok veljaven, in ga doda v verigo blokov. Goran prejme potrjene bitcoine na svoj naslov za prejemanje.
-  10 Ko so v verigo blokov v naslednji uri dodani dodatni bloki, se število potrditev za transakcijo poveča. Z večanjem števila potrditev transakcije postane Goran vse bolj prepričan v njen uspeh in nepovratno naravo.

Povedano na kratko: pošiljatelj podpiše transakcijo s svojim zasebnim ključem, vozlišča preverijo transakcijo neuporabljenih izhodov transakcij (UTXO), rudarji pa preverjeno transakcijo dodajo v verigo blokov. Prejemnik lahko nato do bitcoinov dostopa s svojim zasebnim ključem. Ko je rudarjenje bloka zaključeno, se vse transakcije, vključene vanj, štejejo za potrjene, neuporabljeni izhodi transakcij (UTXO), ki so bili uporabljeni kot vhodi v teh transakcijah, pa se štejejo za porabljene in ne bodo več uporabljeni.



Ob koncu tega poglavja ste pridobili dragocen vpogled v temeljne koncepte delovanja Bitcoina. Obravnavali smo bistvene vidike, od osnov denarja do tehnične plati Bitcoinove tehnologije. V naslednjem poglavju bomo vse skupaj povezali v enoto. Čaka nas 10. poglavje, v katerem se bomo poglobili v pomembno vprašanje: »Zakaj Bitcoin?«



## 10. poglavje

# ***Zakaj Bitcoin?***

### 10.0 Uvod

Dejavnost: kakšna je lahko prihodnost Bitcoina?

### 10.1 Kaj so centralnibančne digitalne valute (CBDC) in kdo jih nadzoruje?

### 10.2 Filozofija Bitcoina

Dejavnost: razprava v razredu – ali imate pravico do nadzora nad lastnim denarjem?

### 10.3 Prednosti Bitcoina

### 10.4 Opolnomočena prihodnost

Dejavnost: razprava v razredu – kako so se spremenili vaši pogledi?



# Zakaj Bitcoin?

## 10.0 Uvod

Bitcoin je več kot le valuta – je revolucija, ki vrača moč ljudem ter ponuja mir in svobodo v svetu, ki hrepeni po opolnomočenju.

Moj Prvi Bitcoin

V tem zaključnem poglavju bomo povzeli pridobljeno znanje v okviru te vsebine, zastavili nekaj pomembnih vprašanj in razpravljali o njih ter raziskali prihodnost Bitcoina.

Bitcoin ni le tehnologija, temveč vrsta omrežja, ki omogoča novo obliko denarja, katerega denarne mase ne more spreminjati noben posamezni udeleženec. Ljudje še nikoli nismo imeli na voljo oblike denarja s fiksno denarno maso in brez centraliziranega nadzora. Če bo Bitcoin široko sprejet, bo to orodje sprožilo gibanje pozitivnih sprememb, ki lahko izboljšajo življenja ljudi po svetu. Predstavlja mirno revolucijo v smeri kolektivne svobode in lastniških pravic, ki z vzpostavitvijo deljenega globalnega denarnega sistema odpira nove priložnosti za človeštvo.

Bitcoin kot decentralizirani globalni sistem zagotavlja večjo finančno svobodo in prenaša moč z manjšine na množico. Zagotavlja varno in proti cenzuri odporno platformo za shranjevanje in prenos vrednosti, tako da lahko posamezniki prevzamejo nadzor nad svojim premoženjem in zaščitijo kupno moč. To je še posebej pomembno v današnjih negotovih gospodarskih razmerah, ko se tradicionalni finančni sistem sooča s popolnoma novimi izzivi.

### Dejavnost: oglejte si videoposnetek

Možnosti za pozitivne spremembe so številne, zato si oglejte ta videoposnetek, kjer lahko pridobite več informacij.



V nadaljevanju je predstavljena še ena oblika digitalne valute, imenovana centralnobančna digitalna valuta (CBDC), ter podobnosti in razlike med njo in Bitcoinom.



## 10.1 Kaj so centralnbančne digitalne valute (CBDC) in kdo jih nadzoruje?

Centralnbančne digitalne valute ali CBDC so digitalne različice običajnih fiatnih valut. Za njih veljajo enaka pravila kot za fiatne valute, kjer lahko osrednji organ, kot je vlada, ustvari večjo denarno maso in s tem zmanjša kupno moč ljudi. Hkrati pa centralnbančne digitalne valute vladam zagotavljajo tudi nova in zmogljiva orodja, da lahko nadzirajo, kako ljudje po svetu uporabljajo ta denar.

Po podatkih raziskave Fundacije za človekove pravice (HRF) 119 od 193 vlad po svetu raziskuje, preizkuša ali uporablja centralnbančne digitalne valute.

Informacije o tem, ali vaša država uporablja centralnbančne digitalne valute, lahko preverite s sledilnikom CBDC Fundacije za človekove pravice na naslovu <https://cbdctracker.hrf.org/home> ali <https://cbdctracker.org/>

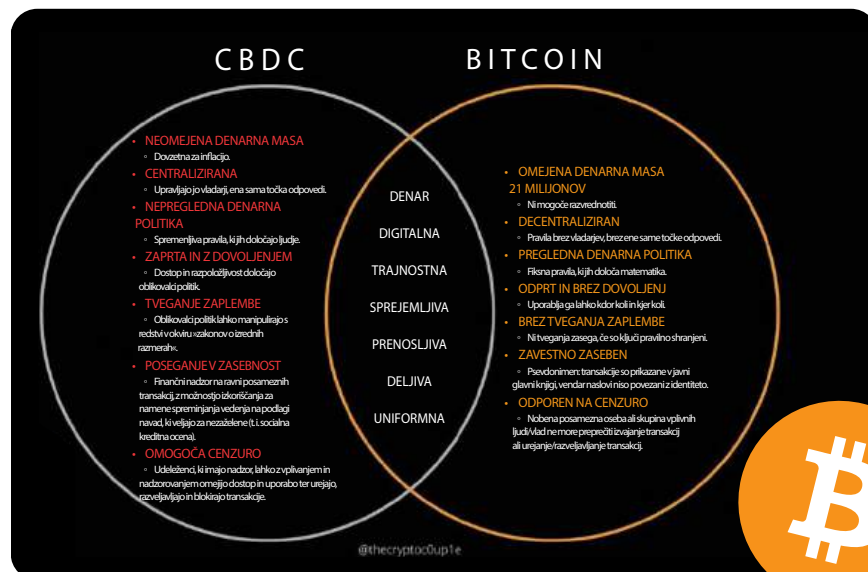


V čem se torej CBDC razlikujejo od običajnih fiatnih valut, razen tega, da so digitalne? Pomembno je razumeti, da v nasprotju z običajnimi fiatnimi valutami v obliki bankovcev ali kovancev centralnbančne digitalne valute vladi omogočajo digitalno spremljanje in nadzorovanje posameznih transakcij po svetu. To pomeni, da lahko vlada ustavi določene transakcije ali celo zamrzne celoten račun, če ji ni všeč določena oseba ali njen način uporabe denarja.

Predstavljajte si na primer, da želite poslati denar družinskemu članu v državo, ki potrebuje pomoč, vendar lokalna vlada zavrne vašo transakcijo, ker se ne strinja s politiko voditeljev te države. Ali pa, da greste na primer v trgovino in želite kupiti določeno stvar, ki vam je všeč, vendar je ne morete, ker ste izrazili svoje mnenje v družbenih omrežjih.

S centralnbančnimi digitalnimi valutami lahko vlade neomejeno nadzorujejo način uporabe denarja po svetu in omejujejo možnosti trošenja denarja posameznikov na osnovi njihovih odločitev. Nekateri so celo mnenja, da lahko centralnbančne digitalne valute omogočijo vplivnim vladam centralno uveljavljanje tiranskih politik na globalni ravni – z enim samim pritiskom – brez potrebnih človeških izvršilnih organov.

CBDC in Bitcoin sta digitalni valuti, vendar z izjemo te skupne značilnosti predstavljata zelo različni obliki denarja z različnimi filozofijami in pomenom za ljudi.



# Zakaj Bitcoin?

## 10.2 Filozofija Bitcoina

V 6. in 9. poglavju je predstavljeno, kako lahko posamezniki, ki vzpostavljajo vozlišča, zagotovijo varnost pravil Bitcoina. To je pomembna stvar, saj lahko vsi ljudje prvič v zgodovini postanemo del ekipe, ki ščiti pravila našega denarnega sistema. Ta pravila vključujejo dejstvo, da je na voljo le omejena količina denarja in da teh pravil ne more spremeniti noben posamezni udeleženec. To je edinstvena priložnost, da običajni ljudje pomagajo zagotoviti varnost in zanesljivost našega denarja.

Filozofija Bitcoina temelji na opolnomočenju, svobodi, finančni neodvisnosti, kritičnem razmišljanju in konceptu, da bi morali imeti vsi možnost odločanja o pravilih sistema, ki si ga sami izberemo. Za razliko od fiatnega sistema, ki ga nadzorujejo vplivne centralne entitete, Bitcoin deluje v omrežju, kjer noben posamezni udeleženec nima vsega nadzora. To pomeni, da vam v nasprotju z drugimi vrstami denarja, kot so centralnobańčne digitalne valute, nihče ne more vzeti vašega premoženja ali vam preprečiti, da bi denar potrošili kakor koli želite.

V svetu fiatnih valut več finančnih sredstev pomeni večji vpliv in nadzor. Nasprotno pa Bitcoin daje vso moč v roke ljudi. Temelji na ekipnem delu, kjer ima vsak posameznik, ne glede na to, koliko denarja ima, ključno vlogo v sistemu. Ima vlogo kolektivne sile, kjer z obsegom finančnih sredstev ne pridobite samodejno tudi nadzora nad vsem. Bitcoin temelji na nespremenljivih pravilih in v tej harmoniji je videti, kot da človeštvo samo nadzira sistem. Odločitev ne sprejema zgolj peščica vplivnih ljudi ali ena sama avtoriteta, temveč vsi sodelujemo skupaj kot odporna skupnost in usmerjamo tok Bitcoina.

Medtem ko v sistemu fiatnih valut vplivni narekujejo pravila, je v ekosistemu Bitcoina skupna moč posameznikov tista, ki vzdržuje omrežje. Noben posameznik, ne glede na svoje bogastvo, ne more narekovati poti ekosistema Bitcoina. Gre za preobrat tradicionalne dinamike vpliva, kjer odpornost sistema ni v rokah peščice, temveč v skupni moči posameznikov.

Glavni namen je ustvariti varen, pregleden in pravičen sistem, v katerem lahko vsi enakovredno dostopajo do svetovnega denarja.

### Dejavnost: razprava v razredu – ali imate pravico do nadzora nad lastnim denarjem?

- 1 Ali je denar človekova potreba ter pravica? In zakaj?
- 2 Če svojega denarja ne morete porabiti za kar koli želite, ga poslati komur koli želite oziroma ga odnesti s seboj v drugo državo, ali je pravzaprav res vaš? In zakaj?
- 3 Zakaj smo nehali uporabljati blagovno menjavo? V čem je težava dvojnega sovpadanja želja?
- 4 Kateri zgodovinski dogodek je bil za vas najbolj pomemben? Zakaj je pomembno razumeti Nixonov šok in njegov pomen za slehernega posameznika?
- 5 V čem se denar s fiksno denarno maso razlikuje od tradicionalnih fiatnih valut?

- 6 Kdaj je bilo ustvarjeno omrežje Bitcoin, kdo ga je ustvaril, s kakšnim namenom je bilo ustvarjeno in kako ta namen opredeljuje koncept decentraliziranega sistema?
- 7 Kakšna je razlika med skrbniško in neskrbniško denarnico? Katera je bila vaša najljubša denarnica?
- 8 Kaj veste o omrežju Lightning Network? Za katere vrste transakcij bi ga uporabljali?
- 9 Zakaj uporaba lastnega vozlišča podpira omrežje?
- 10 Kako vam nadzor nad lastnim denarjem pomaga v vsakdanjem življenju in pri načrtovanju prihodnosti?
- 11 Na kakšen način lahko finančna svoboda izboljša vašo sposobnost, da pozitivno prispevate k skupnosti ali družbi?

### 10.3 Prednosti Bitcoina

»Hiperbitcoinizacija« je teoretična prihodnost, v kateri je Bitcoin prevladujoči svetovni denarni sistem. To pomeni, da bi Bitcoin uporabljali vsi, povsod in za vse – za nakup kave, plačevanje računov in celo za nakup nepremičnin.

Vse večje zanimanje posameznikov, podjetij, držav in vlad za Bitcoin nakazuje na potencialni vpliv njegove široke uporabe na gospodarstvo in družbo. Tukaj je nekaj prednosti hiperbitcoinizacije:

- 1 **Prihodnost samostojnih identitet:**  
Prihodnost samostojnih identitet je prihodnost, v kateri imajo posamezniki po svetu popoln nadzor nad svojo digitalno identiteto in premoženjem. To bi lahko vodilo do večje finančne vključenosti, svobode, zasebnosti in varnosti ter hkrati do večje uspešnosti, izobilja in splošne sreče ljudi.
- 2 **Zanesljivo shranjevanje vrednosti:**  
Bitcoin je zaradi svoje digitalne redkosti zanesljiv vir shranjevanja vrednosti, kar bi lahko spodbudilo več ljudi k njegovi uporabi kot sredstva za varčevanje za prihodnost.
- 3 **Spremembe denarne politike:**  
Če bo omrežje Bitcoin široko sprejeto, lahko vladam onemogoči nadzor nad ponudbo denarja s tradicionalnimi orodji denarne politike. Množično sprejetje Bitcoina bi lahko potencialno povečalo kupno moč ljudi in spodbudilo družbo k preusmeritvi k dejavnostim z nizko časovno preferenco.
- 4 **Večja preglednost in sledljivost:**  
Z nespremenljivim zapisom vseh transakcij v verigi blokov, ki je zaščiten pred nedovoljenim spreminjanjem, lahko povečamo preglednost in odgovornost v različnih panogah in sektorjih. Trenutno lahko vplivne entitete po svetu pretakajo več bilijonov dolarjev brez jasnega vpogleda, kam so ta sredstva namenjena in kako se uporabljajo. Bitcoin bi lahko z odprtim in preverljivim zapisom finančnih transakcij zagotovil odgovornejši pretok kapitala, ki je hkrati tudi bolj dostopen javnosti.

# Zakaj Bitcoin?



Revolucija na trgu nakazil:

Trg nakazil vključuje prenos sredstev od enega udeleženca do drugega, pogosto prek mednarodnih meja. Kljub nižjim stroškom so nakazila še vedno dokaj draga v primerjavi z domačimi bančnimi prenosi, zlasti pri manjših zneskih. Omrežje Lightning Network omogoča hitre in cenovno ugodne transakcije, zaradi česar je primerno za trg nakazil. Odpravlja visoke stroške in druge izzive, povezane z nakazili, kot so počasne poravnave in omejitve delovnega časa.



Obilica energije:

Ko je na voljo veliko cenovno dostopne energije, je družba uspešna, številne industrije in skupnosti pa lahko zadovoljijo vse večje potrebe po energiji v gospodinjstvih, podjetjih in novih tehnologijah. Rudarjenje bitcoinov spodbuja rudarje k uporabi presežne energije, ki bi običajno ostala neuporabljena iz trajnostnih virov energije, kot so sončna, vetrna in vodna energija. Rudarji bitcoinov uporabljajo presežek energije za ustvarjanje novih bitcoinov z rudarjenjem, povečanje varnosti omrežja in vračanje presežne energije, ki jo ustvarijo v energetska omrežje, kjer jo nato družba uporablja za lastne potrebe.

## 10.4 Opolnomočena prihodnost

### Bitcoin je denar.

Denar ljudem sporoča, katere dejavnosti, dobrine in storitve so v družbi najpomembnejše. V okviru tega tečaja smo prišli do spoznanja, da je z denarjem mogoče manipulirati, če ga nadzorujejo centralizirane oblasti.

Ena od napak, ki jih je človeštvo v zgodovini nenehno ponavljalo, je manipuliranje z denarjem, kar negativno vpliva na posameznike, družine, podjetja, vlade in nenazadnje tudi na blaginjo celotnega človeštva.

S tem, ko nadzor nad denarjem vzamemo iz rok centraliziranih udeležencev in z uporabo denarja s fiksno denarno maso, ki je ne more spremeniti noben posamezni udeleženec, lahko ustvarimo drugačen svet – takšen, kjer se nam ni treba obremenjevati s tem, da bodo ljudje ravnali pravilno, temveč takšen, kjer ljudje ne morejo ravnati narobe.

To je bistveno drugačen svet.

In vi, dragi učenci, lahko sodelujete pri oblikovanju tega sveta. Z Bitcoinom, vzpostavitvijo lastnega vozlišča in s pomočjo sočloveku pri spoznavanju prihodnosti denarja glasujete za drugačen svet.

## Dejavnost: zaključna razprava v razredu – kako so se spremenili vaši pogledi?

Odgovorite na spodnjih pet vprašanj:



***Zakaj potrebujemo denar?***

---

---

---

---

---

---

---

***Kaj je denar?***

---

---

---

---

---

---

---

# ***Zakaj Bitcoin?***

***Kdo nadzoruje denar?***

---

---

---

---

---

---

---

---

***Kaj daje denarju »vrednost«?***

---

---

---

---

---

---

---

---

***Zapišite vprašanja učencev, ki so bila izbrana v 1. poglavju, in odgovorite nanje.***

---

---

---

---

---

---

---

1

Vrnite se k prvi dejavnosti v 1. poglavju in primerjajte nove odgovore s starimi.

2

Primerjajte izvirne odgovore in vprašanja ter razpravljajte o njih. Se je kaj spremenilo?

3

Zastavite si to zaključno vprašanje: kakšen je moj naslednji korak? Kako lahko uporabim to novo znanje za lastno opolnomočenje?



Če ste pripravljeni na naslednji korak, si oglejte dodatne vire v naslednjem razdelku, kjer so zbrani najboljši viri za nadaljnje učenje in uspeh.



## 1. Zakaj uporabljati Bitcoin?

**a** »The Bullish Case for Bitcoin« (Bikovski trend Bitcoina) avtorja Vijayja Boyapatija:

V tem članku so predstavljeni razlogi, zakaj je Bitcoin dragoceno sredstvo in zakaj lahko postane prevladujoča svetovna valuta. Avtor obravnava tehnične in ekonomske vidike Bitcoina, zaradi katerih je to učinkovita naložbena priložnost.

**b** »Why Bitcoin Matters« (Zakaj je Bitcoin pomemben) avtorja Aleksa Svetskega (1 ura):

V tem videoposnetku je predstavljen pomen Bitcoina kot decentraliziranega digitalnega premoženja in njegov vpliv na sedanji finančni sistem. Govornik raziše potencial Bitcoina pri zagotavljanju finančne svobode ljudem po svetu.

**c** »Why Bitcoin« (Zakaj Bitcoin) avtorja Wiza:

Ta članek vključuje pregled prednosti uporabe Bitcoina kot valute in hranilca vrednosti. Poudarjena je decentralizirana narava Bitcoina in kako ta zagotavlja večjo finančno svobodo ter varnost.

## 2. Kaj je Bitcoin?

**a** »How Bitcoin Works Under the Hood« (Vpogled v delovanje Bitcoina) avtorja CuriousInventor:

<https://www.youtube.com/watch?v=Lx9zgZCMqXE> V tem videoposnetku so podrobno pojasnjeni tehnični vidiki Bitcoina in njegovo delovanje.

**b** »What Is Bitcoin« (Kaj je Bitcoin) avtorja Grega Walkerja:

V tem članku je podrobno pojasnjeno, kaj je bitcoin, vključno z njegovo zgodovino, tehnologijo in razlikami v primerjavi s tradicionalnimi valutami.

**c** »Bitcoin - The Genesis« (Bitcoin – geneza) avtorja RT (30 minut):

V tem videoposnetku so predstavljeni vzpostavitev in začetki Bitcoina. Razloženi so vzgibi skrivnostnega ustvarjalca Satoshija Nakamota in razvoj Bitcoinovega koncepta.

## 3. Nadaljnje učenje:

**a** »The Bitcoin Standard« (Bitcoinov standard) (1 ura in 40 minut):

Ta zvočna knjiga raziskuje gospodarski in zgodovinski kontekst, ki je privedel do vzpostavitve Bitcoina. V njej so predstavljene prednosti decentralizirane valute in možnosti, da Bitcoin postane svetovni standard.

**c** »Bitcoin Babies« (Bitcoinovi dojenčki)

Avtorice Naomi Wambui - <https://bitcoinbabies.com/>  
Twitter: @btcbabies - @ngachanaomi1  
Brezplačni vir PDF, katerega namen je opolnomočiti matere s pomembnim znanjem glede prehrane, Bitcoina in splošnega duševnega počutja.

**b** »Intro to Bitcoin Austrian Thought« (Uvod v avstrijsko miselnost o Bitcoinu) (1 ura):

V tem zvočnem tečaju je predstavljena avstrijska ekonomska šola in njena povezanost s konceptom Bitcoina. Tečaj vključuje podroben vpogled v ekonomska načela Bitcoina in njihovo usklajenost z avstrijsko miselnostjo.

**d** »BTC Sessions« (Seje BTC)

YouTubeov izobraževalni kanal samo za Bitcoin z uporabnimi navodili in smernicami:  
<https://www.youtube.com/@BTCSessions>

## 4. Tečaji:

**a** »Summer of Bitcoin« (Poletje z Bitcoinom)

<https://www.summerofbitcoin.org/>: globalni spletni program poletne prakse, kjer se univerzitetni študenti seznanijo z odprtokodnim razvojem in načrtovanjem Bitcoina.











## Chaincode Labs

<https://learning.chaincode.com/#FOSS>: spletni tečaji in specializirani program, kjer se učenci pridobijo strokovno znanje, potrebno za delo pri razvoju Bitcoinovega protokola.

## Saylor Academy

Brezplačno izobraževanje na več področjih:  
<https://www.saylor.org/>

## 5. Pomembni avtorji

-  Alex Gladstein: »Check Your Financial Privilege« (Preverite svoj finančni privilegij)
-  Alex Swan: »Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications« (Terapija z utemeljenim nasprotovanjem: perspektive, značilnosti in načini uporabe)
-  Amanda Cavaleri: »Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide«
-  Anita Posch: »Learn Bitcoin: Become Financially Sovereign« (Naučite se uporabljati Bitcoin: postanite finančno neodvisni)
-  Eric Yakes: »The 7th Property: Bitcoin and the Monetary Revolution« (Sedma lastnina: Bitcoin in denarna revolucija)
-  Jeff Booth: »The Price of Tomorrow: Why Deflation is the Key to an Abundant Future« (Jutrišnja cena: zakaj je deflacija ključ do prihodnosti izobilja)
-  Jimmy Song: »The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future« (Mala knjiga o Bitcoinu: zakaj je Bitcoin pomemben za vašo svobodo, finance in prihodnost)
-  Nik Bhatia: »Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies« (Večplastni denar: od zlata in dolarjev do bitcoinov in centralnobančnih digitalnih valut)
-  Robert Breedlove: »Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money« (Hvala za Bitcoin: ustvarjanje, korupcija in odkup denarja)
-  Lyn Alden: »Broken Money« (Uničen denar)

## 6. Citirani avtorji

 Curious Inventor:  
<https://www.youtube.com/@CuriousInventor>

 Anil Patel:  
Twitter: @anilsaidso

Lorem ipsum

## 7. Drugi viri:

-  Bitcoin.org: uradna spletna stran Bitcoinovega protokola.
-  Bitcointalk.org: Bitcointalk je forum, kjer lahko uporabniki razpravljajo o temah, povezanih z Bitcoinom, zastavljajo vprašanja in izmenjujejo informacije. To je odlično mesto za pridobivanje informacij od drugih navdušencev in strokovnjakov za Bitcoin.
-  Bitcoincore.org: to je izvirna programska oprema Bitcoin, ki je še vedno široko razširjena me številnimi uporabniki in razvijalci. Zagotavlja zmogljiv nabor orodij za interakcijo z omrežjem Bitcoin in graditev Bitcoinovih aplikacij.
-  Bitcoinwiki.org: to je vir, ki ga vodi skupnost in zagotavlja celovit priročnik za vse, kar je povezano z Bitcoinom. Vključuje različno vsebino – od tehničnih vidikov Bitcoina do njegove zgodovine in primerov uporabe.
-  Bitcoinmagazine.com: to je spletna publikacija z novicami in vpogledi v Bitcoin ter druge kriptovalute. Zagotavlja odličen vir za vpogled v najnovejše dogodke v Bitcoinovem ekosistemu.
-  Bitcoin.Design: odprtokodno skladišče datotek načrtov, povezanih z Bitcoinom, za ilustracije, spletna mesta, predloge in ikone.
-  NOSTR: <https://nostr.com/> - družbeno omrežje, kjer ste lastnik svojih podatkov.
-  Simple X: <https://simplex.chat/> - zasebni, decentralizirani aplikacijski protokol.
-  Vzpostavite vozlišče Bitcoin: Raspberry Pi DIY avtorja Keitha Mukaia: [https://github.com/kdmukai/raspi4\\_bitcoin\\_node\\_tutorial?ab=README-ov-file](https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?ab=README-ov-file)
-  Kako izbrati denarnico Bitcoin: <https://bitcoin.org/en/choose-your-wallet> - izberite ustrezno denarnico z uporabo novo pridobljenega znanja.
-  BitcoinIcons.com: - <https://bitcoinicons.com/> - zbirka brezplačnih Bitcoinovih ikon.
-  Bitcoin za lokalna podjetja: <https://bitcoinforlocalbusiness.com/> - Akomplet letakov za predstavitev vrednosti Bitcoina s priljubljenimi lokalnimi podjetji.
-  Mempool.Space: <https://mempool.space/> - odprtokodni projekt bazena transakcij, ki vključuje tudi podatke in grafe omrežja Lightning Network.

## 1. Zakaj uporabljati Bitcoin?

### »The Bullish Case for Bitcoin« (Bikovski trend Bitcoina) avtorja Vijayja Boyapatija:

V tem članku so predstavljeni razlogi, zakaj je Bitcoin dragoceno sredstvo in zakaj lahko postane prevladujoča svetovna valuta. Avtor obravnava tehnične in ekonomske vidike Bitcoina, zaradi katerih je to učinkovita naložbena priložnost.

### »Why Bitcoin Matters« (Zakaj je Bitcoin pomemben) avtorja Aleksa Svetskega (1 ura):

V tem videoposnetku je predstavljen pomen Bitcoina kot decentraliziranega digitalnega premoženja in njegov vpliv na sedanji finančni sistem. Govornik raziše potencial Bitcoina pri zagotavljanju finančne svobode ljudem po svetu.

### »Why Bitcoin« (Zakaj Bitcoin) avtorja Wiza:

Ta članek vključuje pregled prednosti uporabe Bitcoina kot valute in hranilca vrednosti. Poudarjena je decentralizirana narava Bitcoina in kako ta zagotavlja večjo finančno svobodo ter varnost.

## 2. Kaj je Bitcoin?

### »How Bitcoin Works Under the Hood« (Vpogled v delovanje Bitcoina) avtorja CuriousInventor:

<https://www.youtube.com/watch?v=Lx9zgZCMqXE> V tem videoposnetku so podrobno pojasnjeni tehnični vidiki Bitcoina in njegovo delovanje.

### »What Is Bitcoin« (Kaj je Bitcoin) avtorja Grega Walkerja:

V tem članku je podrobno pojasnjeno, kaj je bitcoin, vključno z njegovo zgodovino, tehnologijo in razlikami v primerjavi s tradicionalnimi valutami.

### »Bitcoin - The Genesis« (Bitcoin – geneza) avtorja RT (30 minut):

V tem videoposnetku so predstavljeni vzpostavitev in začetki Bitcoina. Razloženi so vzgibi skrivnostnega ustvarjalca Satoshija Nakamota in razvoj Bitcoinovega koncepta.

## 3. Nadaljnje učenje:

### »The Bitcoin Standard« (Bitcoinov standard) (1 ura in 40 minut):

Ta zvočna knjiga raziskuje gospodarski in zgodovinski kontekst, ki je privedel do vzpostavitve Bitcoina. V njej so predstavljene prednosti decentralizirane valute in možnosti, da Bitcoin postane svetovni standard.

### »Bitcoin Babies« (Bitcoinovi dojenčki)

Avtorice Naomi Wambui - <https://bitcoinbabies.com/>  
Twitter: @btcbabies - @ngachanaomi1  
Brezplačni vir PDF, katerega namen je opolnomočiti matere s pomembnim znanjem glede prehrane, Bitcoina in splošnega duševnega počutja.

### »Intro to Bitcoin Austrian Thought« (Uvod v avstrijsko miselnost o Bitcoinu) (1 ura):

V tem zvočnem tečaju je predstavljena avstrijska ekonomska šola in njena povezanost s konceptom Bitcoina. Tečaj vključuje podroben vpogled v ekonomska načela Bitcoina in njihovo usklajenost z avstrijsko miselnostjo.

### »BTC Sessions« (Seje BTC)

YouTubeov izobraževalni kanal samo za Bitcoin z uporabnimi navodili in smernicami:  
<https://www.youtube.com/@BTCSessions>

## 4. Tečaji:

### »Summer of Bitcoin« (Poletje z Bitcoinom)

<https://www.summerofbitcoin.org/>: globalni spletni program poletne prakse, kjer se univerzitetni študenti seznanijo z odprtokodnim razvojem in načrtovanjem Bitcoina.











## Chaincode Labs

<https://learning.chaincode.com/#FOSS>: spletni tečaji in specializirani program, kjer se učenci pridobijo strokovno znanje, potrebno za delo pri razvoju Bitcoinovega protokola.

## Saylor Academy

Brezplačno izobraževanje na več področjih:  
<https://www.saylor.org/>

## 5. Pomembni avtorji

-  Alex Gladstein: »Check Your Financial Privilege« (Preverite svoj finančni privilegij)
-  Alex Swan: »Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications« (Terapija z utemeljenim nasprotovanjem: perspektive, značilnosti in načini uporabe)
-  Amanda Cavaleri: »Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide«
-  Anita Posch: »Learn Bitcoin: Become Financially Sovereign« (Naučite se uporabljati Bitcoin: postanite finančno neodvisni)
-  Eric Yakes: »The 7th Property: Bitcoin and the Monetary Revolution« (Sedma lastnina: Bitcoin in denarna revolucija)
-  Jeff Booth: »The Price of Tomorrow: Why Deflation is the Key to an Abundant Future« (Jutrišnja cena: zakaj je deflacija ključ do prihodnosti izobilja)
-  Jimmy Song: »The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future« (Mala knjiga o Bitcoinu: zakaj je Bitcoin pomemben za vašo svobodo, finance in prihodnost)
-  Nik Bhatia: »Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies« (Večplastni denar: od zlata in dolarjev do bitcoinov in centralnobačnik digitalnih valut)
-  Robert Breedlove: »Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money« (Hvala za Bitcoin: ustvarjanje, korupcija in odkup denarja)
-  Lyn Alden: »Broken Money« (Uničen denar)

## 6. Citirani avtorji

 Curious Inventor:  
<https://www.youtube.com/@CuriousInventor>

 Anil Patel:  
Twitter: @anilsaidso

Lorem ipsum

## 7. Drugi viri:

-  Bitcoin.org: uradna spletna stran Bitcoinovega protokola.
-  Bitcointalk.org: Bitcointalk je forum, kjer lahko uporabniki razpravljajo o temah, povezanih z Bitcoinom, zastavljajo vprašanja in izmenjujejo informacije. To je odlično mesto za pridobivanje informacij od drugih navdušencev in strokovnjakov za Bitcoin.
-  Bitcoincore.org: to je izvirna programska oprema Bitcoin, ki je še vedno široko razširjena me številnimi uporabniki in razvijalci. Zagotavlja zmogljiv nabor orodij za interakcijo z omrežjem Bitcoin in graditev Bitcoinovih aplikacij.
-  Bitcoinwiki.org: to je vir, ki ga vodi skupnost in zagotavlja celovit priročnik za vse, kar je povezano z Bitcoinom. Vključuje različno vsebino – od tehničnih vidikov Bitcoina do njegove zgodovine in primerov uporabe.
-  Bitcoinmagazine.com: to je spletna publikacija z novicami in vpogledi v Bitcoin ter druge kriptovalute. Zagotavlja odličen vir za vpogled v najnovejše dogodke v Bitcoinovem ekosistemu.
-  Bitcoin.Design: odprtokodno skladišče datotek načrtov, povezanih z Bitcoinom, za ilustracije, spletna mesta, predloge in ikone.
-  NOSTR: <https://nostr.com/> - družbeno omrežje, kjer ste lastnik svojih podatkov.
-  Simple X: <https://simplex.chat/> - zasebni, decentralizirani aplikacijski protokol.
-  Vzpostavite vozlišče Bitcoin: Raspberry Pi DIY avtorja Keitha Mukaia: [https://github.com/kdmukai/raspi4\\_bitcoin\\_node\\_tutorial?ab=README-ov-file](https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?ab=README-ov-file)
-  Kako izbrati denarnico Bitcoin: <https://bitcoin.org/en/choose-your-wallet> - izberite ustrezno denarnico z uporabo novo pridobljenega znanja.
-  BitcoinIcons.com: - <https://bitcoinicons.com/> - zbirka brezplačnih Bitcoinovih ikon.
-  Bitcoin za lokalna podjetja: <https://bitcoinforlocalbusiness.com/> - Akomplet letakov za predstavitev vrednosti Bitcoina s priljubljenimi lokalnimi podjetji.
-  Mempool.Space: <https://mempool.space/> - odprtokodni projekt bazena transakcij, ki vključuje tudi podatke in grafe omrežja Lightning Network.

# Ključni koncepti poglavij

## 1. poglavje



### Uvod v tečaj

Spoznajte cilje in pričakovanja tečaja za Diplomsko Bitcoin.



### Refleksivna dejavnost – opredelitev denarja

Sodelujte v refleksivni vaji in navedite pet odgovorov na ključna vprašanja o denarju.



### Razprava v razredu – zakaj potrebujemo denar

- ✿ Sodelujte v razpravi v razredu o temeljni potrebi po denarju.
- ✿ Izmenjajte in primerjajte posamezne poglede na pomen denarja.
- ✿ Določite temelje za razumevanje vloge denarja v gospodarskih sistemih.

## 2. poglavje



### Razumevanje denarja

- ✿ Raziščite temeljno definicijo in pojem denarja.
- ✿ V razredu razpravljajte o različnih pogledih za razumevanje večplastne narave denarja.



### Psihologija denarja

- ✿ Pridobite vpogled v psihološke vidike denarja, vključno s redkostjo, časovno preferenco in kompromisi.
- ✿ Sodelujte v dejavnosti »časovne preference« in povežite psihološke elemente s scenariji iz resničnega življenja.



### Funkcije, lastnosti in vrste

- ✿ Spoznajte funkcije, lastnosti in vrste denarja.
- ✿ Prepoznavajte pomen teh vidikov pri definiranju in uporabi denarja.

## 3. poglavje



### Uvod v zgodovino in razvoj denarja

Raziščite zgodovino in razvoj denarja. Spoznajte, kako so starodavne oblike trgovanja privedle do razvoja valute, ki jo uporabljamo danes.



### Revolucija digitalne valute

- ✿ Odkrijte sedanji vrhunec razvoja denarja – digitalno valuto.
- ✿ Spoznajte, kako je na voljo le v elektronski obliki ter omogoča takojšnje in poceni globalne transakcije.
- ✿ Spoznajte pomembno vlogo Bitcoina pri reševanju začetnih izzivov na področju digitalnih valut in sprejemanju njihove uporabe po svetu.



### Razvoj valute

Raziščite prehod od starodavnih načinov plačevanja, kot so školjke in biseri, do uveljavitve kovancev in papirnatega denarja. Spremljajte razvoj valute skozi zgodovino – od papirja do plastike.



### Dejavnost igre blagovne menjave

Sodelujte v praktični igri blagovne menjave, da spoznate izzive neposredne menjave in potrebe po uveljavitvi učinkovitejšega sistema.

## 4. poglavje



### Izvor fiatnega denarja:

Spoznajte izvor fiatnega denarja v strnjem zgodovinskem pregledu in ugotovite, kako se je razvil v prevladujočo obliko valute.



### Dejavnost bančništva z delnimi rezervami

Sodelujte v dejavnosti bančništva z delnimi rezervami in pridobite vpogled v delovanje tega sistema, s poudarkom na odvisnosti od dolga in posledicah za širše gospodarstvo.



### Sistem fiatnih valut

Spoznajte temeljne pojme sistema fiatnih valut, vključno z njegovo naravo denarnega sistema z uredbo, vlogo bančništva z delnimi rezervami in ključnimi udeleženci, ki nadzorujejo ta sistem.

## 5. poglavje



### Zmanjševanje kupne moči

Pridobite vpogled v razumevanje pojma denarne inflacije in njegovega vpliva na kupno moč. Sodelujte pri učinkih inflacije: Dejavnost dražbe za pridobitev razumevanja učinka inflacije.



### Dejavnost »Vpliv sistema fiatnih valut«

Sodelujte pri dejavnosti »Vpliv sistema fiatnih valut«, z osredotočenostjo na posledice sedanjega denarnega sistema.



### Centralnobančne digitalne valute (CBDC)

Raziščite razvijajoče se okolje centralnobančnih digitalnih valut (CBDC) in njihov potencialni vpliv na prihodnost denarja.



### Breme globalnega dolga in socialna neenakost

Raziščite dvojne učinke bremena globalnega dolga in družbene neenakosti. Prepoznajte posledice za posameznike in družbo, s poudarkom na izgubi kupne moči in vse večji premoženjski vrzeli.



### Cypherpunkovci in decentralizacija

Spoznajte zgodbo cypherpunkovcev in njihovo motivacijo pri iskanju decentralizirane valute. Razlikujte med centraliziranimi in decentraliziranimi sistemi ter pridobite vpogled v zgodovino digitalnih valut.

## 6. poglavje



### Satoshi Nakamoto in vzpostavitev Bitcoina

Spoznajte skrivnostno osebnost – Satoshija Nakamota – in zgodbo o izvoru Bitcoina ter pridobite vpogled v začetne vzgibe za njegovo vzpostavitev.



### Dejavnost v razredu – doseganje soglasja

Sodelujte pri dejavnosti doseganja soglasja v omrežju enakovrednih udeležencev in pridobite praktičen vpogled v način doseganja soglasja v omrežju Bitcoin.



### Sprejemanje osebne odgovornosti

Poudarite pomen osebne odgovornosti v Bitcoinovem kontekstu, s spodbujanjem razumevanja vlog posameznika in odgovornosti v decentraliziranem ekosistemu.



### Kako deluje Bitcoin

Vpogled v mehanizme Bitcoina, vključno z mehanizmom Nakamotovega soglasja. Prepoznajte ključne udeležence v omrežju Bitcoin, kot so rudarji, vozlišča, uporabniki, razvijalci in projekti, ter pridobite vpogled v dinamiko medsebojnega sodelovanja.



### Bitcoin kot stabilni digitalni denar

Raziščite vlogo Bitcoina kot stabilnega digitalnega denarja, razpravljajte o njegovem razvoju, funkcijah in lastnostih ter sodelujte v razpravi v razredu o tem, ali bitcoin izpolnjuje pogoje za uveljavitev kot stabilni denar.

# Ključni koncepti poglavij

## 7. poglavje



### Transakcije med enakovrednimi udeleženci

Sodelujte v decentraliziranih transakcijah in spoznajte temeljna načela Bitcoinovih izmenjav.



### Namestitev denarnice Bitcoin

Spoznajte pomembne korake za prenos, ustvarjanje ključev ter varnostno kopiranje denarnice Bitcoin za izvajanje varnih transakcij.



### Hranjenje in DYOR

Pridobite vpogled v varčevanje v Bitcoinu kot hranilcu vrednosti in spoznajte pomembnost neodvisnih raziskav za sprejemanje informiranih odločitev.



### Vrste Bitcoinovih denarnic

Razlikujte med odprtokodnimi, zaprtokodnimi, skrbniškimi in neskrbnimi denarnicami ter pridobite vpogled v vlogo ključev na področju varnosti.



### Pridobitev bitcoinov

Raziščite metode, kot so transakcije in izmenjave med enakovrednimi udeleženci ter razpravljajte o vprašanjih glede zasebnosti, povezanih s postopki KYC.

## 8. poglavje



### Uvod v omrežje Lightning Network

Spoznajte razvoj Bitcoina prek tehnologij, kot je Lightning Network, ki izboljšujejo njegove zmogljivosti.



### Namestitev denarnice Lightning

Spoznajte pomembne korake za namestitev denarnice Bitcoin Lightning za opravljanje hitrejših in bolj skalabilnih transakcij.



### Praktična dejavnost

Sodelujte v praktični dejavnosti štafete v denarnici Lightning, s čimer spodbudite dinamično razumevanje transakcij v omrežju Lightning Network.



### Vrste denarnic Lightning

Razlikujte med odprtokodnimi, zaprtokodnimi, skrbniškimi in neskrbnimi denarnicami Lightning za različne uporabniške potrebe.



### Transakcije Lightning

Raziščite postopek pošiljanja in prejemanja transakcij Lightning, s poudarkom na hitrosti in učinkovitosti omrežja Lightning.

## 9. poglavje



### Bitcoinova glavna knjiga

Pridobite vpogled v koncept decentralizirane glavne knjige, ki jo omogočajo vozlišča in rudarji ter zagotavlja preglednost in varnost.



### Model UTXO

Pridobite vpogled v model neporabljenih izhodov transakcij (UTXO) kot temeljnega dejavnika postopka Bitcoinovih transakcij.



### Javni in zasebni ključi

Spoznajte pomen kriptografske varnosti pri Bitcoinovih transakcijah z javnimi in zasebnimi ključi, skupaj z dejavnostjo, kjer je predstavljeno zgoščevanje SHA 256.



### Bitcoinova vozlišča in rudarji

Oglejte si vloge vozlišč in rudarjev pri vzdrževanju omrežja Bitcoin, kot so izdajanje, redkost, prepolovitve in težavnost.



### Kako potekajo Bitcoinove transakcije

Pridobite vpogled v celoten življenjski cikel Bitcoinovih transakcij, ki vključuje pošiljatelja, prejemnika, vozlišča, rudarje in bazen transakcij, z namensko dejavnostjo, osredotočeno na bazen transakcij.



## 10. poglavje



### Filozofski temelji Bitcoina

Spoznajte temeljno filozofijo Bitcoina, kako je bil vzpostavljen kot odgovor na gospodarske izzive, s poudarkom na njegovem vplivu na zagotavljanje finančne svobode in na tem, kako se razlikuje od tradicionalnih valut.





### Prihodnost Bitcoina

Spoznajte potencial in prihodnji razvoj Bitcoina kot revolucionarne digitalne valute.



### Povzemanje vsebine Diplome

-  Povzemite ključne ugotovitve Diplome Bitcoin in spodbudite učence k razmišljanju o vsebini in pridobljenih vpogledih.
-  Dejavnosti vključujejo ogled videoposnetka na temo »Zakaj Bitcoin?« in ponovni pregled vprašanj iz 1. poglavja za ocenitev razumevanja.

**51 % napad:** vrsta napada na omrežje verige blokov, pri katerem posamezen subjekt ali skupina nadzoruje večino računalniške zmogljivosti omrežja, zaradi česar lahko manipulira s transakcijami in povzroči motnje v delovanju omrežja.

**Sezona alternativnih kovancev:** obdobje, v katerem se cene alternativnih kriptovalut znatno zvišajo, pogosto zaradi povečanega zanimanja vlagateljev in sprejetja.

**Alternativni kovanci:** digitalne valute brez Bitcoina.

**Atomarna zamenjava:** zamenjava ene kriptovalute za drugo med enakovrednimi udeleženci brez uporabe centralizirane borze ali posrednika.

**Dražba:** postopek, kjer je blago ali premoženje prodano najvišjemu ponudniku.

**Blagovna menjava:** menjava blaga in storitev brez uporabe denarja.

**Košarica blaga:** zbirka blaga ali storitev, ki se uporablja za merjenje sprememb življenjskih stroškov.

**Bitcoin:** digitalna valuta/sistem, ki ljudem omogoča medsebojno pošiljanje denarja brez uporabe vmesnega posrednika.

**Raziskovalec blokov:** orodje za pregledovanje in raziskovanje verige blokov, s katerim si lahko uporabniki ogledajo posamezne bloke, transakcije in naslove denarnic.

**Nagrada za blok:** količina novih bitcoinov, ki jih rudarji prejmejo kot nagrado za dodajanje novega bloka v verigo blokov.

**Veriga blokov:** javni zapis vseh opravljenih transakcij z bitcoini.

**BTC:** enota, ki se uporablja za bitcoine. Digitalna valuta, s katero je mogoče opravljati nakupe ali z njo trgovati.

**Nadzor kapitala:** omejitve čezmejnega pretoka denarja.

**Centralna banka (Fed):** ustanova v državni lasti, ki upravlja denarno politiko države.

**Centralizacija:** koncentracija moči ali nadzora v enem subjektu.

**Centralizirani sistem:** sistem, v katerem je moč ali nadzor koncentriran v enem subjektu.

**Hladno shranjevanje:** metoda shranjevanja bitcoinov brez povezave, kjer ni nevarnosti vdora hekerjev ali drugih spletnih groženj.

**Naturalni denar:** predmeti, ki imajo sami po sebi vrednost in se uporabljajo kot menjalno sredstvo, na primer zlato ali srebro.

**Potrditev:** postopek, pri katerem omrežje obdela transakcijo, za katero je malo verjetno, da bo razveljavljena. Metoda, s katero rudarji preverijo pristnost transakcij s svojo strojno in programsko opremo. Priporočljivo je počakati na vsaj šest potrditev, da preprečite dvojno porabo.

**Mehanizem soglasja:** metoda, uporabljena v tehnologiji verige blokov za potrjevanje transakcij in zagotavljanje integritete verige blokov.

**Menjalnica kriptovalut:** platforma, kjer lahko uporabniki kupujejo in prodajajo kriptovalute ter trgujejo z njimi za druga sredstva, kot so fiat valute ali druge kriptovalute.

**Kriptovalutna denarnica:** program, kjer so shranjeni zasebni ključi in s katerim lahko uporabniki pošiljajo, prejemajo ter upravljajo kriptovalute.

**Kriptografija:** matematično področje ustvarjanja varnih sistemov.

**Razvrednotenje:** zmanjšanje vrednosti valute, pogosto z zmanjšanjem količine plemenite kovine v kovancu.

**Dolg:** denar, ki ga dolgujete drugemu.

**Decentralizacija:** porazdelitev moči in nadzora v omrežju namesto uveljavitve osrednjega organa.

**Decentralizirana avtonomna organizacija (DAO):** organizacija ali omrežje, ki ga upravljajo pametne pogodbe in deluje v verigi blokov brez osrednjega organa ali upravljalvske strukture.

**Decentralizirane finance (DeFi):** gibanje v panogi kriptovalut za ustvarjanje decentraliziranih finančnih produktov in storitev, ki delujejo v verigi blokov.

**Decentralizirani sistem:** sistem, v katerem je moč ali nadzor porazdeljen med več entitet.

**Digitalno sredstvo:** digitalna predstavitev vrednosti, s katero je mogoče trgovati ali jo uporabljati kot hranilec vrednosti, kot so bitcoini.

**Distribuirana glavna knjiga:** zbirka podatkov, ki je razpršena v omrežju računalnikov in ni shranjena na osrednji lokaciji.

**Dvojno sovpadanje želja:** pojav, ko imata dva udeleženca v ekonomiji z blagovno menjavo nekaj, kar želi drugi udeleženec, sama pa želita lastnino drugega udeleženca.

**Dvojna poraba:** ko poskuša oseba hkrati poslati svoje bitcoine dvema različnima prejemnikoma.

**Transakcija z minimalno vrednostjo:** transakcija izjemno majhne količine bitcoinov, ki je premajhna, da bi bila ekonomsko izvedljiva.

Menjalni tečaj: vrednost ene valute v razmerju do druge.

FOMO: bojazen pred zamujenimi priložnostmi – izraz, ki se uporablja za opis občutka tesnobe ali obžalovanja glede zamujene donosne priložnosti na trgu kriptovalut.

FUD: strah, negotovost in dvom – izraz, ki se uporablja za opis negativnih govoric ali informacij, ki lahko povzročijo paniko na trgu ali njegov padec.

BDP: bruto domači proizvod, skupna vrednost blaga in storitev, proizvedenih v državi v določenem časovnem obdobju.

Trda odcepitev: sprememba Bitcoinovega protokola, kjer je ustvarjena nova različica verige blokov, ki ni združljiva s prejšnjo različico (npr. Bitcoin Cash).

Strojna denarnica: fizična naprava za hranjenje zasebnih ključev in upravljanje kriptovalute, ki zagotavlja večjo varnost kot programska denarnica.

Funkcija zgoščevanja: matematična funkcija, ki sprejme vhodne podatke poljubne velikosti in ustvari izhodni niz znakov fiksne velikosti, ki se pogosto uporablja v kriptografiji in tehnologiji verige blokov.

Hitrost zgoščevanja: način merjenja procesorske moči omrežja Bitcoin.

HODL: izraz iz napačno zapisane besede „hold“ (držati), ki se uporablja v kriptovalutni skupnosti in označuje dolgoročno posedovanje kriptovalute, namesto prodaje ali trgovanja.

Vroča denarnica: Bitcoinova denarnica, ki je povezana z internetom in omogoča preprost dostop do bitcoinov.

Uvoz: blago in storitve, proizvedene v drugi državi in prodane na domačem trgu.

Inflacija: povečanje splošne ravni cen blaga in storitev v gospodarstvu.

Prva javna ponudba kovancev (ICO): metoda zbiranja sredstev, kjer je nova kriptovaluta prodana investitorjem v zameno za bolj uveljavljeno kriptovaluto, kot je Bitcoin.

Protokol 1. plasti: temeljna plast omrežja verige blokov, odgovorna za temeljne vidike soglasja, potrjevanja transakcij in hranjenja podatkov.

Protokol 2. plasti: sekundarna plast, zgrajena na vrhu omrežja verige blokov 1. plasti, ki se pogosto uporablja za povečanje skalabilnosti, hitrosti in funkcionalnosti.

Glavna knjiga: evidenca finančnih transakcij.

Lightning Network: plačilni protokol 2. plasti, ki omogoča hitrejša in cenejša Bitcoinove transakcije z uporabo kanalov izven verige za manjše transakcije.

**Menjalna sredstva:** predmeti ali sistemi, ki so splošno sprejeti kot zamenjava za blago in storitve.

**Merklovo drevo:** drevesu podobna podatkovna struktura, ki se v Bitcoinovi verigi blokov uporablja za učinkovito preverjanje celovitosti velikih naborov podatkov.

**Bazen za rudarjenje:** skupina rudarjev, ki sodelujejo, da bi povečali svoje možnosti glede iskanje novih blokov in zaslužka bitcoinov.

**Rudarstvo:** postopek uporabe računalniške strojne opreme za izvajanje matematičnih izračunov v omrežju Bitcoin za namene potrjevanja transakcij in zagotavljanje večje varnosti.

**Denarna in fiskalna politika:** politike centralne banke in vlade, ki vplivajo na denarno maso ter obrestne mere v gospodarstvu.

**Denarna masa:** skupni znesek denarja v obtoku gospodarstva.

**Denarnica z več podpisi (Multisig):** denarnica, ki pred izvedbo transakcije zahteva več podpisov ali odobritev, kar zagotavlja dodatno plast varnosti in nadzora.

**Več podpisov:** varnostna funkcija, ki zahteva več kot en zasebni ključ za odobritev Bitcoinove transakcije.

**Omrežje:** skupina medsebojno povezanih entitet.

**Omrežje vozlišč:** omrežje povezanih računalnikov ali naprav, ki podpirajo in vzdržujejo omrežje Bitcoin.

**Vozlišče:** računalnik ali naprava, ki je povezana z omrežjem Bitcoin ter sodeluje pri postopku preverjanja in prenosa transakcij.

**Nezamenljivi žeton (NFT):** vrsta digitalnega sredstva, ki predstavlja enolični oziroma edinstveni predmet – običajno umetniški, zbirateljski ali drug enolični predmet.

**Nonce:** naključno število, dodano glavi bloka za namene ustvarjanja zgoščene vrednosti, ki ustreza ciljni težavnosti.

**Osamljeni blok:** blok, ki ni vključen v glavno verigo blokov, ker je bil razveljavljen zaradi daljše konkurenčne verige.

**Papirnata denarnica:** natisnjena kopija uporabnikovih zasebnih in javnih ključev, ki se uporablja za hranjenje in upravljanje kriptovalute brez povezave.

**Enakovredni udeleženci (P2P):** decentralizirano omrežje, kjer udeleženci komunicirajo neposredno drug z drugim in ne prek osrednjega organa.

**Vezano:** fiksni menjalni tečaj med dvema valutama, pri katerem je ena valuta vezana na vrednost druge.

**Zasebna veriga blokov:** veriga blokov, ki jo nadzira ena sama organizacija, namesto da bi bila decentralizirana.

**Zasebni ključ:** tajni podatek, ki s kriptografskim podpisom dokazuje pravico osebe do porabe bitcoinov iz določene denarnice.

**Dokaz o vložku (PoS):** mehanizem soglasja, ki se uporablja v nekaterih omrežjih verige blokov in zahteva, da ima uporabnik določeno količino kriptovalute, da lahko sodeluje pri potrjevanju transakcij.

**Dokaz o delu (PoW):** mehanizem soglasja, ki zahteva, da uporabnik opravi določeno količino računalniškega dela, da lahko sodeluje v omrežju.

**Javna veriga blokov:** veriga blokov, ki je dostopna vsakomur za sodelovanje pri opravljanju in preverjanju transakcij, zaradi česar je decentralizirana.

**Javni ključ:** enolični identifikator, ki se uporablja za prejemanje bitcoinov in je z matematičnim postopkom pridobljen iz uporabnikovega zasebnega ključa.

**Javni ključ/Bitcoinov naslov:** javno geslo/številka, ki se uporablja za prejemanje bitcoinov.

**Javna glavna knjiga:** decentralizirana zbirka podatkov, kjer je shranjena javna evidenca vseh transakcij v omrežju Bitcoin.

**Kupna moč:** sposobnost denarja za nakup blaga in storitev.

**Obnovitvena fraza/semenska ključna beseda:** niz 12, 18 ali 24 besed, s katerimi lahko ustvarite več parov zasebnih in javnih ključev. Z njimi lahko obnovite Bitcoinovo denarnico.

**Stopnja obveznih rezerv:** delež depozitov, ki jih mora banka hraniti kot rezerve.

**Restriktivno bančništvo:** omejitve bančnih storitev ali dostopa do bančnih storitev.

**Satoshi Nakamoto:** psevdonim za anonimnega ustvarjalca Bitcoina.

**Satoshi:** najmanjša enota bitcoina, enaka 1/100.000.000 bitcoina. Imenuje se po Satoshiju Nakamotu, ustvarjalcu Bitcoina.

**Satoshi na bajt (sat/b):** enota, ki se uporablja za merjenje višine provizije za Bitcoinovo transakcijo, plačane na bajt podatkov transakcije.

SegWit (Segregated Witness): nadgradnja Bitcoinovega protokola, ki spreminja način hranjenja podatkov v verigi blokov za zagotavljanje večje zmogljivosti in nižjih transakcijskih provizij.

Stranska veriga: veriga blokov, ki je povezana z drugo verigo blokov in omogoča prenos sredstev ali informacij med obema verigama.

Podpis: matematični mehanizem, s katerim lahko oseba dokaže lastništvo.

Pametna pogodba: samoizvršljiva pogodba, katere pogoji so zapisani v kodi.

Mehka odcepitev: sprememba Bitcoinovega protokola, ki je vzvratno združljiva s starejšimi različicami programske opreme.

Stabilni kriptožeton: vrsta kriptovalute, zasnovana za ohranjanje stabilne vrednosti, pogosto tako, da je vezana na fiat valuto ali drugo sredstvo.

Ponudba in povpraševanje: ekonomsko načelo, kjer je cena blaga ali storitev določena z medsebojno odvisnostjo količine dobavljenega blaga ali storitev od količine povpraševanja.

Časovna vrednost denarja: načelo, da je denar v sedanosti vreden več kot v prihodnosti.

Žeton: enota vrednosti, ustvarjena v verigi blokov, ki je pogosto uporabljena za predstavitev določenega sredstva ali pripomočka v določenem ekosistemu.

Tokenizacija: postopek ustvarjanja digitalne predstavitve sredstva ali skupine sredstev v verigi blokov, ki omogoča delno lastništvo in prenosljivost.

Trgovalni par: nabor dveh valut ali sredstev, s katerimi se lahko trguje na borzi kriptovalut.

Transakcijska provizija: majhen znesek bitcoinov, ki ga plača pošiljatelj transakcije, s čimer spodbudi rudarje, da vključijo transakcijo v blok in jo dodajo v verigo blokov.

ID transakcije: niz števil in črk, ki prikazuje podrobnosti prenosa bitcoinov (kot so poslani znesek, naslova pošiljatelja in prejemnika ter datum prenosa) v Bitcoinovi verigi blokov.

Transakcija: prenos bitcoinov z enega naslova na drugega v omrežju Bitcoin.

Brez potrebe po zaupanju: sistem ali transakcija, ki ne zahteva zaupanja v tretjo osebo ali posrednika, temveč se zanaša na varnost in preglednost osnovne tehnologije.



Dvojno preverjanje pristnosti (2FA): varnostni ukrep, ki za dostop do računa ali dokončanje transakcije zahteva dva načina preverjanja pristnosti – običajno geslo in ločeno kodo ali napravo.

Brez bančnega računa: posamezniki ali skupnosti, ki nimajo dostopa do tradicionalnih bančnih storitev.

Obračunska enota: standardna merska enota, ki se uporablja za izražanje vrednosti blaga in storitev.

Volatilnost: stopnja nihanja cene sredstva v določenem časovnem obdobju.

Naslov denarnice: enolični identifikator, ki se uporablja za pošiljanje in prejemanje bitcoinov v omrežju Bitcoin in je običajno označen kot niz črk in števil.

Varnostna kopija denarnice: kopija zasebnih ključev in obnovitvenih fraz/semenskih ključnih besed Bitcoinove denarnice, ki jo je mogoče uporabiti za obnovitev dostopa do denarnice v primeru izgube ali kraje izvornika.

Denarnica: virtualni vsebnik za bitcoine, podoben fizični denarnici, ki vsebuje zasebne ključe, s katerimi lahko porabite bitcoine, dodeljene vsebniku v verigi blokov.

Kit: posameznik ali organizacija, ki ima v lasti veliko količino kriptovalute in lahko z velikimi posli vpliva na tržne cene.

Beli klobuk: etični heker, ki uporablja svoje znanje za odkrivanje in odpravljanje ranljivosti v računalniških sistemih in omrežjih.

Bela knjiga: poročilo, kjer sta pojasnjena težava in rešitev, ki ju obravnava projekt verige blokov ali kriptovaluta.

XBT in BTC: okrajšavi za bitcoin.



 **My  
First  
Bitcoin**  
EL SALVADOR

ISBN 978-961-96233-3-6

