



Bitcoindiploma

Financiële educatie voor het bitcointijdperk

Studenten werkboek

Nederlandse versie | januari 2024

Mijn Eerste Bitcoin heeft dit werk gemaakt en vrij beschikbaar gesteld onder [Creative Commons](#).

Dit werk is gelicenseerd onder licentie
[Creative Commons](#)
[Attribution-ShareAlike](#)
4.0 International (CC BY-SA 4.0)

ISBN: 9789916749180



Bitcoindiploma

Financiële educatie voor het bitcointijdperk

Studenten werkboek

Nederlandse versie | 2024 | JK



EL SALVADOR

DONEER NU



bc1q5es60qpa7gpkp0k32xl4zefkj43kd9zjkzd54sgmv3y3r34dw8dqm9pzs

Dankbetuigingen

Het bitcoindiploma verhaal

Er is niets krachtiger dan een idee waar de tijd rijp voor is.

Het verhaal van het bitcoindiploma begon in El Salvador, met de eerste pilot van 38 leerlingen van openbare scholen die in juni 2022 afstudeerden.

Het is moeilijk te geloven dat dit nog maar anderhalf jaar geleden is.

De groei in 2023 was fenomenaal, met duizenden studenten uit het hele land die afstudeerden met een bitcoindiploma. In september, slechts 15 maanden na dat eerste diploma, begon een veel groter pilot programma. Het Ministerie van Onderwijs in El Salvador maakte hun eigen bitcoindiploma met ons werkboek als belangrijkste bronmateriaal. Samen met Bitcoin Beach gaven onze leraren het bitcoindiploma aan 150 leraren van openbare scholen. Deze docenten keerden terug naar hun eigen scholen en gaven les aan hun eigen leerlingen. Dit jaar zijn we van plan om te beginnen met het trainen van nog eens 700 leraren van openbare scholen verspreid over het land, en de hoop is om binnen twee jaar bitcoinonderwijs van hoge kwaliteit naar elke school in El Salvador te brengen.

Een van onze oorspronkelijke doelen was om een natie te onderwijzen en de potentie van bitcoinonderwijs te demonstreren op grote schaal. Die droom is nu goed op weg.

El Salvador is de focus; de missie is de wereld.

We hebben het werkboek open-source gemaakt, net als een verscheidenheid aan ander educatief materiaal, en zijn overweldigd door de internationale interesse. Toen het in 2022 voor het eerst werd onderwezen in El Salvador, was dat de eerste keer dat er ooit een bitcoindiploma werd onderwezen in een openbaar schoolsysteem waar ook ter wereld. In 2023 explodeerde het bitcoindiploma en is het vertaald in 12 talen. Het bitcoindiploma wordt nu onderwezen in Guatemala, Honduras, de VS, Canada, Cuba, de Dominicaanse Republiek, Zuid-Korea, Costa Rica, Brazilië, Uruguay, Argentinië, India, Italië, Mexico, Zuid-Afrika, Zambia, Kenia, Portugal, het Verenigd Koninkrijk en Hongkong. En, net zoals de groei in 2023 het voorgaande jaar overtrof, verwachten we dat in 2024 hetzelfde zal gebeuren.

Dit is een wereldwijde, gedecentraliseerde beweging.

Onafhankelijk, onpartijdig, door de gemeenschap geleid bitcoinonderwijs zal de wereld veranderen. Dat heeft het al gedaan.

Voor een betere wereld,

Mijn Eerste Bitcoin team - 2024

Inhoudsopgave

Hoofdstuk #1: Waarom hebben we geld nodig?

1.0 Inleiding	01
1.1 Ontmoet Satoshi	01
Activiteit: vijf vragen over geld	01
1.2 Discussie in de klas: waarom hebben we geld nodig?	04

Hoofdstuk #2: Wat is geld?

2.0 Inleiding	07
Activiteit: discussie in de klas - "wat is geld?"	07
2.1 Definitie van geld	07
2.2 Functies van geld	09
2.3 Eigenschappen van geld	10
2.4 Soorten geld	13
2.5 De psychologie van geld: schaarste, tijdsvoorkeur en afwegingen	14
Activiteit: tijdsvoorkeur	16

Hoofdstuk #3: De geschiedenis van geld

3.0 Inleiding	21
Activiteit: ruilhandelspel	21
3.1 Evolutie van ruilhandel naar moderne valuta	23
3.1.1 Problemen met vroege vormen van geld	23
3.1.2 Ontwikkeling van munten en papiergeld	24
3.1.3 Overgang van eerlijk naar oneerlijk geld	25
3.1.4 Van papieren naar plastic geld	27
3.2 Digitaal geld	28

Hoofdstuk #4: Wat is fiatgeld en wie beheert het?

4.0 Inleiding	31
4.1 Korte geschiedenis van fiatgeld	31
4.2 Het fiatsysteem	34
4.2.1 Een monetair systeem per decreet	34

4.2.2 Bankieren met fractionele reserve: een systeem gevoed door schulden	35
Activiteit: fractioneel bankieren	38
4.2.3 Wie beheert het fiatsysteem en hoe profiteren zij ervan?	39
4.3 Digitaal centralebankgeld: De toekomst van fiatgeld	41

Hoofdstuk #5: Hoe problemen tot oplossingen leiden

5.0 Introductie van het probleem	45
5.1 Afnemende koopkracht	45
5.1.1 Monetaire inflatie en het effect ervan op de koopkracht	45
Activiteit: de gevolgen van inflatie - een veilingactiviteit	46
5.2 De wereldwijde schuldenlast en sociale ongelijkheid	47
5.2.1 Gevolgen voor het individu - verlies van koopkracht	47
5.2.2 Impact op de samenleving - toenemende welvaartsongelijkheid	52
Activiteit: gevolgen van het fiatsysteem	53
5.2.3 De wereldwijde schuldenlast	54
5.3 De cypherpunks en de zoektocht naar gedecentraliseerd geld	55
5.3.1 De cypherpunks	56
5.3.2 Gecentraliseerde versus gedecentraliseerde systemen	57
5.3.3 Korte geschiedenis van digitale valuta	59

Hoofdstuk #6: Een introductie tot bitcoin

6.0 Satoshi Nakamoto en de creatie van bitcoin	63
6.1 Hoe werkt bitcoin?	65
6.1.1 Het Nakamoto consensus mechanisme	65
6.1.2 De spelers van het spel	67
Activiteit: consensusvorming in een peer-to-peer netwerk	69
6.2 Bitcoin als eerlijk digitaal geld	71
6.2.1 Inleiding	71
6.2.2 Kenmerken van bitcoin	72
Activiteit: discussie in de klas - Is bitcoin eerlijk geld?	76
6.2.3 Omarm persoonlijke verantwoordelijkheid	76

Hoofdstuk #7: Hoe gebruik ik bitcoin?

7.0 Inleiding	81
7.1 Bitcoin verkrijgen en ruilen	81
7.1.1 P2P: persoonlijk in de echte wereld	81
7.1.2 P2P: online	82
7.1.3 Gecentraliseerde exchanges	82
7.2 Bitcoinwallets, een introductie	83
7.2.1 Self-custodial vs custodial wallets	83
7.2.2 Verschillende type bitcoinwallets	85
7.3.3 Open-source vs closed-source	86
Activiteit: evaluatie van bitcoinwallets	87
7.3 Een mobiele bitcoinwallet instellen	87
Activiteit: een bitcoinwallet opzetten/herstellen	87
7.4 Transacties ontvangen en versturen	89
Activiteit: bitcointransacties in de praktijk	91
7.5 Sparen in bitcoin	93
7.6 Don't Trust, Verify	94

Hoofdstuk #8: Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

8.0 Inleiding	97
Activiteit: bekijk deze video over het lightningnetwerk	98
8.1 Het lightningnetwerk	98
8.2 Verschillende soorten lightningwallets	100
8.2.1 Self-custodial versus custodial wallets	100
8.2.2 Open-source versus closed-source	100
8.3 Een bitcoin lightningwallet opzetten	100
8.4 Ontvangen en versturen van lightningtransacties	102
Activiteit: lightningwalletestafette	106
8.5 Koffie en boodschappen kopen met bitcoin	107
8.5.1 Online: payment plugins - ecommerce	108
8.5.2 Persoonlijk: zoek een winkelier bij jou in de buurt	109
8.5.3 Overgangshulpmiddelen: vouchers, cadeaubonnen en betaalkaarten	110
8.5.4 Circulaire economieën en bitcoin als ruilmiddel	110

Hoofdstuk #9: Een introductie tot de technische kant van bitcoin

9.0 Inleiding	115
Activiteit: bekijk "Hoe bitcoin werkt onder de motorkap"	115
9.1 Public keys en private keys: beveiliging door cryptografie	116
9.1.1 Cryptografische public keys en private Keys	116
9.1.2 Uitleg over hashing	119
Activiteit: genereer een SHA-256 hash	121
9.2 Het UTXO model	122
9.3 Bitcoinnodes en miners nader bekeken	125
9.3.1 Wat is een bitcoinnode en hoe zet ik er een op?	125
Activiteit: bekijk een video over bitcoinnodes	126
9.3.2 Wat is een bitcoinminer en hoe werkt mining?	126
9.4 Wat is de mempool?	132
Activiteit: mempool	134
9.5 Hoe bitcointransacties van begin tot eind werken	135

Hoofdstuk #10: Waarom bitcoin?

10.0 Inleiding	139
Activiteit: hoe zou een bitcoin toekomst eruit kunnen zien?	139
10.1 Wat is digitaal centralebankgeld en wie beheert het?	140
10.2 De filosofie van bitcoin	141
Activiteit: discussie in de klas - heb je het recht om over je eigen geld te beschikken?	141
10.3 De voordelen van bitcoin	142
10.4 Een zelfredzame toekomst	143
Activiteit: discussie in de klas - hoe is je perspectief veranderd?	143
Additionele bronnen	147
Begrippen	149
Woordenlijst	153

Bitcoindiploma

*Een transformatieve reis
van tien weken door onafhankelijk,
onpartijdig, kwalitatief en gratis onderwijs*

Het is essentieel om een goed begrip te hebben van de basisprincipes van geld, de geschiedenis en het huidige financiële systeem voordat u zich gaat verdiepen in [bitcoin](#). Als u deze concepten begrijpt, legt u een sterke basis voor het begrijpen van het unieke en ontwrichtende karakter van [bitcoin](#).

Door te leren over de evolutie van geld, kunt u de mogelijkheden en beperkingen van het huidige financiële systeem beter begrijpen en hoe [bitcoin](#) deze wil aanpakken. Zonder deze basis kan het een uitdaging zijn om het belang en de potentiële impact van [bitcoin](#) volledig te begrijpen.

Vertrouw op het leerproces en blijf gefocust, want de beloning van een dieper begrip en waardering van dit baanbrekende veld zal het zeker waard zijn.

Hoofdstuk #1

Waarom hebben we geld nodig?

1.0 Inleiding

1.1 Ontmoet Satoshi

Activiteit: Vijf vragen over geld

1.2 Discussie in de klas: Waarom is geld nodig?

Studenten Werkboek

Nederlandse versie | 2024

Waarom hebben we geld nodig?

1.0 Inleiding



Geld is een van de grootste instrumenten voor vrijheid die de mens ooit heeft uitgevonden.

Friedrich Hayek

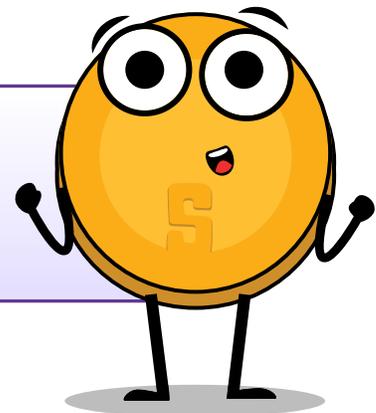


Welkom bij het bitcoindiploma. In dit hoofdstuk verkennen we de fundamentele vraag waarom geld essentieel is in ons leven. We kijken naar de aard van geld en de verschillende vormen ervan, om zo de betekenis van geld beter te begrijpen. Geld is iets dat we bijna elke dag gebruiken, maar begrijpen we eigenlijk wel waarom we het nodig hebben en wat het is? Waarom ruilen onze ouders en familieleden hun tijd voor geld? Waarom hebben sommige mensen er meer van dan anderen? Waarom is geld in andere landen anders? Waarom kunnen we er niet gewoon meer van maken als we het nodig hebben?

1.1 Ontmoet Satoshi



Hoi! Ik ben Satoshi, een interactieve assistent die je tijdens het hele bitcoindiploma zal helpen. Ik geef je bronnen en nuttige aanbevelingen, zodat je dieper in kunt gaan op de belangrijkste begrippen.



Activiteit - Laten we het hoofdstuk beginnen met het beantwoorden van de vijf onderstaande vragen:

Denk aan praktische toepassingen zoals het kopen van voedsel of voorwerpen die je graag zou willen hebben. Probeer specifiek te zijn in je voorbeelden en zorg voor een evenwicht tussen creativiteit en realisme.



Waarom is geld nodig?

Wat is geld?

Waarom hebben we geld nodig?

Wie beheert het geld?

Wat geeft geld zijn "waarde"?



Welke vraag heb jij over geld? Schrijf je vraag hieronder op.

Breid de discussie uit naar de hele klas. Bedenk, deel en vergelijk de vijf belangrijkste redenen waarom we geld nodig hebben. Identificeer gemeenschappelijke ideeën in de klas. Denk na over jullie eigen unieke ideeën die deze lijst niet hebben gehaald, maar wel het overwegen waard zijn. Noteer deze aanvullende inzichten.

1.2 Discussie in de klas: waarom hebben we geld nodig?

Verdeel de klas in groepen en:

- Deel en bespreek elkaars antwoorden op de eerste vier vragen. Schrijf de beste antwoorden op.
- Deel elkaars antwoorden op de laatste vraag en stem op één favoriete vraag. Schrijf het resultaat op.
- Aan het einde van het bitcoindiploma zal de klas deze antwoorden en vragen opnieuw bekijken.

Nu je beter begrijpt waarom we geld nodig hebben, gaan we in de volgende hoofdstukken onderzoeken wat geld is, hoe het zich in de loop der tijd heeft ontwikkeld, wie het beïnvloedt en wat de nieuwste vorm ervan is. Blijf refereren aan de lijsten van deze eerste lesdag om verbanden te leggen tussen je eigen inzichten en de evolutie van geldcreatie, de definitie van geld, en het gebruik ervan door de tijd heen.

Hoofdstuk #2

Wat is geld?

2.0 Inleiding

Activiteit: discussie in de klas - "Wat is geld?"

2.1 Definitie van geld

2.2 Functies van geld

2.3 Eigenschappen van geld

2.4 Soorten geld

2.5 De psychologie van geld: schaarste, tijdsvoorkeur en afwegingen

Activiteit: tijdsvoorkeur

Wat is geld?

2.0 Inleiding

Geld is een garantie dat we in de toekomst kunnen hebben wat we willen. Hoewel we op dit moment niets nodig hebben, verzekert het ons van de mogelijkheid om aan een nieuwe behoefte te voldoen als die zich voordoet.

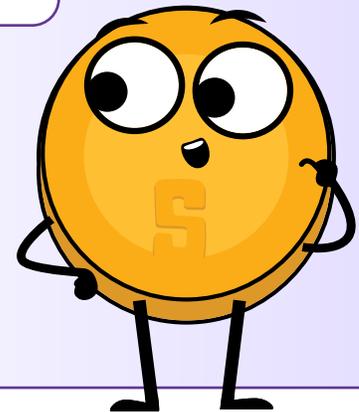
Aristoteles

Voortbouwend op ons onderzoek naar de noodzaak van geld, onderzoekt dit hoofdstuk de kernvraag: Wat is geld? We beginnen met een groepsdiscussie en een activiteit

Activiteit: Discussie in de klas - "Wat is geld?"

- ☀ Eet het snoepje dat op je bureau ligt als je blijft nog niet op.
- ☀ Wie zou zijn snoepje willen ruilen voor een briefje van vijf euro?
- ☀ Steek je handen omhoog als je ook bereid zou zijn om je snoepje in te ruilen voor een monopolybiljet van vijf in plaats van je snoepje?
- ☀ Waarom wel en waarom niet?
- ☀ Wat maakt het ene zo bijzonder ten opzichte van het andere?
- ☀ Wat geeft geld zijn "waarde"?
- ☀ Waar komt het geld vandaan en wie bepaalt hoeveel er wordt gedrukt?
- ☀ Waarom drukken we niet meer geld en verdelen we het gelijkmatig over iedereen?

Het enige verschil tussen deze twee briefjes is jouw geloof dat het ene briefje meer waarde heeft dan de ander.



2.1 Definitie van geld

Heb je er ooit bij stilgestaan wat geld eigenlijk is? Heb je je ooit afgevraagd wat geld nou eigenlijk geld maakt? De meesten van ons weten hoe ze het moeten gebruiken, maar weinigen van ons begrijpen waar het vandaan komt of hoe het werkt. Geld is in wezen een manier om goederen en diensten uit te wisselen. Het vertegenwoordigt de waarde van deze goederen in een vorm die gemakkelijk kan worden verhandeld. Dit kan in veel verschillende vormen, zoals papieren biljetten, metalen munten en elektronische betalingen. Overheden of andere autoriteiten zijn meestal de uitgever van geld en beheren het. Maar geld is zoveel meer dan een fysiek of digitaal ruilmiddel. Het is als een universele taal waarmee we handel kunnen drijven met mensen over de hele wereld, zelfs als we niet dezelfde taal spreken of niet dezelfde cultuur hebben. Je kunt bijvoorbeeld aan de andere kant van de wereld zijn en toch geld "spreken" door een product op de toonbank te leggen en het te ruilen voor de lokale munteenheid of door een bankpas/creditcard te gebruiken.

Geld is als een sociaal contract dat het mogelijk maakt om handel te drijven zonder afhankelijk te zijn van ruilhandel of het vinden van iemand die specifiek wil hebben wat jij te bieden hebt. Als een groep mensen chocolade zou accepteren als betaling voor de meeste goederen en diensten, dan zou chocolade geld worden (hoewel we het als slecht geld kunnen beschouwen omdat het, onder andere, in sommige delen van de wereld zou smelten).

Zoals de Franse econoom Jean-Baptiste Say opmerkte: "Geld vervult slechts een kortstondige functie in een ruil; en als de transactie uiteindelijk is afgesloten, zal altijd blijken dat het ene soort goed is geruild voor een andere."

Met andere woorden, geld heeft zelf niet de kracht om aan menselijke behoeften te voldoen. Het is slechts een instrument waarmee we het ene goed voor het andere kunnen ruilen.



Een **transactie** is een uitwisseling of overdracht van goederen en diensten. Het is een manier om waarde uit te wisselen tussen twee of meer partijen.

Er zijn veel verschillende soorten transacties, variërend van eenvoudige transacties (zoals het kopen van een broodje) tot complexere transacties (zoals het kopen van een huis of het beleggen in aandelen of obligaties). Transacties kunnen persoonlijk, telefonisch, online of op een andere manier worden uitgevoerd en er kunnen veel verschillende partijen bij betrokken zijn, waaronder personen, bedrijven en financiële instellingen.



Check deze korte video!

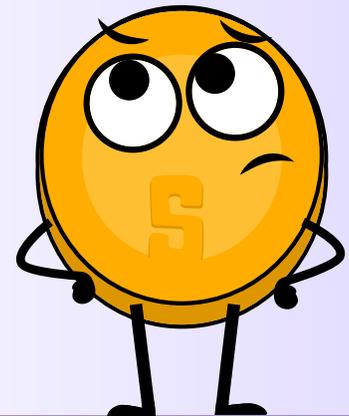
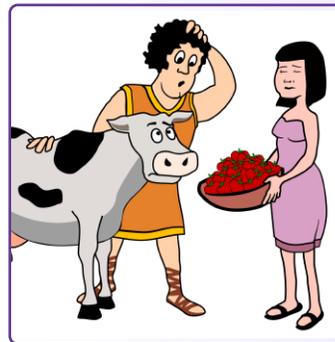


Geld **IS** de waarde **WAARMEE** goederen en diensten worden uitgewisseld. Geld **IS NIET** de waarde **WAARVOOR** goederen worden geruild

Hoe gemakkelijk of haalbaar zou deze transactie zijn zonder geld?

Zou jij één koe ruilen voor 1.000.000 aardbeien?

Of voor 600.000 aardbeien? Wat dacht je van 50.000?



Samengevat:

Geld vergemakkelijkt de handel omdat iedereen het accepteert als uiteindelijke betaling. Het stelt ons in staat om waarde te meten en vergelijkingen te maken tussen verschillende goederen en diensten. Vervolgens bekijken we de functies van geld.

Wat is geld?

2.2 Functies van geld

Bij het kopen en verkopen van goederen en diensten speelt geld een cruciale rol. Het heeft verschillende belangrijke functies in de wereld, zoals:



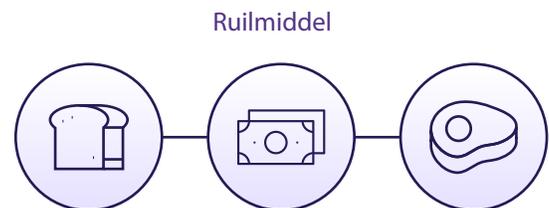
Spaarmiddel

Geld moet na verloop van tijd zijn waarde behouden. Hierdoor kunnen mensen geld gebruiken om plannen te maken voor de toekomst en om geld te lenen en uit te lenen. Dus als je de volgende keer aan het sparen bent voor iets speciaals, onthoud dan dat geld meer is dan alleen een manier om dingen te betalen, het is een hulpmiddel om je te helpen plannen en investeren in je toekomst.



Ruilmiddel

Met geld is het niet nodig om iemand te vinden die precies wil ruilen wat jij hebt. In plaats daarvan kun je geld gebruiken om alles te kopen en verkopen wat je maar wilt. Dit maakt handel en zakendoen veel handiger en efficiënter.

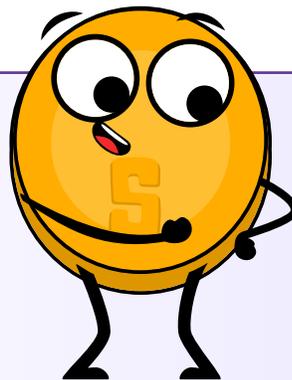


Rekeneenheid

Geld biedt een universele waardestandaard waarmee mensen de prijs van verschillende goederen en diensten kunnen uitdrukken en vergelijken. Dit zorgt voor een efficiëntere en transparantere markt, waarin mensen weloverwogen beslissingen kunnen nemen over wat ze kopen en verkopen.

Rekeneenheid

Consumenten weten de waarde van iets wanneer je het een prijs (monetaire waarde) geeft



Zie het als volgt: als je een nieuwe auto wilt kopen, kun je de prijzen van verschillende dealers vergelijken en een weloverwogen beslissing nemen over welke auto je wilt kopen op basis van de prijs in euro's. Zonder rekeneenheid zou je de waarde van de ene auto met de andere moeten vergelijken aan de hand van iets anders, zoals het aantal koeien dat de auto waard was of de tijd die het kostte om de auto te maken.

Dankzij deze drie functies kunnen economieën complex en dynamisch worden. Zonder geld zou het veel moeilijker zijn om goederen en diensten te kopen en te verkopen en zou onze economie veel minder ontwikkeld zijn.

Oefening in de klas: van welke functie van geld is dit een voorbeeld?

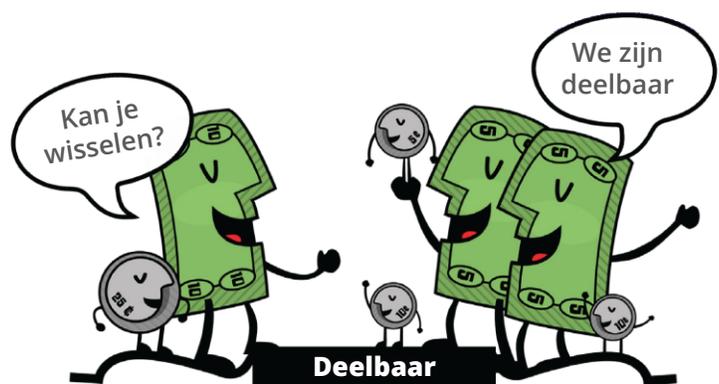
- ☀️ Eva besluit een deel van haar wekelijkse loon te sparen om een puppy te kopen.
- ☀️ Adam koopt twee stukken pizza voor €8,30 bij Ray's Pizza.
- ☀️ Marc kan niet beslissen of hij concertkaartjes voor €75 of een skipas voor €95 koopt.

2.3 Eigenschappen van geld

In de loop der tijd hebben mensen zich uiteindelijk gerealiseerd dat geld bepaalde kwaliteiten moet bezitten om effectief te zijn als ruilmiddel. Deze kenmerken zijn duurzaamheid, deelbaarheid, draagbaarheid, aanvaardbaarheid, schaarste en uitwisselbaarheid.

- ☀️ **Duurzaam** verwijst naar het vermogen van geld om fysieke achteruitgang te weerstaan en lang mee te gaan. Dit zorgt ervoor dat geld in een acceptabele en herkenbare staat in de economie kan circuleren. Goud is een duurzaam materiaal dat bestand is tegen slijtage, waardoor het een goede weergave is van het duurzaamheidskenmerk van geld.

- ☀️ **Deelbaar** verwijst naar het vermogen van geld om in kleinere eenheden te worden verdeeld, zodat mensen het kunnen gebruiken om aankopen van verschillende bedragen te doen. Papieren biljetten kunnen gemakkelijk in kleinere eenheden worden verdeeld, wat ze een goede weergave maakt van de deelbaarheid van geld.



Wat is geld?

☀ **Draagbaar** verwijst naar het gemak waarmee geld vervoerd en meegenomen kan worden. Hierdoor kunnen mensen geld gebruiken om zonder problemen goederen en diensten te kopen en verkopen. Creditcards/bankpassen zijn draagbaar, omdat ze gemakkelijk kunnen worden meegenomen in een portemonnee of tas, waardoor ze een goede illustratie zijn van de draagbaarheidseigenschap van geld.



☀ **Aanvaardbaar** verwijst naar de wijdverspreide acceptatie van geld als betaalmiddel, zodat mensen het met vertrouwen kunnen gebruiken om goederen en diensten te kopen en verkopen. De Amerikaanse dollar wordt algemeen geaccepteerd als betaalmiddel, waardoor het een goede weergave is van de aanvaardbaarheid van geld.



☀ **Schaars** verwijst naar de beperkte hoeveelheid van geld, waardoor het zijn waarde behoudt en we niet steeds meer geld hoeven uit te geven om dezelfde hoeveelheid goederen te kopen. Verzamelbare postzegels, vooral zeldzame postzegels, kunnen een goede vorm van geld zijn omdat ze schaars zijn en na verloop van tijd in waarde kunnen stijgen. Postzegelverzamelaars investeren soms in postzegels om hun investeringen te spreiden en hun vermogen te vergroten.



☀ **Uitwisselbaar** verwijst naar de gelijkwaardigheid van de ene geldeenheid aan een andere eenheid van dezelfde waarde. Geld moet uniform zijn. Koperen munten zijn uniform in grootte en gewicht, waardoor ze een goede representatie zijn van het uniformiteitskenmerk van geld. Eén cent is altijd één cent.



Al met al maken deze kenmerken geld tot een nuttig en effectief instrument voor handel en zakendoen, en zijn ze essentieel voor de ontwikkeling en stabiliteit van economieën.

Oefening in de klas

Verschillende goederen hebben verschillende eigenschappen en vervullen in verschillende mate de functies van geld. Uiteindelijk bepaalt de samenleving welke middelen als geld worden gebruikt, gebaseerd op factoren zoals stabiliteit, schaarste, deelbaarheid, draagbaarheid en acceptatie als ruilmiddel.

Om te bepalen hoe goed verschillende voorwerpen voldoen aan de specifieke kenmerken van geld, kun je elk voorwerp scoren op een schaal van 1 tot 5 voor elk kenmerk. Door de scores voor elk item bij elkaar op te tellen, kun je bepalen welk item het meest geschikt is als vorm van geld.

[0 = Verschrikkelijk; 3 = Oké; 5 = Uitstekend]

* Vul alsjeblieft niet de kolom voor Bitcoin in; we komen hier later in de cursus op terug.

Gebruik de volgende vragen om te bepalen in hoeverre de verschillende items in de tabel voldoen aan de kenmerken van geld

- Duurzaam: kan het geld de tand des tijds doorstaan?
- Uitwisselbaar: zijn de geldeenheden met elkaar uitwisselbaar?
- Aanvaardbaar: wordt het geld algemeen geaccepteerd als betaalmiddel?
- Schaars: is het geld schaars en niet te overvloedig?
- Draagbaar: kan het geld gemakkelijk worden vervoerd en op verschillende locaties worden gebruikt?
- Deelbaar: kan het geld in kleinere eenheden worden verdeeld voor transacties?

Karakteristieken van goed geld	Koeien	Cigaretten	Diamanten	Euros	Bitcoin
Duurzaam					
Uitwisselbaar					
Aanvaardbaar					
Schaars					
Draagbaar					
Deelbaar					
Totaal					

Wat is geld?

2.4 Soorten geld

Geld kan worden onderverdeeld in twee hoofdcategorieën: fysiek en digitaal.

Fysiek geld omvat:

- ☀️ Fiatgeld, dat zijn de papieren biljetten en munten die overheden uitgeven en worden geaccepteerd als ruilmiddel.
- ☀️ Representatief geld, vertegenwoordigt een vordering op een fysiek goed, zoals zilver certificaten.
- ☀️ Goederengeld, een fysiek object met intrinsieke waarde dat algemeen geaccepteerd wordt als ruilmiddel. Bijvoorbeeld goud en zilver.



Niet al het geld is hetzelfde!



Goederengeld



Objecten zoals buskruit waren vroeger goederengeld.

Representatief geld



Representatief geld zoals zilver certificaten zijn te ruilen voor echt zilver.

Fiatgeld

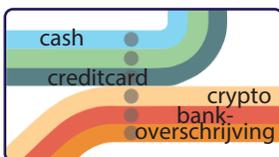


Het geld dat de overheid uitgeeft en accepteert voor de afbetaling van schulden.



Digitale valuta kunnen gebruikt worden voor online transacties en omvatten elektronische valuta, stablecoins en cryptocurrencies.

Elektronische valuta zijn digitale versies van regulier geld, zoals dollars of euro's, en kunnen gebruikt worden om online betalingen te verrichten.



Betaalsystemen maken het mogelijk om elektronische valuta en andere digitale bezittingen van de ene persoon naar de andere over te maken. In het traditionele financiële systeem is er echter altijd een tussenpersoon, zoals een bank of financiële instelling, die kosten in rekening brengt en de bevoegdheid heeft om transacties te accepteren, annuleren, terug te draaien of uit te stellen.

In het traditionele financiële betaalsysteem verzorgen betaalsystemen de overdracht van geld. Gebruikers kunnen hiermee hun elektronische valuta opslaan, beheren en betalingen doen door geld over te maken van hun rekening naar de rekening van de ontvanger.



Digitaal Centraalbankgeld (CBDCs):

zijn digitale versies van de fiatvaluta van een land, die worden uitgegeven en gedekt door de centrale bank en worden beheerd door de overheid.



Stablecoins

zijn digitale valuta die zijn ontworpen om een stabiele waarde te behouden ten opzichte van een bepaald goed, zoals de Amerikaanse dollar.



Cryptocurrencies

zijn een soort digitale valuta. Sommige cryptocurrencies zijn gedecentraliseerd en worden aangestuurd aan de hand van vastgestelde regels, terwijl anderen gecentraliseerd zijn en beheerd worden door een kleine groep mensen.

Uiteindelijk is een valuta die zonder tussenpersonen werkt efficiënter en beter voor de samenleving, omdat het voorkomt dat een paar individuen de geldvoorraad beheersen en hun macht concentreren. Het creëren van zo'n munteenheid die veilige transacties mogelijk maakt zonder afhankelijk te zijn van vertrouwen tussen partijen is door de geschiedenis heen echter een uitdaging geweest. Om dit te bereiken moet een valuta worden gecreëerd die werkt zoals het internet, waarbij de controle wordt verdeeld over iedereen en niemand tegelijkertijd. Dit vereist de instemming van alle partijen, inclusief de machthebbers, om controle af te staan voor het grotere geheel.

2.5 De psychologie van geld: schaarste, tijdsvoorkeur en afwegingen

Stel je voor dat je gestrand bent in een woestijn en je hebt nog maar één fles water over. Je hebt dorst en wilt wanhopig wat drinken, maar je weet ook dat je het water nodig hebt om te overleven totdat je meer kunt vinden. Dit is een klassiek voorbeeld van schaarste - je hebt maar een beperkte hoeveelheid van een hulpbron (water) en je moet een keuze maken over hoe je het gaat gebruiken. In deze situatie zou je kunnen besluiten om het te rantsoeneren en over een langere periode kleine slokjes te nemen, zodat het zo lang mogelijk meegaat.

Wat is geld?



Schaarste dwingt ons om de voor- en nadelen van het gebruik van onze hulpbronnen tegenover elkaar te zetten en afwegingen te maken.

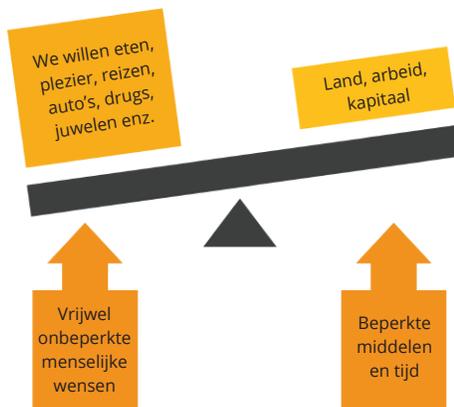
Je kunt ook besluiten om in één keer zoveel te drinken als je kunt, in de hoop dat de uitbarsting van hydratatie je de energie geeft die je nodig hebt om meer water te vinden. Welke keuze je ook maakt, je staat voor een moeilijke beslissing. In dit geval kun je kiezen tussen het onmiddellijke lessen van je dorst of om het water te bewaren voor later. Dit concept van schaars(heid) geldt voor alle soorten hulpbronnen, niet alleen voor water. Of het nu gaat om geld, tijd of zelfs liefde en aandacht, we worden voortdurend geconfronteerd met keuzes over hoe we onze beperkte middelen inzetten.

Er zijn twee soorten schaarste:

- Door mensen gecreëerde schaarste, ook wel gecentraliseerde schaarste genoemd, omvat dingen zoals designertassen in beperkte oplage of zeldzame sportkaarten. Namaak hiervan is vrij makkelijk.
- Natuurlijke schaars(heid), ook wel decentrale schaarste genoemd, omvat zaken als zout, schelpen en edelmetalen zoals goud. Deze zijn moeilijker na te maken of te vervalsen.

Gecentraliseerde schaarste is onder controle van één entiteit, zoals een bedrijf of overheid, terwijl niemand controle heeft over gedecentraliseerde schaarste. Een voorbeeld van gecentraliseerde schaarste, dat vooral arme mensen raakt, is de controle over essentiële hulpbronnen zoals schoon water. In sommige regio's wordt de toegang tot schoon water beheerd door private bedrijven of overheidsinstanties die de distributie ervan kunnen beperken, wat leidt tot schaarste aan deze essentiële hulpbron. Deze gecentraliseerde controle kan leiden tot prijsverhogingen of ongelijke toegang tot schoon water, waarbij verarmde gemeenschappen vaak het zwaarst getroffen worden. Beperkte toegang tot schoon water heeft niet alleen invloed op hun gezondheid en welzijn, maar versterkt ook de armoede omdat ze gedwongen kunnen worden tot het betalen van hogere prijzen voor water, of tot het afleggen van grote afstanden om het te krijgen.

Schaarste beïnvloedt onze keuzes. Inzicht hierin kan onze besluitvorming verbeteren. We moeten vaak kiezen tussen onmiddellijke voordelen en voordelen op de lange termijn, en deze afwegingen vormen ons pad naar het bereiken van onze doelen.



Tijdsvoorkeur verwijst naar het principe dat mensen over het algemeen de voorkeur geven aan het NU in plaats van later



Een voorbeeld van tijdsvoorkeur :

Stel dat je de optie hebt om vandaag €100 te ontvangen of €110 over een jaar. Als je een hoge tijdsvoorkeur hebt, zou je ervoor kunnen kiezen om de €100 vandaag te ontvangen, omdat je meer waarde hecht aan het hebben van de €100 nu dan aan de voordelen van een jaar wachten op de extra €10. Aan de andere kant, als je een lage tijdsvoorkeur hebt, zul je liever wachten op de grotere beloning, omdat je meer gericht bent op langetermijnplanning en minder bezig bent met onmiddellijke voldoening.

Activiteit: tijdsvoorkeur

Activiteit in de klas: hoge tijdsvoorkeur versus lage tijdsvoorkeur

- 1 Luister naar de uitleg over de snoepkeuze.
- 2 Beslis of je nu een klein snoepje of een marshmallow wilt ontvangen, of wacht tot het einde van de les om twee snoepjes of een groter, aantrekkelijker snoepje te ontvangen.
- 3 Neem je beslissing en laat de docent je keuze weten. Ontvang je snoep onmiddellijk of aan het einde van de les, afhankelijk van je beslissing
- 4 Neem deel aan de klassikale discussie over de activiteit en denk na over je besluitvormingsproces en het concept van tijdsvoorkeur .

Conclusie en discussie:

- Welke factoren hebben je beslissing om het snoep nu te nemen, of om te wachten op een grotere beloning in de toekomst, beïnvloed?
- Wat vind je van je beslissing nu deze activiteit voorbij is?
- Kun je voorbeelden uit het echte leven bedenken waar een hoge tijdsvoorkeur schadelijk kan zijn en waar een lage tijdsvoorkeur gunstig kan zijn?
- Wat zijn enkele mogelijke gevolgen van de keuze voor hoge tijdsvoorkeur boven lage tijdsvoorkeur?

In de context van het voorbeeld van de woestijn betekent dit dat je misschien eerder geneigd bent om al het water meteen op te drinken, zelfs als dat betekent dat je dan niets meer over hebt voor later. Dit komt omdat de dorst die je nu voelt dringender is dan de mogelijke dorst die je in de toekomst zou kunnen voelen.

Als je er daarentegen voor kiest om het water te rantsoeneren en het langzaam op te drinken, geef je blijk van een lagere tijdsvoorkeur. Dit betekent dat je bereid bent om te wachten met het lessen van je dorst en het vergroten van je overlevingskansen. Het concept van opportuniteitskosten is nauw verbonden met het idee van schaarste en tijdsvoorkeur.

Wat is geld?



Opportunitetskosten verwijzen naar de waarde van het volgende beste alternatief dat je opgeeft als je een beslissing neemt. **Bij elke beslissing worden afwegingen gemaakt.**

Keuze vandaag



Koop een aardbeien-smoothie voor 7 euro

Nu



Geef de 7 euro uit op een andere manier

Later



Profiteer van het regelmatig sparen van 7 euro

In het voorbeeld van de woestijn zijn de opportunitetskosten om al het water meteen op te drinken de overlevingsvoordelen die je zou hebben gehad door het water te rantsoeneren en over een langere periode te gebruiken.

Stel dat je besluit om het water te rantsoeneren en over een langere periode kleine slokjes te nemen. Daardoor heb je de energie en hydratatie die nodig is om op zoek te gaan naar meer water. Maar terwijl je zoekt, kom je een cactus tegen die een kleine hoeveelheid water bevat. Het is niet veel, maar genoeg om je dorst te lessen. Als je had besloten om al je water in één keer op te drinken, had je misschien niet de energie gehad om meer water te zoeken en de cactus tegen te komen.

In dit geval zou de kans om de cactus te vinden en een betere hydratatie te krijgen de opportunitetskost zijn geweest van het in één keer opdrinken van al je water.

Dit voorbeeld illustreert hoe opportunitetskosten niet alleen betrekking hebben op de onmiddellijke afweging tussen twee opties, maar ook op de potentiële toekomstige kansen die we kunnen krijgen of mislopen als gevolg van onze keuzes.

Onze bereidheid om een grotere beloning in de toekomst op te geven in ruil voor een kleinere beloning nu wordt beïnvloed door onze tijdsvoorkeur, oftewel hoeveel waarde we hechten aan onmiddellijke voldoening van onze behoeftes versus planning op de lange termijn.

In dit hoofdstuk hebben we het fundamentele concept van geld onderzocht. Dit hoofdstuk behandelde de definitie van geld, de functies, eigenschappen en verschillende soorten geld. Een essentieel aspect van onze discussie was het begrijpen van de psychologie van geld, waarbij we ons richtten op concepten als schaarste, tijdsvoorkeur en afwegingen. Dit onderzoek legde de basis voor het begrijpen van de ingewikkelde aard van geld en de rol ervan in ons leven. In het volgende hoofdstuk gaan we het hebben over de geschiedenis van geld en hoe het zich in de loop der tijd heeft ontwikkeld.

Hoofdstuk #3

De geschiedenis van geld

3.0 Inleiding

Activiteit: ruilhandelspel

3.1 Evolutie van ruilhandel naar moderne valuta

3.1.1 Problemen met vroege vormen van geld

3.1.2 Ontwikkeling van munten en papiergeld

3.1.3 Overgang van eerlijk naar oneerlijk geld

3.1.4 Van papieren naar plastic geld

3.2 Digitaal geld

De geschiedenis van geld

3.0 Inleiding

Geld is niet ontwikkeld door ontwerp, maar is ontstaan uit het marktproces. Het werd niet gecreëerd door overheden. Het ontstond in de loop der tijd als een spontane orde.

Murray Rothbard



Stel je een tijd voor, lang geleden, toen mensen nog niet de munten of papieren biljetten hadden die we vandaag de dag gebruiken. In die tijd hadden ze een unieke manier om dingen te verhandelen: ze gebruikten schelpen of edelmetalen zoals goud als een speciaal soort valuta. Dit klinkt misschien vreemd, maar het was hun versie van geld, iets waarvan iedereen vond dat het waarde had. In dit hoofdstuk maken we een reis door de tijd en bestuderen we de evolutie van geld in detail. We traceren de oorsprong en zien hoe geld in de loop van de geschiedenis is veranderd en aangepast.

Activiteit in de klas - ruilverhandelspel

De docent heeft je een papiertje gegeven. Het doel is om wat je "bezit" te ruilen voor je "wens", in een handelsspel dat de monetaire geschiedenis doorloopt. Schrijf je naam bovenaan het papiertje in kleine leesbare letters.

Ronde #1- ruilverhandel

Het is het jaar 6000 voor Christus. Het geld zoals wij dat kennen is vanzelfsprekend nog niet uitgevonden. Je bent in Mesopotamië en wisselt rechtstreeks goederen en diensten met elkaar uit door middel van ruilverhandel.



Veel bedrijven accepteren nog steeds niet-monetaire betalingen voor hun diensten. Fiscaal gezien behandelen overheden deze ruilverhandelingen hetzelfde als valutatransacties.

 Knip je vel papier af op de stippellijn. Je doel is om zoveel mogelijk van je "bezit" weg te ruilen om uiteindelijk je oorspronkelijke "wens" te krijgen. Je kunt je oorspronkelijke "willen" niet veranderen. Je hebt 5 minuten om het doel van deze oefening te bereiken.



Als je nieuwe "bezit" overeenkomt met je oorspronkelijke "wens", ga dan terug naar je stoel. Als de tijd is afgelopen of als je geen handelspartner hebt gevonden, ga je terug naar je stoel.



Steek je hand op als je na één ruil kon krijgen wat je wilde. Twee? Drie?

Beantwoord de volgende vragen kort maar bondig.

1. Waarom konden sommigen van jullie iemand krijgen om mee te ruilen en anderen niet?

2. Wat zijn de voordelen van ruilhandel?

3. Wat zijn de nadelen van ruilhandel op basis van je ervaring met deze oefening?



Ronde #2 - goederengeld

We zijn nu aan de westkust van Afrika, ergens rond de 14e eeuw voor Christus. Ruilhandel is vervelend en inefficiënt geworden. We zijn als beschaving geëvolueerd en gebruiken nu goederengeld.

Van Kaurischelpen naar munten



1,300 v.Chr



1,000 v.Chr



687 v.Chr

Deze proto-munten waren ovaalvormig, gemaakt van "electrum" (een goud/zilver legering) en hadden maar aan één kant een ontwerp.

1.300 v.Chr
Kaurischelpen zijn de belangrijkste vorm van betaling in het grootste deel van Azië, Afrika, Oceanië en sommige delen van Europa.

1.000 v.Chr
De Chinese Westelijke Zhou-dynastie begint metalen munten te gebruiken.

687 v.Chr
Koning Alyattes van Lydië (het huidige Turkije) geeft opdracht om de eerste metalen munten te slaan in de Westerse wereld.



Grappig feitje

Tot in de 20e eeuw werden Kaurischelpen in sommige delen van Afrika geaccepteerd als wettig betaalmiddel.

De geschiedenis van geld

De docent heeft je één macaroni gegeven (voor de eenvoud). Laten afspreken dat de prijs van elk goed één macaroni waard is.

Het doel is weer je "wens" in bezit te krijgen. Maar nu is de menseheid een beetje slimmer geworden en heeft het een manier gevonden om bepaalde problemen op te lossen.

- ☀️ Waarom beschouwen we macaroni als goederengeld?
- ☀️ Hoe krijgen we nu de dingen die we willen?
- ☀️ Was de macaronironde makkelijker?
- ☀️ Waarom denk je dat geld ruilhandel heeft vervangen?
- ☀️ Op welke manieren is het gebruik van goederengeld efficiënter dan ruilhandel?
- ☀️ Wat zijn de nadelen van het gebruik van macaroni als geld?
- ☀️ Wat denk je dat er gebeurde toen Spanje boten vol "macaroni" naar de Amerikaanse gemeenschappen begon te brengen (en goud en zilver uit Amerika terug naar Spanje)?

3.1 Evolutie van ruilhandel naar moderne valuta

3.1.1 Problemen met vroege vormen van geld



Bekijk deze korte video over de oorsprong van ruilmiddelen in de serie "The History of Paper Money".

In ruileconomieën drijven mensen handel met elkaar op basis van de relatieve waarde van de goederen en diensten die ze te bieden hebben. Ruilhandel is inefficiënt en kan moeilijk te overzien zijn, vooral in complexe samenlevingen.

Het "toevallige samenvallen van behoeften" is noodzakelijk in elk ruilhandelsysteem omdat mensen altijd iemand moeten vinden die heeft wat zij willen, en ook bereid zijn om het te ruilen voor wat zij te bieden hebben.



Stel:

- ✿ Joseph wil zijn banaan ruilen voor de kokosnoot van Yael.
- ✿ Maar Yael wil alleen haar kokosnoot ruilen voor Tammy's mango.
- ✿ En Tammy wil alleen haar mango ruilen voor Jozefs banaan.
- ✿ Ze zitten vast in een eindeloze cyclus zonder dat hun behoeften samenvallen.
- ✿ Joseph stelt voor dat ze hun fruit ruilen voor een lekkere koude frisdrank, maar ze realiseren zich dat ze op een afgelegen eiland zijn en dat er geen frisdrank is.
- ✿ Ze besluiten om gewoon op het strand te gaan zitten en in stilte van hun fruit te genieten.

Dit is de tweede aflevering "Not Just Noodles" uit "The History of Paper Money".



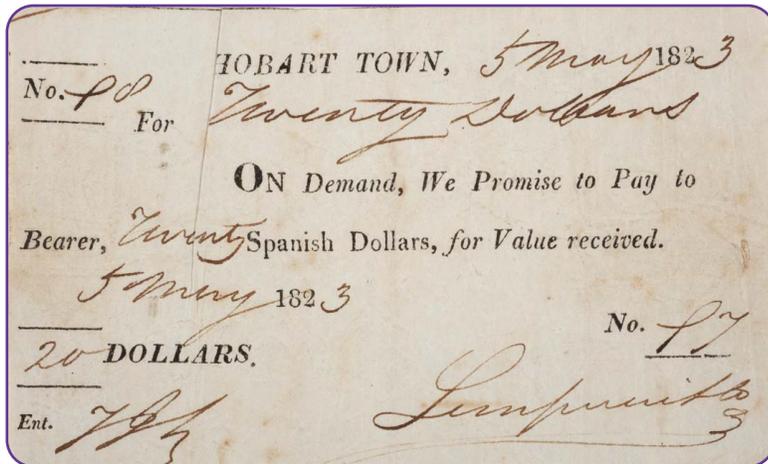
3.1.2 Ontwikkeling van munten en papiergeld

Naarmate jij en je gemeenschap meer betrokken raken bij handel en het zakendoen, realiseer je je de beperkingen van ruilhandel en andere vormen van niet-monetaire ruilhandel. Je besluit om metalen munten als geld te gaan gebruiken.



Goederen die als geld gebruikt worden, zoals goud en zilver, worden **goederengeld** genoemd. Deze edelmetalen worden van oudsher gebruikt als spaarmiddel, ruilmiddel en in het verre verleden ook als rekeneenheid.

De geschiedenis van geld



Naarmate je de metalen munten vaker begint te gebruiken, kom je echter een aantal nadelen tegen. Ze kunnen zwaar en onhandig zijn om mee te nemen bij grote transacties, en je merkt dat sommige mensen misbruik maken van het systeem door de munten om te smelten, ze te mengen met goedkopere metalen, en nieuwe munten te slaan, waardoor de prijzen stijgen en het vertrouwen in het systeem wordt ondermijnd. In een poging om deze problemen aan te pakken, beginnen jij en je gemeenschap papieren bonnetjes te gebruiken als een vorm van geld. Deze papieren bonnetjes,

die hun oorsprong vinden in het oude China, zijn een handige en gemakkelijk inwisselbare vorm van valuta. Ze worden gedekt door goud en andere waardevolle metalen, en kunnen ervoor ingeruild worden van de zeventiende tot en met de negentiende eeuw. Hierdoor heb je een meer draagbare en gemakkelijk overdraagbare vorm van geld, terwijl je toch de waarde en veiligheid van edelmetalen behoudt.

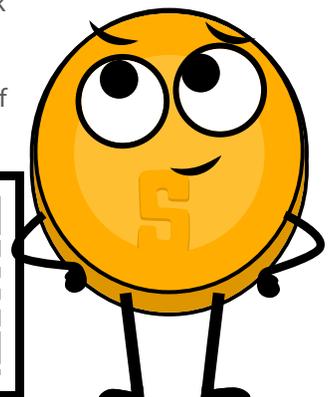


3.1.3 Overgang van eerlijk naar oneerlijk geld

We gaan naar de 17e eeuw in Zweden en je bent nu volledig afhankelijk van banken voor de opslag van je waardevolle bezittingen. Je begint echter te merken dat er iets vreemds aan de hand is met deze bankiers. Het lijkt erop dat ze meer papieren bonnen uitgeven dan dat ze goud in voorraad hebben, waardoor ze meer geld creëren dan ze bezittingen hebben. Door deze stiekeme handeling kunnen de bankiers profiteren van het verschil tussen de waarde van de papieren bonnetjes en de waarde van het goud dat ze voor hun klanten bewaren.



Wat gebeurt er als je de stiekeme praktijk van papiergeld echt in de praktijk probeert te brengen? Kom erachter in de vierde aflevering van "The History of Paper Money".



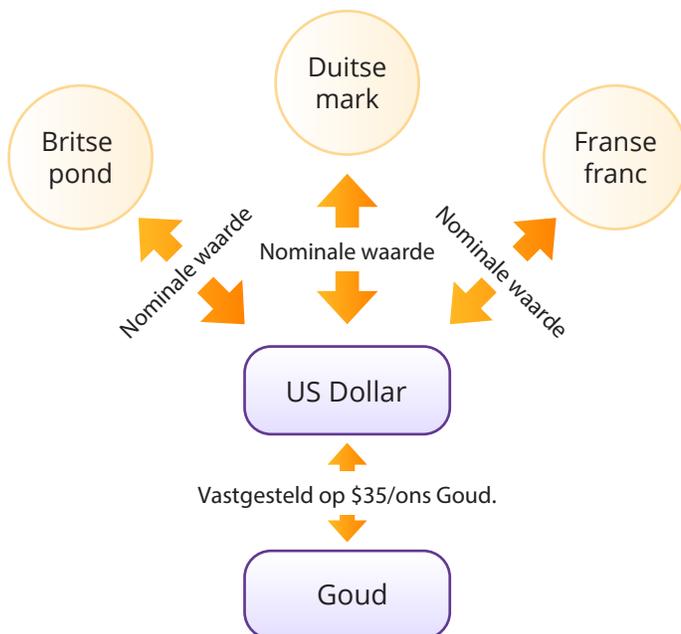
Je realiseert je dat dit een grote verschuiving betekent in de manier waarop geld werkt. Je gaat van een systeem van eerlijk geld (d.w.z. geld dat wordt gedekt door edelmetalen) naar een systeem van oneerlijk geld (d.w.z. fiatvaluta die niet worden gedekt door een fysieke grondstof). Deze overgang gebeurde niet van de ene op de andere dag, maar was een geleidelijk proces dat door verschillende factoren werd beïnvloed. De industriële revolutie, met zijn massaproductie en verstedelijking, speelde een rol, net als de groei van geavanceerde financiële systemen zoals banken en aandelenmarkten. De opkomst van centrale banken en andere monetaire autoriteiten droeg bij aan de centralisatie van de macht over het geld, wat leidde tot de uitgifte van fiatvaluta om de economische groei te stimuleren.



Je begint echter ook de **nadelen** van deze centralisatie te zien, zoals onverantwoorde consumptie, toename van **schulden** en manipulatie van het gedrag van burgers door de invoering van economische prikkels.

Tot de Eerste Wereldoorlog kon je je papiergeld omruilen voor een afgesproken hoeveelheid goud. De twee wereldoorlogen en de economische crisis van 1929 maakten daar echter een einde aan. In 1944 werd de overeenkomst van Bretton Woods getekend, waardoor de Amerikaanse dollar de wereldreservemunt werd en de waarde van de Amerikaanse dollar werd gekoppeld aan de goudprijs tegen een koers van \$35 per Troy Ounce (≈31.1 gram) goud. De valuta van andere landen werden gekoppeld aan de dollar, wat hielp om de internationale financiële markten te stabiliseren.

Bretton Woods Systeem (1945-1972)



Helaas begon het systeem eind jaren zestig in te storten, wat leidde tot de Nixon Shock in 1971, toen de Amerikaanse regering de omwisselbaarheid van de dollar in goud opschortte. Dit markeerde het einde van de goudstandaard en het begin van een wereld die gedreven wordt door de creatie en accumulatie van schulden. In je dagelijkse leven merk je dat de waarde van geld niet meer zo stabiel is als vroeger. Net zoals dat een liniaal met een constant veranderende meeteenheid het moeilijk zou maken om de lengte van een tafel nauwkeurig te meten, kan het leven in een fiatwereld waar de waarde van geld onderhevig is aan de onvoorspelbaarheid van de machthebbers het ook moeilijk maken om de waarde van goederen en diensten nauwkeurig te meten. Een wereld waarin de waarde van geld niet langer gekoppeld is aan een fysiek goed zoals goud resulteert in verwarring en ongemak.

De geschiedenis van geld

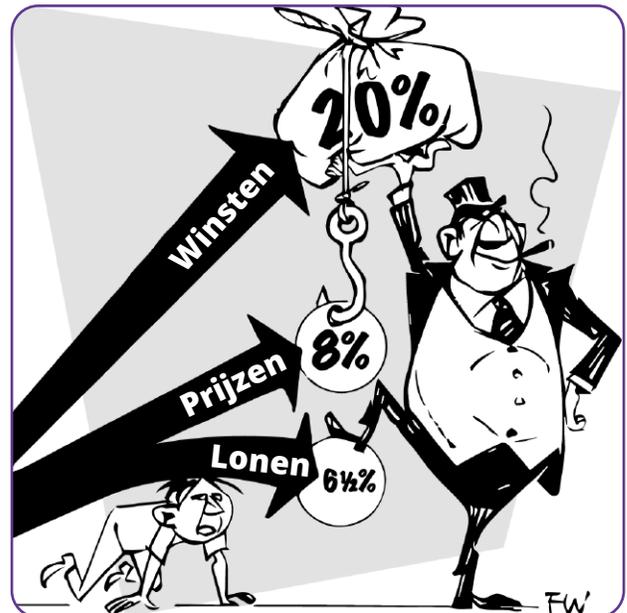
Je ziet de gevolgen van deze verschuiving op de wereldeconomie en begint vraagtekens te zetten bij de stabiliteit en betrouwbaarheid van fiatgeld. Je realiseert je dat in deze moderne wereld de dollar niet langer vast en consistent is zoals toen hij nog aan goud was gekoppeld, maar in plaats daarvan onderhevig is aan fluctuaties. Dit maakt het moeilijker om overheidsgeld als rekeneenheid te gebruiken, omdat de waarde wordt beïnvloed door verschillende factoren, waaronder inflatie (stijgende prijzen), rentetarieven, de sterkte van de economie van het land, politieke gebeurtenissen, marktspeculatie en de vraag in de internationale handel. Het kan een verwarrende en onvoorspelbare tijd zijn, waarin je probeert te navigeren door de voortdurend veranderende waarde van het geld en de invloed ervan op je dagelijkse leven.

Ondanks inspanningen om de kwaliteit van leven te verbeteren door moderne monetaire systemen, grotere efficiëntie, betere toegang tot informatie en verbeterde communicatie, begint de levensstandaard van de meeste mensen te dalen als gevolg van:

- Misbruik van gecentraliseerde macht.
- Stijgende prijzen.
- Stagnerende reële lonen.
- Verzwakkende valuta.
- De noodzaak om meer geld uit te geven voor minder dingen.

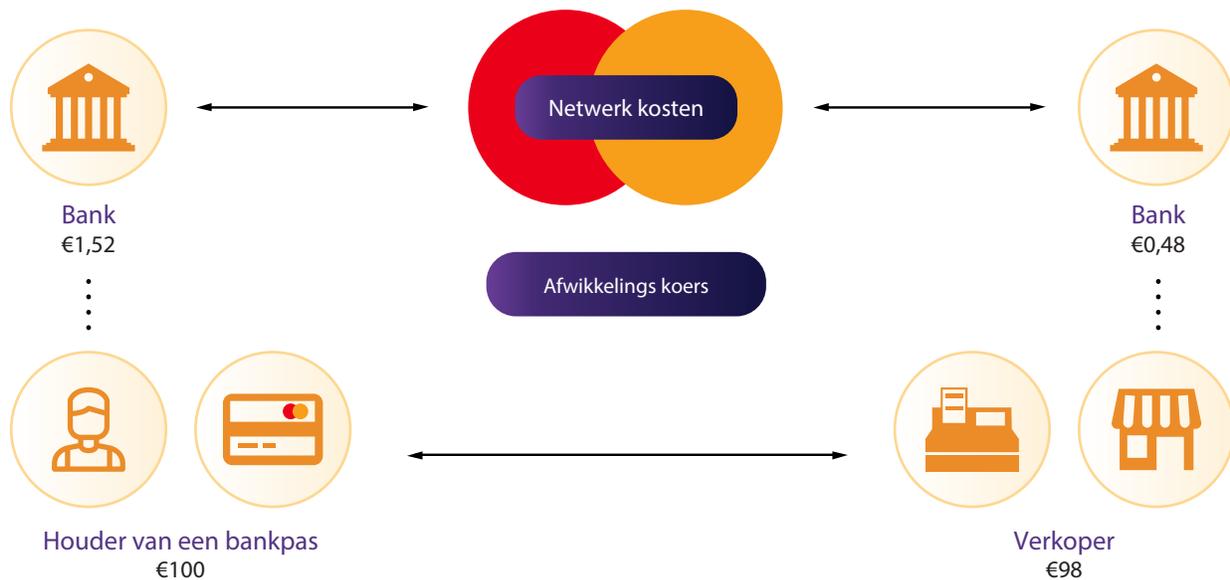
Dit brengt uitdagingen met zich mee voor mensen met minder economische middelen, die mogelijk beperkte toegang hebben tot onderwijs, krediet, middelen, sociale netwerken en politieke vertegenwoordiging. Dit beperkt hun kansen op succes.

Als gevolg daarvan lijken de rijken steeds rijker te worden en de armen steeds armer.



3.1.4 Van papieren naar plastic geld

We hebben een lange weg afgelegd sinds de introductie van de eerste creditcard in de jaren 1950. Met zo'n plastic pas kunnen we kopen wat we willen, wanneer we willen, zonder gedoe. Het is alsof er een wereld van eindeloze mogelijkheden voor ons opengaat en de opwinding om te ontdekken wat die wereld in petto heeft is voelbaar... dat dachten we tenminste. Toen wisten we nog niet dat onze afhankelijkheid van krediet pijnlijke gevolgen zou hebben - zoals de toename van de kosten van goederen of het aanjagen van een economie die gedoemd is te mislukken.



Naarmate de technologie zich ontwikkelt, verandert ook de manier waarop we met geld omgaan. Het internet wordt een belangrijke speler in de financiële wereld, met online bankieren en e-commerce websites die het mogelijk maken om geld volledig online te beheren en uit te geven.

De opkomst van digitaal geld markeert de volgende belangrijke sprong in deze evolutie, die nieuwe mogelijkheden biedt en de manier waarop we financiële transacties uitvoeren verandert.

3.2 Digitale valuta

Digitale valuta bestaan, in tegenstelling tot traditionele valuta, alleen in elektronische vorm. Ze worden opgeslagen en uitgewisseld met behulp van computers en speciale software.

Digitale valuta stellen mensen in staat om hun geld via internet te versturen. Net zoals e-mail ons in staat stelt om onmiddellijk en zonder verzendkosten berichten te versturen, stellen digitale valuta ons in staat om onmiddellijk en met zeer weinig kosten waarde te versturen en te ontvangen.

Het geld dat we vandaag de dag gebruiken wordt steeds meer digitaal. Slechts een klein deel van de geldvoorraad bestaat nog in de vorm van munten en papieren biljetten. Banken en bankdiensten bieden hun gebruikers apps aan om onbelemmerd transacties te doen via het internet. Maar waar komt het geld vandaan?

In dit hoofdstuk zijn we getuige geweest van de transformatie van eerlijk geld, vertegenwoordigd door goud, naar oneerlijk geld in de vorm van papier, en nu digitaal fiatgeld. In het volgende hoofdstuk zullen we onderzoeken hoe het huidige fiatgeldsysteem werkt en hoe het is ontstaan.

Hoofdstuk #4

Wat is fiatgeld en wie beheert het?

4.0 Inleiding

4.1 Korte geschiedenis van fiatgeld

4.2 Het fiatsysteem

4.2.1 Een monetair systeem per decreet

4.2.2 Fractioneel bankieren een systeem gevoed door schulden

Activiteit: fractioneel bankieren

4.2.3 Wie beheert het fiatsysteem en hoe profiteren zij ervan?

4.3 Digitaal centralebankgeld: De toekomst van fiatgeld

Wat is fiatgeld en wie beheert het?

4.0 Inleiding

De geschiedenis van de mensheid is de geschiedenis van geld dat zijn waarde verliest.

Milton Friedman

In het vorige hoofdstuk zagen we hoe geld zich in de loop der tijd ontwikkelde en hoe ons monetaire systeem veranderde van eerlijk naar oneerlijk geld, waardoor de wereld waarin we nu leven vorm heeft gekregen. In dit hoofdstuk gaan we dieper in op hoe deze ontwikkelingen hebben geleid tot het huidige fiatsysteem en hoe het werkt.

Dus, hoe ziet dit fiatsysteem eruit en hoe is het ontstaan? Om deze vraag te beantwoorden moeten we beginnen met onze aandacht te richten op de Amerikaanse dollar, de huidige wereldreservemunt, die vandaag de dag een dominante rol speelt in de wereld. Elk land voelt, direct of indirect, de invloed van de beslissingen die worden genomen over de Amerikaanse dollar. Om echt te begrijpen hoe het systeem in jouw land werkt, is het essentieel om de historische connectie met de geboorteplaats van het fiatsysteem te doorgronden - de Verenigde Staten van Amerika.

4.1 Korte geschiedenis van fiatgeld

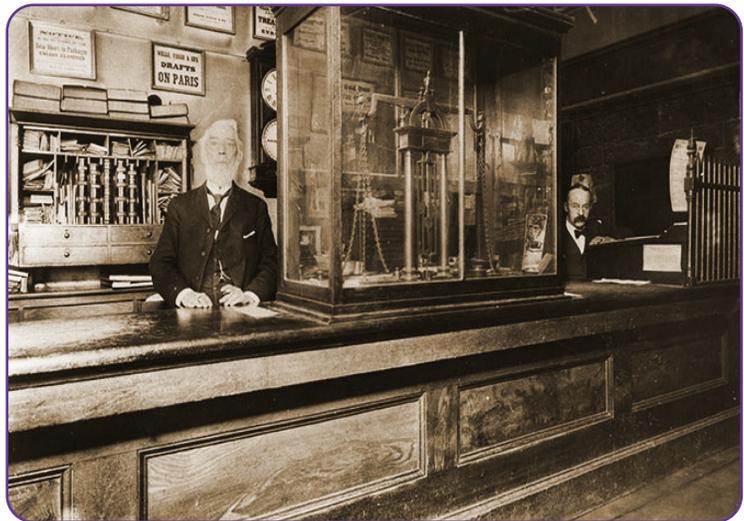
1815-1933	1913	1933	1934	1944	1971	1980
De Goudstandaard	Oprichting van de Amerikaanse Centrale Bank genaamd "de Federal Reserve".	Executive Order 6102. Iedereen was verplicht om zijn goud in te leveren tegen een wisselkoers van \$20,67 per Troy Ounce.	Gold Reserve Act. Rijkdom stelen van het volk door de dollar met 40% te devalueren tot \$35 per Troy Ounce goud.	Overeenkomst van Bretton Woods: USD werd de dominante wereldreservemunt	Nixon Shock. Nixon maakte een einde aan de inwisselbaarheid van Amerikaanse dollars voor goud.	De waarde van goud steeg van \$35 per Troy Ounce in 1970 naar \$870 in 1980, waardoor het geld van mensen in slechts 10 jaar 96% aan waarde verloor.

Visuele tijdlijn

In de 19e eeuw floreerden beschavingen wereldwijd op een eerlijke geldstandaard, waarbij edelmetalen als goud en zilver werden gebruikt vanwege hun schaarsheid, duurzaamheid en herkenbaarheid. Toen de wereldhandel groeide, werd het vervoeren van grote hoeveelheden metaal een uitdaging, wat leidde tot de opkomst van goud- en zilvermagazijnen. Deze beveiligde opslagplaatsen bewaarden de edelmetalen van mensen en verstrekten papieren geldbewijzen die konden



worden ingewisseld voor specifieke hoeveelheden goud of zilver. In ruil voor het storten van hun geld ontvingen mensen papieren geldbewijzen die direct gekoppeld waren aan de exacte hoeveelheid goud of zilver die ze hadden opgeslagen. Deze directe link tussen geldbewijzen en tastbaar goederengeld markeerde het begin van wat we nu kennen als banken.

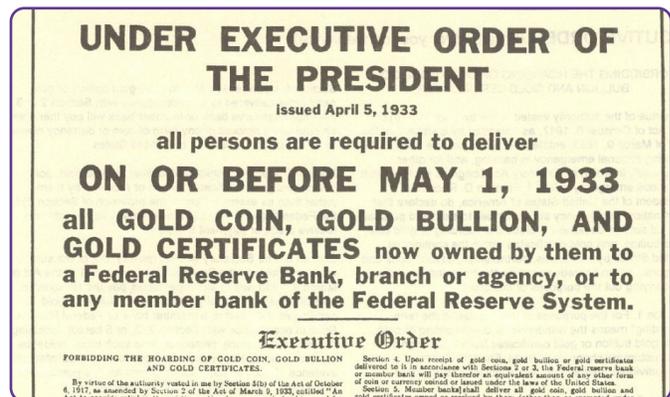


Aanvankelijk probeerden banken het geld van hun klanten veilig te stellen, maar later gingen ze over tot riskante uitleenpraktijken waarbij geldbewijzen werden uitgegeven voor goud dat ze niet hadden. Hierdoor dreigden bankruns te gebeuren, waarbij te veel klanten tegelijkertijd hun geld opeisen. Om dit risico aan te pakken, werkten banken samen met overheden om een systeem op te zetten dat het meermaals uitleenen van geld legaliseerde. In 1913 richtten ze de Federal Reserve op, de Amerikaanse centrale bank, die verantwoordelijk was voor het uitgeven van nieuwe geldbewijzen om er vervolgens banken in moeilijkheden mee te redden. Wereldwijd erkenden regeringen de waarde van goud en zilver, wat leidde tot conflicten en oorlogen om de controle erover. In de jaren voorafgaand aan de Tweede Wereldoorlog namen leiders als Lenin, Stalin, Churchill, Roosevelt, Mussolini en Hitler goud in beslag voor strategische doeleinden.



In het begin van de jaren 1930 vond er een belangrijke verandering plaats in de manier waarop geld in de Verenigde Staten werd gedekt door activa. In die tijd hadden mensen veel van hun vermogen in de vorm van goud. Maar in 1933 vaardigde president Roosevelt Executive Order 6102 uit, die eiste dat elke burger zijn goud opgaf. Dit was geen vrijwillige ruil - mensen moesten hun goud inleveren en als ze weigerden, stonden hen zware straffen te wachten.

De overheid stelde de wisselkoers vast op \$20,67 per Troy Ounce goud. Dit betekende dat voor elke Ounce goud die iemand had, hij papieren certificaten ontving die gelijk waren aan \$20,67. Mensen moesten deze papieren dollars accepteren, in de hoop dat ze ze op een dag weer zouden kunnen inwisselen voor goud.

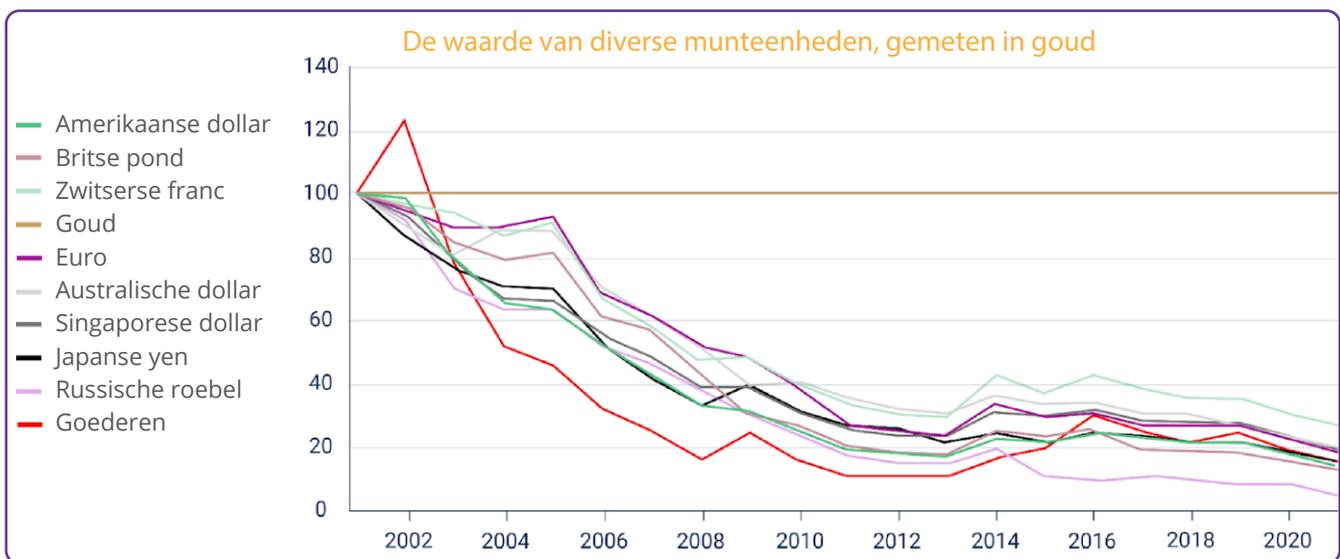


Wat is fiatgeld en wie beheert het?

In 1934 zorgde de Gold Reserve Act ervoor dat mensen hun papieren dollars weer konden inwisselen voor goud. Er zat echter een addertje onder het gras. De regering devalueerde de papieren dollars opzettelijk door de wisselkoers te verhogen naar \$35 per ounce goud. Deze devaluatie trof vooral hardwerkende mensen in de lagere en middenklasse, omdat het betekende dat hun spaargeld, dat ooit meer koopkracht vertegenwoordigde, hen nu minder opleverde door de daling van de koopkracht van de papieren dollars.

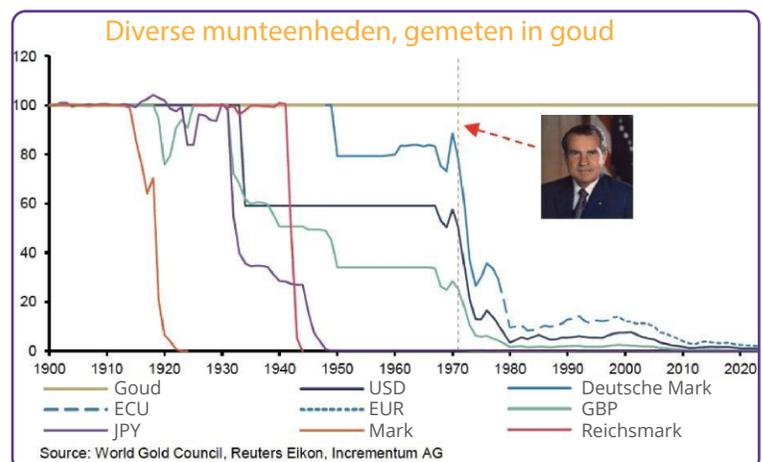
Na de Tweede Wereldoorlog werd de Amerikaanse dollar de wereldreservemunt door de overeenkomst van Bretton Woods in 1944. In die tijd kon de Amerikaanse dollar door overheden worden ingewisseld voor goud. Deze koppeling tussen de Amerikaanse dollar en goud werd echter verbroken in 1971 toen president Nixon een einde maakte aan de inwisselbaarheid van de Amerikaanse dollar voor goud. Dit betekende een belangrijke verschuiving, die leidde tot de invoering van een systeem van fiatgeld waarbij de valuta niet wordt gedekt door een fysiek goed zoals goud, maar eerder door het vertrouwen van de mensen die het gebruiken.

Terwijl regeringen en centrale banken de meerderheid van het goud van het volk in beheer had, steeg de prijs van goud tot \$870 per Troy Ounce in 1980.



Samenvattend is het verhaal van hoe de menselijke samenleving overging van een eerlijke geldstandaard naar een oneerlijke (fiat)standaard het verhaal van hoe overheden en banken edelmetalen van hun burgers afpakten.

Terwijl het echte geld in de zakken van regeringen en banken belandde, bleven de mensen achter met stukjes papier waarvan de enige reden om het te gebruiken voortkomt uit de verplichting die de overheid hiertoe oplegt.



4.2 Het fiatsysteem

Het kernprobleem van conventionele valuta is het vertrouwen dat nodig is om het te laten werken. Je moet de centrale bank kunnen vertrouwen dat ze de munt niet zal devalueren, maar de geschiedenis van de fiatvaluta staat bol van de schendingen van dat vertrouwen.

Satoshi Nakamoto

De mensheid is overgegaan van eerlijk geld beheerd door velen, naar oneerlijk geld dat beheerd wordt door enkelen. Maar hoe werkt dit systeem precies?

4.2.1 Een monetair systeem per decreet

Het fiatsysteem wordt gekenmerkt door zijn dwingende aard, opgelegd aan mensen door middel van wetten. Het overheidsgeld wordt een wettig betaalmiddel. De term "fiat", afkomstig uit het Latijn, betekent "per decreet" en staat voor een richtlijn van de overheid.

In tegenstelling tot geld dat gedekt wordt door tastbare goederen zoals goud, ontbreekt een dergelijke dekking bij fiatgeld. In plaats daarvan wordt het gebruik ervan bij wet verplicht gesteld. Alledaagse valuta zoals dollars, euro's, ponden, yuans, peso's en andere vallen onder de categorie fiatgeld.

Wettig betaalmiddel: Een specifieke valuta die door alle burgers verplicht moet geaccepteerd worden.



De waarde van fiatgeld is gebaseerd op het geloof dat het kan worden ingewisseld voor goederen en diensten, en de illusie dat het zijn koopkracht in de loop der tijd zal behouden. Fiatgeld is vergelijkbaar met een concertkaartje; de waarde ervan zit niet in het kaartje zelf, maar in het geloof dat de artiesten (de regering en haar centrale bank) een geweldige show zullen geven (voor economische stabiliteit zullen zorgen).

Voordelen van fiatgeld

- Gebruiksgemak: fiatgeld is handig voor dagelijkse transacties.
- Lagere kosten en risico's: fiatgeld vereist geen zware beveiliging zoals goud, waardoor het goedkoper en veiliger is.

Nadelen van fiatgeld

- Inflatierisico's: doordat meer geld kan worden gemaakt, kunnen prijzen stijgen en kan zelfs hyperinflatie optreden.
- Gecentraliseerde controle en manipulatie: kleine groepen kunnen het systeem beïnvloeden en manipuleren, wat leidt tot censuur en inbeslagname.
- Tegenpartijrisico: als de overheid voor uitdagingen komt te staan, kan men de munteenheid devalueren.
- Potentie op misbruik: kan leiden tot corruptie en verlies van vertrouwen

Wat is fiatgeld en wie beheert het?

Goederen vs. fiatgeld: zie het verschil

Onthoud: voordat fiatgeld ontstond, sloegen regeringen munten uit een waardevol, schaars en moeilijk te krijgen fysiek goed, zoals goud of zilver, of drukten ze papiergeld dat kon worden ingewisseld voor een vaste hoeveelheid van dit fysieke goed. Dit was het door goederen gedekte systeem.

In het fiatsysteem lijkt het meer op monopoly geld. Geld in het fiatsysteem bestaat uit stukjes papier die gedrukt zijn door de centrale bank, en het beleid van de overheid beïnvloedt direct de koopkracht ervan. De overheid en de centrale banken zijn in feite "de bankiers van het monopolyspel" die bepalen hoe het spel werkt, wie wat krijgt en hoeveel het waard is. Met andere woorden, de overheid belooft het monetaire systeem goed te beheren.

De conclusie is dat fiatgeld alleen waarde vertegenwoordigt omdat de overheid het gebruik ervan verplicht stelt.

Samengevat is het fiatsysteem een vertrouwensspel waarbij de koopkracht van ons geld afhangt van de beloften van de machthebbers, en mensen alleen maar kunnen hopen dat hun regering handelt in het voordeel van iedereen. Hierna zullen we zien hoe banken nieuw geld maken, wie erbij betrokken zijn en hoe dit de economie beïnvloedt.

4.2.2 Fractioneel bankieren: een systeem gevoed door schulden

Het is goed dat de mensen van de natie ons bank- en monetaire systeem niet begrijpen, want als ze dat wel deden, denk ik dat er vóór morgenochtend een revolutie zou zijn.

Henry Ford

Fractioneel bankieren is een van de belangrijkste onderdelen van het fiatsysteem, waardoor banken een aanzienlijk deel van de deposito's van hun klanten kunnen uitlenen. Heb je je ooit afgevraagd waarom banken hun klanten zoveel diensten aanbieden? Hoewel het misschien lijkt alsof ze vrijgevig zijn, is het belangrijk om te onthouden dat banken bedrijven zijn en dat hun primaire doel is om winst te maken. Maar hoe maken ze winst als ze geld weggeven via leningen?

Naast het verdienen van rente op deposito's, genereren banken inkomsten op andere manieren, zoals door:

- Rente in rekening te brengen op leningen die ze verstrekken.
- Kosten in rekening te brengen voor diensten zoals het gebruik van pinautomaten en het bijhouden van een rekening.
- Geld te verdienen met beleggen, zoals het kopen en verkopen van aandelen of door te beleggen in onroerend goed.
- Een percentage van de leningen in reserve te houden en de rest te investeren of uit te lenen.
- Rente te laten betalen op deposito's en kosten in rekening te brengen op betaal- en spaarrekeningen.



Als een bank een storting ontvangt, moet ze slechts een deel houden (dit heet de reserveverplichting) en kan ze het resterende deel uitlenen. Als je bijvoorbeeld €100 stort met een reserveverplichting van 10%, kan de bank €90 uitlenen en slechts €10 als reserve aanhouden. De lener stort €90 bij een andere bank, waardoor de cyclus doorgaat. Ondanks de eerste storting van €100 groeit de totale hoeveelheid geld in de economie tot €271, schijnbaar uit het niets - een fenomeen dat bekend staat als het multipliereffect.

Dit proces leidt tot een door schuld gedreven monetair systeem omdat banken bij elke lening nieuw geld in omloop brengen, waardoor de totale geldhoeveelheid toeneemt. Als fractioneel bankieren door blijft gaan, stijgt de totale schuld in de economie, wat bijdraagt aan prijsstijgingen.

Zo'n systeem vertrouwt op een voortdurende cyclus van geldschepping door leningen, vergelijkbaar met een constante voorraad drugs voor een drugsverslaafde. Maar, als banken meer geld uitlenen dan ze aan reserves hebben en depositohouders haasten zich om tegelijkertijd geld op te nemen, een zogenaamde bankrun, kunnen die banken failliet gaan.

In dat geval treedt de centrale bank op als kredietverstrekker, als laatste redmiddel, door nieuw geld te verschaffen en zo bankfaillissementen te voorkomen. De centrale bank doet dit door bankactiva op te kopen of door direct geld te storten op de rekeningen van de banken in nood. In feite worden banken gered van faillissementen door de constante injectie van nieuw geld door centrale banken. Dit door schulden gevoede systeem, systematisch gered door de centrale bank, leidt tot cycli van hoog- en laagconjunctuur.

Stel je voor dat je een vriend hebt die toevallig bankier is, laten we hem Dax noemen.

Dax is gek op fietsen en hij wil jouw fiets lenen omdat hij nog heel wat te doen heeft. Je geeft hem jouw fiets, en in een opwelling belooft Dax aan een heleboel andere vrienden dat ze altijd gebruik kunnen maken van de fiets. Met jouw ene echte fiets die je hem leent, slaagt Dax erin om meer denkbeeldige fietsen te maken en begint hij ze uit te lenen aan vrienden. Al zijn vrienden denken dat ze een leuk ritje kunnen maken wanneer ze maar willen. Maar er is één probleem - er is maar één echte fiets! Alle ander fietsen zijn denkbeeldig en alleen maar beloftes.

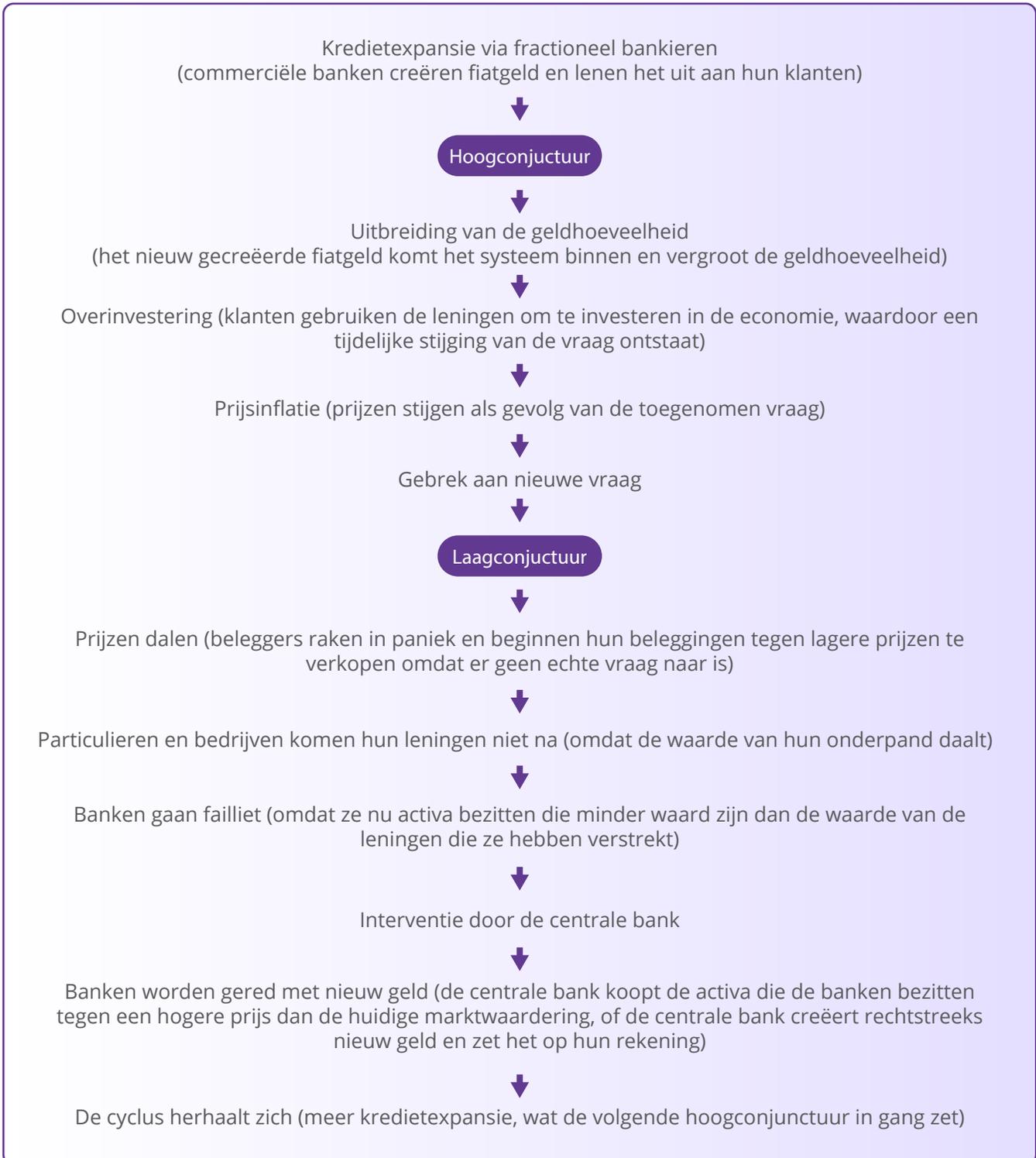
Dus wat gebeurt er... naarmate er meer denkbeeldige fietsen in omloop komen, wordt iedereen erg blij. In eerste instantie tenminste. Want in het begin gebruikt niemand de fiets op hetzelfde moment. Het lijkt alsof er geen probleem is. Het voelt alsof er een overvloed aan fietsen is voor iedereen. Dus beginnen alle vrienden meer plannen te maken, na te denken over alle plaatsen waar ze met hun fietsen naartoe zullen gaan.

Hier begint de magie echter zijn charme te verliezen. Op een zonnige dag besluit iedereen dat het een perfecte dag is voor een fietstocht. Ze staan allemaal vol enthousiasme voor de deur bij Dax, klaar om een ritje te maken op hun denkbeeldige fietsen. Maar dan komt de realiteit - er is maar één echte fiets. Teleurstelling volgt en plotseling neemt de waarde van de beloofde ritjes af.

In de wereld van fractioneel bankieren is het een vergelijkbaar verhaal. Banken lenen meer geld uit dan ze eigenlijk hebben en daar profiteert iedereen een tijdje van. Er circuleert meer geld en iedereen acht zich rijk. Maar als te veel mensen tegelijkertijd hun geld proberen op te nemen, wordt de werkelijke waarde duidelijk: er is niet genoeg geld om alle beloftes na te komen.

Dit scenario tast het algemeen welzijn en het gevoel van vertrouwen van alle betrokkenen aan. De belofte van overvloed verandert in oplichterij. Net zoals dat de beloofde fietsen hun ingebeelde waarde verliezen wanneer iedereen een echt ritje wil maken, kan de waarde van geld in de economie afnemen wanneer iedereen zich haast om zijn echte deel op te eisen. Als dat gebeurt, komen mensen erachter dat het geld dat ze bij een bank hebben er niet echt is, wat leidt tot paniek, bankruns en zelfs de ineenstorting van hele economieën. Degenen die voor deze ineenstortingen betalen zijn tot nu toe altijd dezelfde groep geweest: de lagere en middenklassen van de wereld.

Wat is fiatgeld en wie beheert het?



Activiteit: fractioneel bankieren

In de volgende oefening onderzoeken we hoe fractioneel reservebankieren kan leiden tot geldontwaarding, inflatie en een afname van de koopkracht. We gebruiken een vereenvoudigd voorbeeld met zes deelnemers, waarvan één iemand de bank speelt met een reservevereiste die vandaag de dag nog steeds veel gebruikt wordt, namelijk 10%.

- ✿ Persoon A heeft net €100.000 gewonnen in de loterij en stort dit op de bank (B). Met een reservevereiste van 10% moet B €10.000 in de kluis houden en kan de resterende €90.000 worden uitgeleend.
- ✿ Persoon C leent het maximale bedrag (€90.000) van B en gebruikt het om een huis van D te kopen.
- ✿ Persoon D stort de €90.000 die hij van C heeft ontvangen op de bank (B). De totale deposito's op de bank zijn nu €190.000.
- ✿ Persoon E vraagt een lening aan bij B, waarna de bank 90% van de nieuwe inleg uitleent, wat €81.000 is.
- ✿ Persoon E gebruikt de lening van €81.000 om een kunstwerk te kopen van F, die het geld vervolgens op de bank (B) stort. Het totaal aan geregistreerde stortingen is nu €271.000.

In dit scenario heeft de eerste storting van €100.000 geleid tot een totaal van €271.000 aan deposito's na circulatie door de economie.

Als de reservevereiste zou worden verlaagd naar 1%, zou de hoeveelheid geld die wordt gecreëerd aanzienlijk hoger zijn ($€100.000 / 0,01 = €10.000.000$). Hoeveel geld zou er in dit geval daadwerkelijk worden gecreëerd met die €100.000 als het geld door de economie blijft circuleren?

Het is belangrijk om te weten dat de Federal Reserve (de centrale bank van de VS), om de economie te stimuleren, vanaf 2020 de reserveverplichtingen heeft verlaagd naar nul procent.

We hebben de volgende vrijwilligers nodig:

- A = Depositohouder (wint Loterij) (Lichtblauw)
- B = Bankkassier (Bank)
- C = Debiteur #1 (Donkerblauw)
- D = Eigenaar/Depositohouder (Rood)
- E = Debiteur #2 (Lichtpaars)
- F = Kunstgalerie Eigenaar en Depositohouder (Groen)

Fractioneel bankieren

½ aanhouden



Stort
€1,000



€1,000

Enrique

½ in reserve houden

€500

½ uitleen

€500

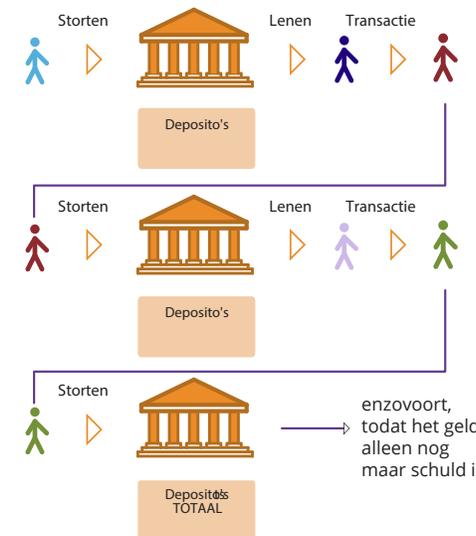


€500

Kari



Geldhoeveelheid groeide van €1,000 naar €1,500.



Wat is fiatgeld en wie beheert het?

4.2.3 Wie beheert het fiatsysteem en hoe profiteren zij ervan?

Er zijn vier hoofdrolspelers: de overheid, rijke individuen, de financiële sector en de centrale bank. Samen beheersen ze het fiatsysteem.

☀ De overheid: de overheid is als het ware de regisseur van de fiatshow. Samen met het innen van belastingen wordt ze gefinancierd door het uitgeven van nieuw schuldpapier (staatsobligaties) door het ministerie van financiën van het land. Als er onvoldoende vraag is naar deze obligaties, wordt de resterende schuld opgekocht door de centrale bank. Dit betekent dat ze hun activiteiten kunnen blijven uitvoeren en hun belangen kunnen blijven nastreven zonder de goedkeuring van het volk nodig te hebben. Het is alsof je een creditcard krijgt zonder dat je je zorgen hoeft te maken over het onmiddellijk terugbetalen ervan. Dit lijkt misschien goed voor de overheid, maar het gaat ten koste van alle anderen.

☀ Rijke individuen: rijke individuen hebben veel baat bij het fiatsysteem. Met de mogelijkheid om meer schuld op te bouwen, kunnen ze investeren in activa zoals goederen, onroerend goed en aandelen, waardoor ze bijna moeiteloos nieuwe rijkdom opbouwen.

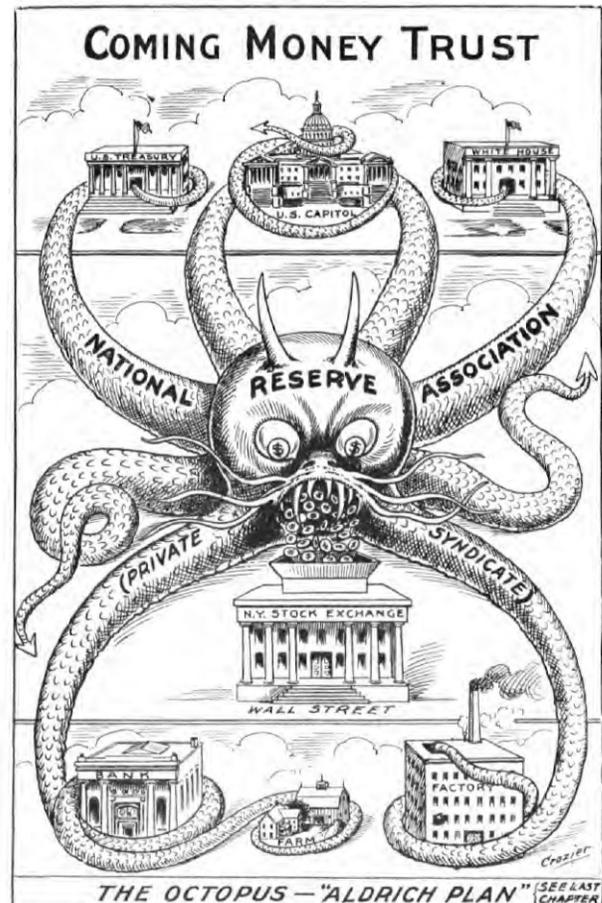
☀ Financiële sector: banken en andere financiële instellingen hebben geen directe controle over het fiatsysteem, maar profiteren er wel enorm van. Vrij van verantwoordelijkheid kunnen ze de creatie van nieuw geld nastreven en versnellen door het fractioneel uit te lenen, waardoor ze profiteren van hogere inkomsten. Bankieren zijn vrijwel gevrijwaard van consequenties omdat ze worden gered met nieuw gecreëerd fiatgeld om te voorkomen dat het hele systeem instort.

☀ De Centrale Bank: de centrale bank is degene die aan de touwtjes trekt en zogenaamd de groei van de geldhoeveelheid regelt. Maar dit is de truc: de centrale bank is ook onderworpen aan de wetten van de overheid en dient de belangen van de overheid. Het is alsof een poppenspeler wordt bestuurd door een andere poppenspeler. De centrale bank lijkt misschien de baas te zijn, maar dient indirect de wensen van de overheid om geld uit het niets te drukken wanneer ze het nodig hebben.

Hoe ze profiteren:

Deze groepen profiteren op verschillende manieren, waardoor een complex web van controle ontstaat. De overheid krijgt geld zonder onmiddellijke gevolgen, rijke individuen en banken verdienen moeiteloos geld en de centrale bank houdt de show draaiende. Ondertussen kan de rest van de bevolking de gevolgen dragen en voor steeds meer uitdagingen komen te staan naarmate dit systeem zich verder uitbreidt.

Uiteindelijk creëren de poppenspelers van het fiatsysteem een show waar enkelen veel profijt van hebben, maar velen zich afvragen of het financiële toneel waarop ze zich bevinden wel eerlijk is.



De rol van centrale banken

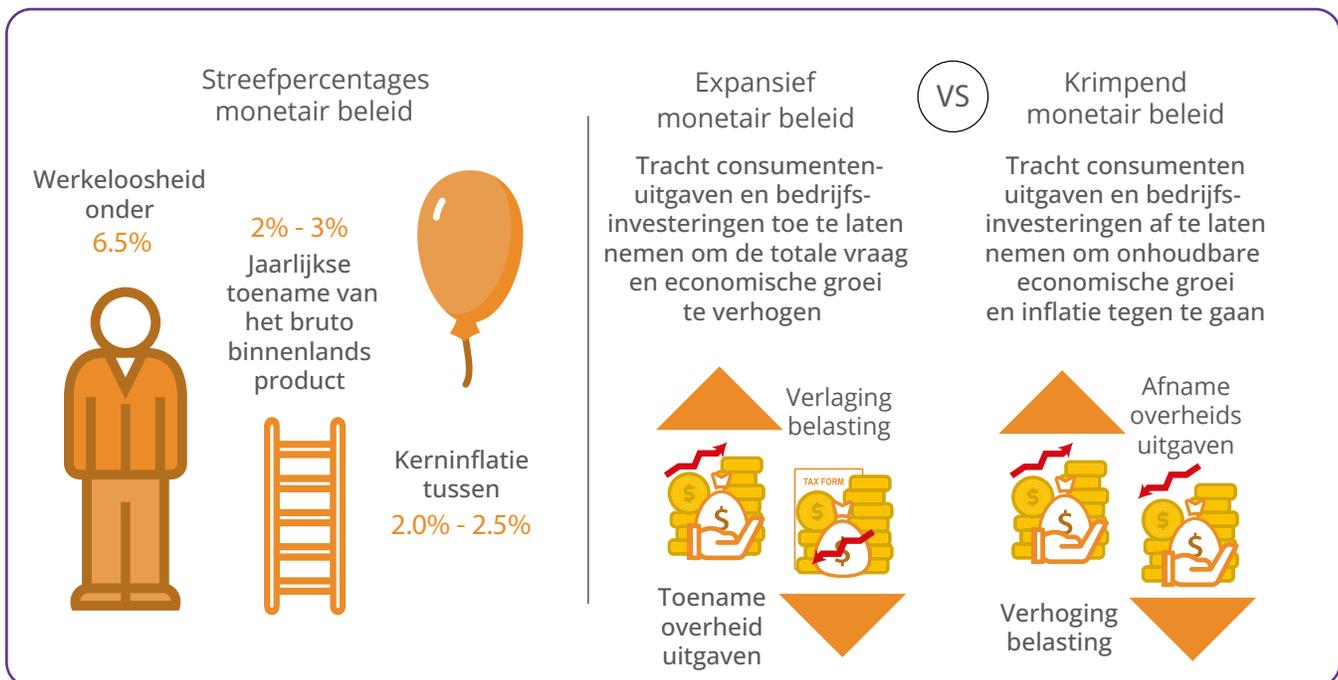
Centrale banken geven de economie in stilte vorm. Hun officiële taak is het waarborgen van stabiliteit en integriteit van het financiële systeem, maar hun methoden onthullen een mysterieuzere kant.

Centrale banken werken nauw samen met regeringen en trekken aan de touwtjes van het monetaire beleid door de geldhoeveelheid te manipuleren met behulp van instrumenten zoals rentetarieven. In tijden van crisis drukken ze geld uit het niets en injecteren het via commerciële banken in de economie, waardoor het voor een buitenstaander lijkt alsof er niets aan de hand is.

Ze houden niet alleen de boel in de gaten; centrale banken reguleren commerciële banken, bepalen de spelregels en springen bij als banken in de problemen komen (door als laatste redmiddel krediet te verstrekken). Dit web van controle lijkt beschermend, maar maakt de economie en de banken nog afhankelijker.

Om te begrijpen waar biljoenen dollars aan stimuleringsgeld vandaan komen en wie mag beslissen over de toewijzing ervan is het cruciaal om het bredere financiële systeem te begrijpen. Overheden gebruiken verschillende instrumenten om de geldhoeveelheid op specifieke momenten te manipuleren.

Centrale banken en overheden kunnen monetaire en fiscale beleidsinstrumenten gebruiken om de geldhoeveelheid en de economie te beïnvloeden. De Federal Reserve van de Verenigde Staten (The Fed) gebruikt monetair beleid bijvoorbeeld door de rentetarieven aan te passen, wat een effect heeft op de hoeveelheid geld dat in omloop is. Fiscaal beleid daarentegen gebruikt het uitgaven- en belastingbeleid om de economische activiteit te beïnvloeden.



Wat is fiatgeld en wie beheert het?

Wisselkoersbeleid, invoerbepalingen en prijscontroles dienen als extra instrumenten om de geldhoeveelheid te reguleren en hebben invloed op de handel en de economie. Hoewel dit beleid gericht is op het stabiliseren van prijzen en het beheersen van inflatie, leidt de interventie vaak tot de cycli van hoog- en laagconjunctuur, wat uitdagingen creëert voor iedereen die de valuta gebruikt.

Voorbeeld: "Te groot om failliet te gaan" verwijst naar financiële instellingen die zo groot en onderling verbonden zijn dat hun faillissement catastrofale gevolgen zou hebben voor het hele financiële systeem. Tijdens de financiële crisis van 2008 werden verschillende grote banken geacht "te groot te zijn om failliet te gaan", wat ertoe leidde dat de Amerikaanse overheid ingreep en financiële reddingsoperaties uitvoerde om hun ondergang te voorkomen.

Een van de meest prominente voorbeelden van een "too big to fail" instelling tijdens de financiële crisis was investeringsbank Lehman Brothers. Toen Lehman Brothers in september 2008 het faillissement aanvroeg, veroorzaakte dat een domino-effect van gebeurtenissen, waaronder de bijna ineenstorting van verzekeringsgigant AIG en een enorme daling van de aandelenmarkt. De Amerikaanse overheid moest ingrijpen en andere grote financiële instellingen een financiële injectie geven om verdere chaos te voorkomen en de economie in het algemeen te beschermen.

Het is essentieel om te begrijpen hoe dit beleid werkt om de beperkingen van gecentraliseerde fiatsystemen te begrijpen. Totdat je het probleem begrijpt, zul je de oplossing niet herkennen. Nu we hebben besproken hoe het fiatsysteem in het verleden en het heden heeft gewerkt, zullen we bespreken hoe de toekomst van fiat er op dit moment uitziet: digitaal centralebankgeld, ook wel CBDC's genoemd.

4.3 Digitaal centralebankgeld: de toekomst van fiatgeld

Digitaal centralebankgeld zoals de Digitale Euro worden ook wel CBDC's (Central Bank Digital Currencies) genoemd en zijn de volgende stap in de ontwikkeling van fiatvaluta. In tegenstelling tot de combinatie van fysieke biljetten, munten en digitale betalingen, zijn CBDC's volledig digitale vormen van fiatvaluta uitgegeven door overheden en beheerd door centrale banken.

Stel je het geld voor dat je elke dag gebruikt, maar dan zonder fysieke aanwezigheid - geen munten die rinkelen in je zak of biljetten die je moet vouwen en ontvouwen. CBDC's onderscheiden zich door het hogere niveau van controle en toezicht dat ze overheden en centrale banken bieden. Met CBDC's krijgen autoriteiten een ongekeerd zicht op financiële transacties, waardoor het makkelijker wordt om de geldstroom te volgen en te reguleren.

Overheden en centrale banken kunnen de vorm en het aanbod van CBDC's gemakkelijk aanpassen, rentetarieven manipuleren en monetaire en fiscale beleidsinstrumenten met grotere precisie inzetten. In wezen bieden CBDC's een efficiëntere manier voor overheden om hun fiatvaluta te beïnvloeden en te beheren.

Hoewel CBDC's mogelijk de toekomst van fiatgeld zijn, functioneert het huidige monetaire systeem van de wereld al op basis van een pure fiatstandaard. Fiatvaluta zijn niet langer gebonden aan goud, wat resulteert in een aanzienlijke uitbreiding van de geldhoeveelheid zonder enige echte beperking.

Nu je beter begrijpt hoe het fiatsysteem werkt, is het tijd om de gevolgen ervan te onderzoeken in Hoofdstuk 5.

Hoofdstuk #5

Hoe problemen tot oplossingen leiden

5.0 Introductie van het probleem

5.1 Afnemende koopkracht

5.1.1 Monetaire inflatie en het effect ervan op de koopkracht

Activiteit: de gevolgen van inflatie - een veilingactiviteit

5.2 De wereldwijde schuldenlast en sociale ongelijkheid

5.2.1 Gevolgen voor het individu - verlies van koopkracht

5.2.2 Impact op de samenleving - toenemende welvaartsongelijkheid

Activiteit: gevolgen van het fiatsysteem

5.2.3 De wereldwijde schuldenlast

5.3 De cypherpunks en de zoektocht naar gedecentraliseerd geld

5.3.1 De cypherpunks

5.3.2 Gecentraliseerde versus gedecentraliseerde systemen

5.3.3 Korte geschiedenis van digitale valuta

Hoe problemen tot oplossingen leiden

5.0 Introductie van het probleem

Wie de hoeveelheid geld in ons land beheerst, heeft de macht over alle industrie en handel. Als je begrijpt dat dit systeem gemakkelijk in handen kan komen van een paar machtige mannen, begrijp je ook hoe periodes van inflatie en depressie ontstaan.

James A. Garfield, President van de V.S.

In hoofdstuk 4 heb je geleerd dat de financiële wereld steunt op een systeem dat misschien niet zo sterk is als het lijkt. In het fiatsysteem, overeind gehouden door constante toevoegingen van papiergeld, lijken sommigen meer te profiteren dan anderen. Dit hoofdstuk bespreekt wat het fiatsysteem betekent voor gewone mensen en de samenleving in het algemeen. Tot slot verkennen we het verhaal van een groep mensen die de problemen opmerkten en in stilte werkten aan een oplossing die de toekomst van de menselijke samenleving kan veranderen.

5.1 Afnemende koopkracht

5.1.1 Monetaire inflatie en het effect ervan op de koopkracht

Monetaire inflatie is de toename van de geldvoorraad binnen een economie, wat een direct effect heeft op de gemiddelde mens doordat hun koopkracht afneemt. De cyclus van prijsinflatie begint wanneer er meer geld in omloop komt. Dit stimuleert op zijn beurt de vraag naar goederen en diensten, waardoor de prijzen uiteindelijk stijgen.

Stel je een kleine groep vrienden voor - Alex, Bob en Charlie - met elk een euro in de hand en er zijn drie flessen water te koop. De Ausgangssituatie is eenvoudig: drie mensen met in totaal drie euro en drie flessen water. Stel nu dat de lokale overheid besluit om Alex drie euro extra te geven omdat hij bevriend is met iemand in de regering. Nu hebben ze samen zes euro, maar Alex heeft voordeel door zijn nauwe banden met de bron van het geld. Hij heeft vier euro terwijl Bob en Charlie er maar één hebben.

Omdat alle drie de vrienden dorst hebben, beginnen ze tegen elkaar op te bieden voor de flessen water. Met zijn nieuwe geld besluit Alex gelijk twee flessen water te kopen voor twee euro per stuk. Bob en Charlie kunnen elk nu nog slechts een halve fles water kopen met de euro die ze hebben. De prijs van een fles water is dus toegenomen door de grotere hoeveelheid geld in de economie.

Bob en Charlie ervoeren een afname van hun koopkracht doordat Alex toegang heeft tot nieuw gecreëerd geld, en zij niet. Dit fenomeen komt voor in alle economieën met fiatgeld en staat bekend als het Cantillon-effect.

Het Cantillon-effect beschrijft de ongelijke verdeling van nieuw geld dat wordt geïntroduceerd in een economie. Het gaat eerst naar degenen die het dichtst bij de bron staan, zoals banken en andere delen van de financiële sector. Deze partijen genieten voordelen van de geldcreatie omdat zij het geld kunnen uitgeven voordat het een effect heeft op de consumentenprijzen. Hoe verder van de bron, hoe groter de nadelen.



Dit voorbeeld illustreert hoe Bob en Charlie's koopkracht werd beïnvloed door factoren buiten hun macht, wat het belang aantoont van begrip en bevraging van de systemen die de waarde van ons geld beïnvloeden.

Laten we nu ontdekken hoe dit in zijn werk gaat in het echte leven.

Activiteit: de gevolgen van inflatie - een veilingactiviteit

Doel: begrijpen wat inflatie is en hoe het de prijzen van goederen en diensten in een economie beïnvloedt.

Definities:

 De geldhoeveelheid: de totale hoeveelheid geld die op een bepaald moment in omloop is in een economie. Dit omvat:

- Fysiek geld, zoals munten en biljetten
- Spaarrekeningen
- Geldmarktrekeningen
- Kleine termijndeposito's zoals Depositocertificaten onder €100.000

 Veiling: een openbare verkoop aan de hoogste bidder van goederen of andere eigendommen

Oefening in de klas. Volg de onderstaande instructies:

1. Elke student ontvangt een willekeurig bedrag aan monopolygeld van de docent. Dit vertegenwoordigt de geldvoorraad in een samenleving.
2. Schrijf de totale geldhoeveelheid op in de bijgeleverde grafiek.
3. De docent veilt een reep snoep onder de studenten. Om de reep te winnen moet je het hoogste bod uitbrengen met je monopolygeld. Noteer het winnende bod naast de geldvoorraad.
4. De docent voegt dan een aanzienlijke hoeveelheid monopolygeld toe aan de totale geldhoeveelheid. Dit vertegenwoordigt een toename van de geldhoeveelheid in een economie. Later zul je leren hoe de geldhoeveelheid in een economie toeneemt of afneemt.

Samenlevingen kunnen vaak onvoorspelbaar en onrechtvaardig zijn, wat wordt geïllustreerd in de simulatie waarbij de docent een aanzienlijk bedrag aan slechts een paar leerlingen geeft. Dit bootst echte situaties na waarin een ongelijke verdeling van middelen en kansen kan voorkomen en benadrukt de inherente willekeur en oneerlijkheid in veel situaties.

5. De docent veilt een tweede reep aan de leerlingen volgens hetzelfde proces als eerder. Noteer het winnende bod naast de geldvoorraad op de kaart.
6. De docent herhaalt de veiling een derde keer.



Hoe problemen tot oplossingen leiden

Ronde	Geldhoeveelheid	Winnende bod
1		
2		
3		

Conclusie:

1. Hoe beïnvloedde de toename van de geldhoeveelheid de winnende biedingen?
2. Wat is de relatie tussen het verhogen van de geldhoeveelheid en inflatie?
3. Welke rol speelt de geldhoeveelheid in de echte wereld?
4. Als er nieuw geld in de economie wordt geïnjecteerd, wat denk je dat er dan gebeurt met de prijzen van goederen en diensten? Denk je dat de prijsveranderingen tijdelijk of permanent zijn, en waarom? Op welke manier denk je dat de prijsveranderingen op de lange termijn invloed zullen hebben op de burgers in een samenleving?

5.2 De wereldwijde schuldenlast en sociale ongelijkheid

5.2.1 Gevolgen voor het individu - verlies van koopkracht

Jamie is een student die in een klein appartement woont. Hij werkt parttime in een café om zijn levensonderhoud en collegegeld te betalen. Zodra hij zelfstandig begon te wonen, werd Jamie goed in het beheren van zijn eigen kasboek.



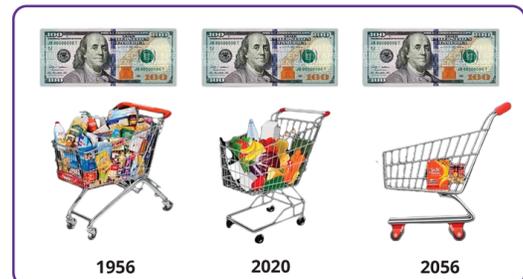
Een kasboek is een gedetailleerde registratie van al je monetaire transacties. Of je nu geld verdient of uitgeeft, een kasboek helpt je om alles bij te houden.

Aan het begin van 2023 begrootte hij €10.000 voor zijn levensonderhoud voor het hele jaar, inclusief huur, eten en andere benodigdheden. Dit waren zijn transacties voor januari 2023:

Datum	Omschrijving	Bedrag	Type	Balans
01-01-2023	Startbalans			€1.600
01-01-2023	Huur voor januari	€800	Debet	€800
05-01-2023	Boodschappen	€100	Debet	€700
15-01-2023	Parttime salaris	€500	Krediet	€1.200
20-01-2023	Benzine voor auto	€350	Debet	€850
30-01-2023	Studieboeken	€150	Debet	€700

Dit kasboek laat zien dat Jamie's beginsaldo €1.600 was, waarvan hij €800 **uitgaf** (een **debet**) om de huur te betalen. Daarna gaf hij €100 uit aan boodschappen en **ontving** hij €500 (een **Krediet**) als salaris voor zijn parttime baan, wat zijn saldo op €1200 bracht. Daarna gaf hij geld uit aan benzine en studieboeken, waardoor zijn saldo aan het einde van de maand €700 bedroeg.

Twaalf maanden later luncht Jamie met zijn opa met wie hij de details van zijn budget voor 2024 deelt. Jamie merkt dat zijn budget niet meer zo ver reikt als vroeger en dat zijn kosten voor levensonderhoud het afgelopen jaar aanzienlijk zijn gestegen. Terwijl Jamie zich afvraagt hoe dit kan, laat zijn opa hem de volgende afbeelding zien. Jamie kan zijn ogen niet geloven.

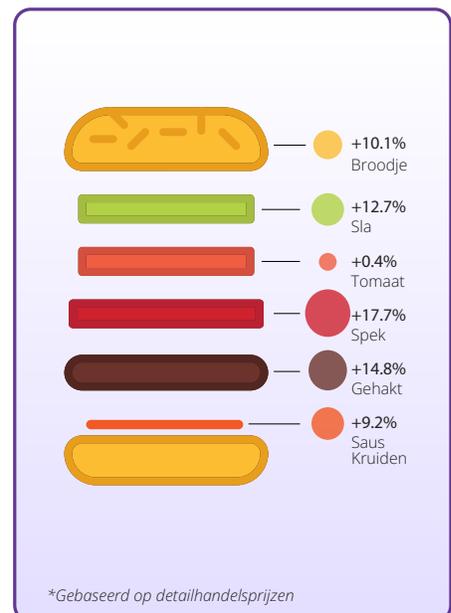


Dit is het moment waarop hij ontdekt dat de kosten van goederen en diensten na verloop van tijd drastisch stijgen, waardoor zijn koopkracht afneemt.

Zijn opa vertelt: "In 1956 was ik nog maar een jongeman die zijn eerste stappen in de wereld zette. Ik herinner me dat ik €380 per maand verdiende als fabrieksarbeider. Dat lijkt misschien niet veel, maar het was een behoorlijk loon in die tijd. Ik kon zelfs genoeg geld sparen om een huis te kopen."

Zijn opa vervolgt: "De kosten van dingen waren in de vorige eeuw heel anders. In 2020 zou de aankoop van 30 repen Hershey's chocolade je bijvoorbeeld €26,14 kosten. Als we echter teruggaan in de tijd naar 1913, zouden deze Hershey's chocoladerepen je slechts €1,00 kosten."

Dit aanzienlijke prijsverschil benadrukt de verandering in koopkracht in de loop der tijd en laat het effect van inflatie zien.



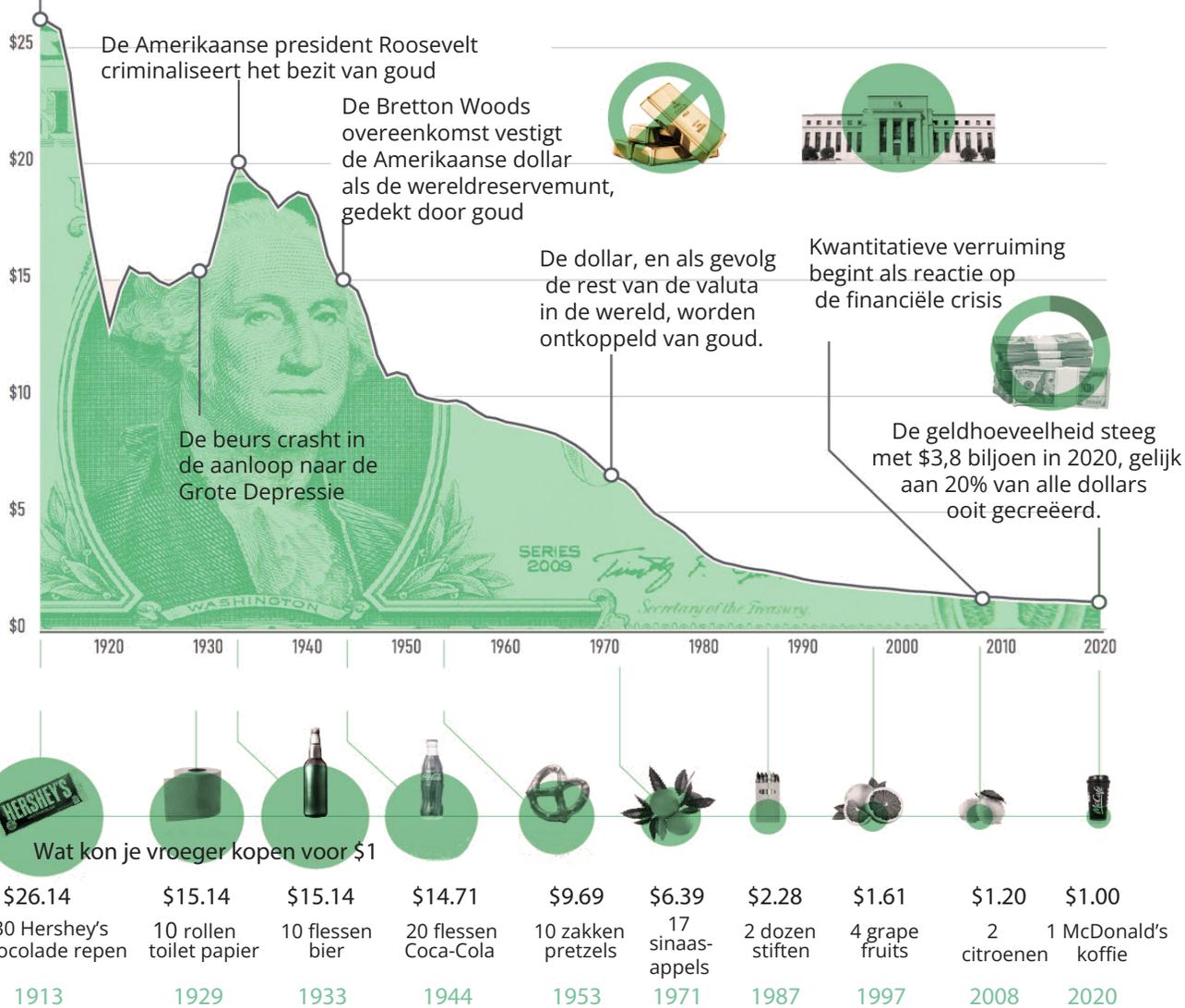
Hoe problemen tot oplossingen leiden



De koopkracht van de U.S. Dollar

De koopkracht van de Amerikaanse dollar is de afgelopen eeuw sterk gedaald door de toegenomen geldhoeveelheid.

De Federal Reserve Act creëerde een centrale bank die de geldhoeveelheid van het land kan beheren.



Jamie: "Wat? Dat is te gek voor woorden. Ik kan me niet voorstellen hoe laag mijn huur toen zou zijn geweest vergeleken met nu."

Opa: "Nou, ja, je huur zou toen veel goedkoper zijn geweest. Ik heb nog een voorbeeld om dit te illustreren: toen kon je voor \$1,00 ongeveer 10 zakken pretzels kopen. In 2020 betaalde ik \$9,69 voor dezelfde hoeveelheid. Stel je eens voor hoeveel 10 zakken pretzels vandaag de dag zouden kosten."

Jamie: "Wow, dat is echt interessant, opa. Hoe heb je dit zelf ervaren toen je jonger was?"

Opa: "Oh Jamie, alle dingen waren gewoon veel goedkoper toen ik jong was. Een brood kostte maar \$0,18 en je kon een liter benzine kopen voor maar \$0,29. Het is ongelooflijk hoeveel de kosten van levensonderhoud zijn gestegen."

Na het gesprek met zijn grootvader ging Jamie naar huis om nog eens naar zijn kasboek te kijken. Hij ontdekte al snel dat hij voor 2024 €1.000 extra moet begroten om hetzelfde mandje goederen en diensten te kunnen kopen als in het voorgaande jaar. Dit betekent dat zijn koopkracht met €1.000 is afgenomen, omdat hij nu meer geld moet uitgeven om dezelfde goederen en diensten te kopen. Terwijl Jamie's salaris slechts licht stijgt, rijzen zijn kosten voor levensonderhoud elk jaar de pan uit.

De volgende tabel toont de kosten van Jamie in het eerste jaar en het tweede jaar, evenals de procentuele prijsstijging:

Om te overleven, zal Jamie meer uren per week moeten werken om €1.000 extra te krijgen om met dezelfde levensstandaard te kunnen leven.

Gebaseerd op informatie van het Amerikaanse Bureau of Labor Statistics zijn de prijzen vandaag de dag ongeveer 30 keer zo hoog als in 1913. Dit betekent dat je met een dollar vandaag de dag slechts 3% kunt kopen van wat je er toen mee kon kopen.

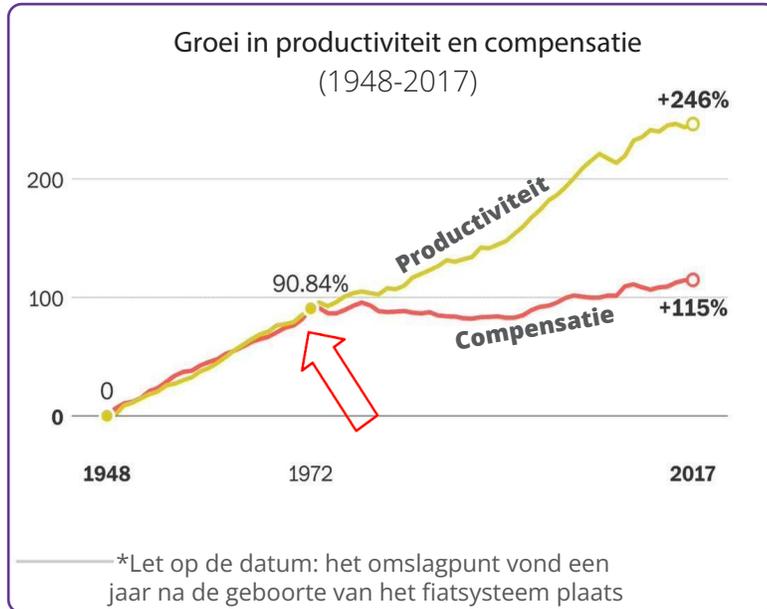
Item	Kosten Jaar #1	Kosten Jaar #2	% Toename
Huur	€4.000	€4.500	12.5%
Boodschappen	€2.000	€2.300	15%
Benodigdheden	€4.000	€4.200	5%
Total	€10.000	€11.000	10%

Ter illustratie: als Jamie in de tijd zou kunnen reizen, in welke tijd zou hij dan het beste €100 kunnen spenderen? In 1913 zou hij uitgebreid kunnen winkelen, terwijl hij in 2023 slechts enkele kleine transacties zou kunnen doen, wat vergelijkbaar zou zijn met maar €3 in 1913. Dit significante verschil in waarde laat zien hoeveel de koopkracht van geld in de loop der jaren is afgenomen.

1938 COST OF LIVING	
<u>LIVING</u>	
New House	\$3,900.00
Average Income	\$1,731.00 per year
New Car	\$860.00
Average Rent	\$27.00 per month
Tuition to Harvard University	\$420.00 per year
Movie Ticket	25¢ each
Gasoline	10¢ per gallon
United States Postage Stamp	3¢ each
<u>FOOD</u>	
Granulated Sugar	59¢ for 10 pounds
Vitamin D Milk	50¢ per gallon
Ground Coffee	39¢ per pound
Bacon	32¢ per pound
Eggs	18¢ per dozen

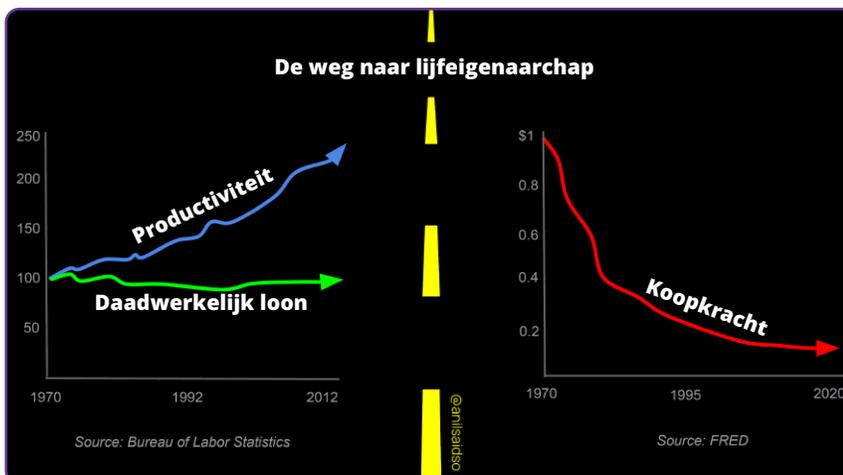
Hoe problemen tot oplossingen leiden

Als we in getallen denken, verdient Jamie veel meer dollars of euro's in een jaar dan zijn grootvader ooit deed, maar met de dollars of euro's die Jamie's grootvader bezat, kon er veel meer gekocht worden.



In de wereld van vandaag worden mensen door de grote invloed van inflatie ontmoedigd om geld te sparen. In plaats daarvan kiezen de meesten ervoor om hun geld meteen uit te geven omdat de waarde ervan snel daalt. Deze pessimistische kijk belemmert hun vermogen om plannen te maken voor de toekomst. Zoals te zien is in de grafiek, stagneert de salarisgroei van de gemiddelde persoon wanneer deze wordt gecorrigeerd voor inflatie, wat betekent dat hun loon niet toeneemt in hetzelfde tempo als de dalende waarde van hun geld, ondanks dat ze productiever werken.

Jamie's voorbeeld is er slechts één van velen. In de fiatwereld is het heel gewoon dat regeringen geld uit het niets creëren om hun eigen agenda voort te zetten, en mensen wereldwijd voor de gevolgen te laten opdraaien. De prijzen van alledaagse dingen, van brood tot huizen, van boodschappen tot vakanties, stijgen elk jaar. Terwijl de rijken profiteren van de inflatie omdat ze schaarse bezittingen hebben, zien gewone mensen hun zuurverdiende geld in koopkracht dalen. Het resultaat? Mensen en gezinnen over de hele wereld hebben het moeilijk door de daling van hun koopkracht.



Mensen wereldwijd hebben meer banen en maken meer uren, alleen maar om dezelfde levensstandaard te behouden. Het is alsof je op een loopband staat die steeds sneller gaat maar je nooit echt vooruit brengt. Het fiatsysteem geeft mensen het gevoel dat ze in een eeuwigdurende race zitten tegen stijgende prijzen.

Velen wenden zich tot schulden in hun strijd om gelijke tred te houden met de stijgende kosten, vergelijkbaar met het gebruik van een te kleine pleister op een hele diepe wond. Mensen gaan leningen aan of nemen impulsieve beslissingen om maar rond te kunnen komen. Snel geld wordt een noodzaak en mensen komen terecht in een cyclus waarin overleven vandaag belangrijker is dan plannen voor morgen.

Het fiatsysteem, met het constant drukken van geld, beïnvloedt de psychologie van de mensheid. Het brengt een bepaalde tijdsvoorkeur met zich mee - een focus op kortetermijnwinsten boven langetermijnplanning. Mensen in de fiatwereld hebben de neiging om prioriteit te geven aan kortetermijnvoordelen. Het is een overlevingsinstinct dat een cyclus van afhankelijkheid creëert waarin mensen elk middel zoeken om snel geld te verkrijgen, zelfs als dat op de lange termijn niet duurzaam of werkbaar is.

In wezen schetst de impact van het fiatsysteem een uitdagend beeld voor mensen wereldwijd. In het fiatsysteem stijgen de prijzen, stagneren inkomens en ontstaat er een strijd om te overleven. Terwijl bepaalde groepen rijker worden, blijven de meeste mensen wereldwijd afhankelijk van een systeem dat hen steeds armer maakt.

5.2.2 Impact op de samenleving - toenemende welvaartsongelijkheid

In een samenleving die gebaseerd is op eerlijk geld, is de financiële besluitvorming van een regering gebonden aan de goedkeuring van het volk. In het fiatsysteem kunnen overheden zich echter ongelimiteerd in de schulden steken, over de ruggen van hun burgers.

De macht om naar believen geld bij te drukken leidt vaak tot politieke centralisatie. Het fiatsysteem stelt regeringen in staat om enorme schulden op te bouwen en beslissingen te nemen die hen zelf ten goede komen in plaats van de meerderheid. Grootmachten, zoals de Verenigde Staten, krijgen door dit fenomeen een concurrentievoordeel. Ze kunnen eindeloos geld drukken om hun plannen te financieren, waaronder oorlogen. Dit vermogen stelt deze dominante naties in staat om macht en invloed uit te oefenen, en geopolitieke conflicten aan te gaan, waardoor een wereldwijde machtsongelijkheid ontstaat. Oorlogen en grote acties om controle over anderen te houden worden financieel haalbaar voor supermachten, terwijl anderen zonder dezelfde financiële flexibiliteit te maken krijgen met beperkingen.

Onder het fiatsysteem verdeelt rijkdom zich niet gelijkmatig. In plaats daarvan concentreert het zich in de handen van een selecte groep. Dit fenomeen lijkt op het spelen van een spelletje Monopoly waarbij een handjevol spelers bijna alle hotels en eigendommen bezit, terwijl de meerderheid worstelt om het hoofd boven water te houden. Het fiatsysteem is een instrument geworden voor bepaalde groepen om rijkdom te concentreren. Door de nauwe samenwerking met centrale banken kunnen regeringen met centrale banken meer geld in de economie injecteren, waarbij de ontvangers van dit nieuw gecreëerde geld degenen zijn met reeds bestaande rijkdom en status: machtige entiteiten en individuen. Deze groepen profiteren van het vers gedrukte geld voordat de negatieve effecten, zoals een afname van de koopkracht, zich in de economie manifesteren.

Hoe problemen tot oplossingen leiden

Ongelijkheid in rijkdom gaat niet alleen over de “haves” en de “have-nots”; het gaat over het onderdrukken van economische mobiliteit. Degenen met een minder bevoorrechte achtergrond vinden het steeds moeilijker om de economische ladder te beklimmen, vergelijkbaar met het starten van een race met een zware rugzak. De groeiende kloof tussen arm en rijk veroorzaakt problemen voor iedereen, waarbij de rijken het beleid in hun voordeel vormgeven. Dit maakt het moeilijker voor gewone mensen, wat leidt tot sociale onrust, een gebrek aan vertrouwen in instellingen en gemeenschappen die uit elkaar vallen, vergelijkbaar met een kaartenhuis. De instabiliteit van het fiatsysteem uit zich in economische onzekerheid, politieke onrust en wereldwijde gevolgen wanneer de westerse wereld te maken krijgt met een economische neergang.



Dit is een wereldwijd fenomeen dat zowel ontwikkelde landen als ontwikkelingslanden treft. De rijken, die vaak op transnationale schaal opereren, gebruiken het wereldwijde financiële systeem in hun voordeel, waardoor de kloof tussen arm en rijk nog groter wordt. Onder het fiatsysteem is schuld opbouwen voor de mensheid de norm geworden. Overheden, instellingen, bedrijven en mensen over de hele wereld worden ondergedompeld in een zee van schulden. De psychologische verschuiving om schulden als acceptabel te beschouwen, heeft zijn wortels in het ontwerp van het fiatsysteem. In de afgelopen decennia werd het steeds makkelijker om grote schulden aan te gaan en voor gewone mensen wordt het vaak een noodzaak vanwege de stijgende prijzen en kosten van levensonderhoud. Koopzucht, een constante drang om te kopen en te consumeren, leidt ertoe dat mensen meer kopen dan ze nodig hebben, wat resulteert in overconsumptie en verspilling. Hoewel het misschien lijkt alsof je eindeloos aan het winkelen bent, gaan de echte kosten verder dan het prijskaartje en hebben ze invloed op de psychologie en het welzijn van mensen.

Het wordt duidelijk dat het fiatsysteem niet slechts een economisch mechanisme is. Het is eerder een systeem dat de menselijke samenleving als geheel vormgeeft: het vormt de concentratie van macht, verschillen in rijkdom en maatschappelijke normen. Het fiatsysteem raakt iedereen, van hele naties tot de individuele burger.

Activiteit: gevolgen van het fiatsysteem

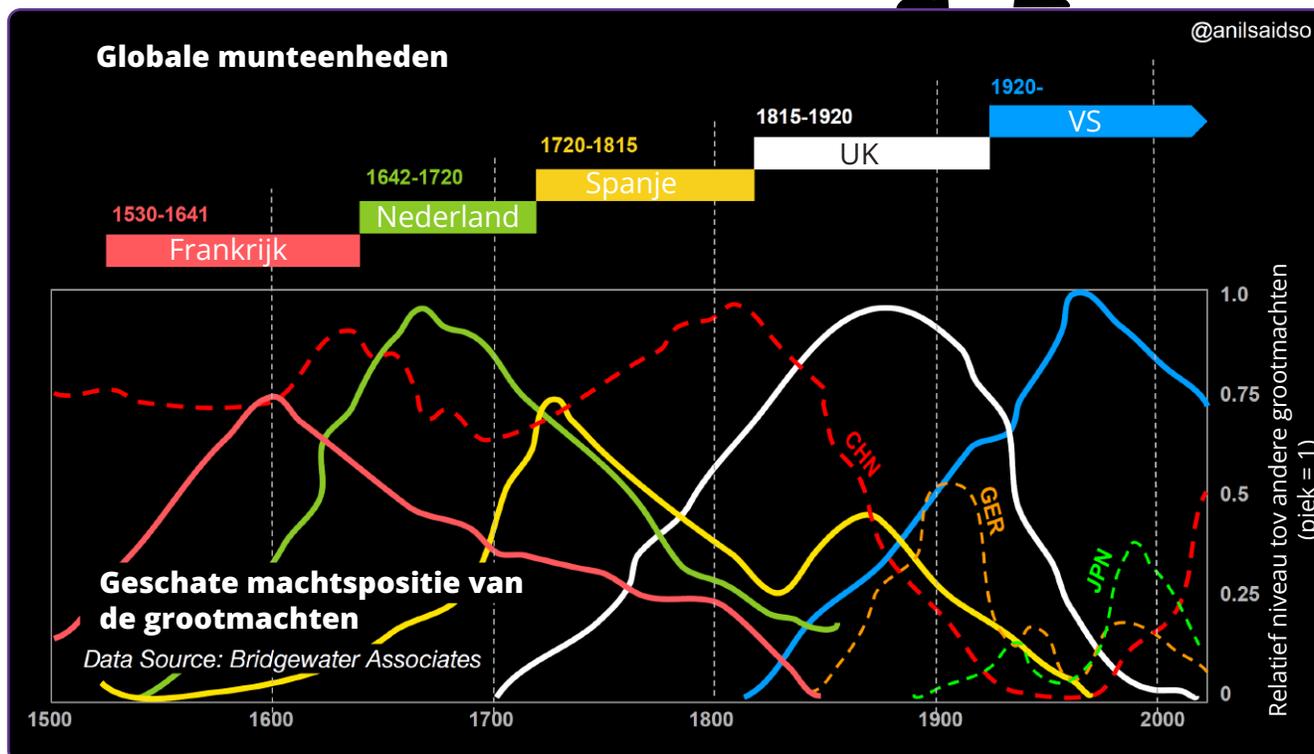
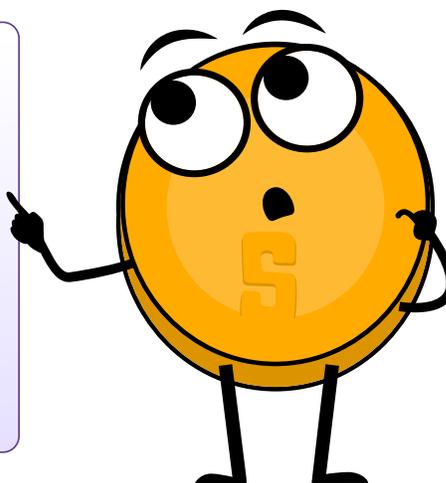
1. Zijn er nog andere gevolgen die mensen en een samenleving als geheel ervaren als gevolg van het fiatsysteem?
2. Wat zijn de gevolgen van het fiatsysteem in jouw land? Wat is er in de loop van de geschiedenis gebeurd en hoe heeft dat de mensen in jouw land beïnvloed?
 - a. Deel persoonlijke voorbeelden in een interactieve sessie

Hoe problemen tot oplossingen leiden



"Ik geloof niet dat we ooit nog eerlijk geld zullen hebben totdat we het uit handen van de overheid nemen... het enige wat we kunnen doen, is op een slinkse, omslachtige manier iets introduceren dat zij niet kunnen stoppen..."

Friedrich Hayek
Nobelprijswinnaar voor economie



5.3 De cypherpunks en de zoektocht naar gedecentraliseerd geld

Door de geschiedenis heen zagen we een geleidelijke overname van geld door banken en overheden, wat leidde tot het fiatstelsel dat we nu kennen en de desastreuze gevolgen daarvan voor de samenleving. Maar door de opkomst van nieuwe technologieën zoals encryptie en internet konden nieuwe ideeën ontstaan, zoals onafhankelijk digitaal geld, vrij van overheidsinterventie, open en toegankelijk voor iedereen. Laten we eens duiken in de geschiedenis van degenen die deze revolutionaire beweging leiden: de cypherpunks.

5.3.1 De cypherpunks



De computer kan worden gebruikt als hulpmiddel om mensen te bevrijden en te beschermen in plaats van ze te controleren

Hal Finney



De tweede helft van de 20e eeuw zag de opkomst van verschillende technologische doorbraken zoals de computer en het internet, die de weg vrijmaakten voor een nieuw digitaal tijdperk.

Een groep mensen ontdekte dat deze enorme innovaties het functioneren van de maatschappij snel zouden veranderen. Ze voorzagen zowel het potentieel als het gevaar van de personal computer, hetzij als een instrument dat vrijheid mogelijk maakt en het individu versterkt, hetzij als een instrument voor volledige controle en bewaking.

Deze mensen werden de cypherpunks genoemd. Ze ontstonden als een losjes verbonden groep activisten, cryptografen, programmeurs en privacyactivisten die een gemeenschappelijke visie deelden: het streven naar privacy, veiligheid en een gedecentraliseerde digitale toekomst. De term "cypherpunk" is een samenvoeging van "cypher", dat verwijst naar cryptografische code, en "punk", dat staat voor het tegenculturele ethos van rebellie.

De cypherpunks geloofden in de kracht van cryptografie om individuele vrijheden te beschermen. Hun doelen waren onder andere het ontwikkelen van tools om online communicatie te beveiligen, internetactiviteiten te anonimiseren en digitale valuta te gebruiken om buiten de controle van gecentraliseerde autoriteiten te opereren.

De cypherpunks begrepen de gevolgen van het fiatstelsel en zagen de dreiging van een "Orwelliaanse toekomst". Ze geloofden dat ze ervoor moesten zorgen dat de personal computer en het internet een goede zaak voor de mensheid zouden worden, in plaats van een hulpmiddel voor de staat om mensen te controleren.

De definitie van een Orwelliaanse toekomst:

Een Orwelliaanse toekomst verwijst naar een dystopische visie geïnspireerd door de werken van George Orwell. De term wordt geassocieerd met een nachtmerrieachtige en totalitaire samenleving die wordt gekenmerkt door onderdrukkende overheidscontrole, uitgebreide bewaking, propaganda en de manipulatie van informatie. De term "Orwelliaans" beschrijft vaak een scenario waarin de vrijheden en individuele autonomie van burgers ernstig worden beperkt, afwijkende meningen worden onderdrukt en de werkelijkheid wordt vervoemd om de belangen van een machtig en autoritair regime te dienen. Het begrip is vernoemd naar George Orwell, die in zijn geschriften waarschuwde voor de potentiële gevaren van ongecontroleerde overheidsmacht en de uitholling van fundamentele mensenrechten.



Hoe problemen tot oplossingen leiden

Eric Hughes, Timothy C. May en John Gilmore waren sleutelfiguren binnen de cypherpunk beweging. In 1992 schreef Eric Hughes "A cypherpunk manifesto", waarin hij de principes van de groep uiteenzette. Het manifest benadrukte het belang van privacy, encryptie en de noodzaak voor mensen om controle te krijgen over hun digitale identiteiten.



Bekijk deze video en ontdek het verhaal van de cypherpunks!

Een van de meest opmerkelijke uitvindingen van de cypherpunks was het maken van cryptografische gereedschappen en protocollen. In 1991 introduceerde Phil Zimmermann PGP (Pretty Good Privacy), email-encryptie-software die een vlaggenschip project werd. PGP stelde gebruikers in staat om versleutelde berichten over het internet te versturen zonder dat iemand anders dan de beoogde ontvanger ze kon ontsleutelen. Vóór deze ontwikkelingen kon elk internet bericht worden onderschept en gelezen door anderen, waaronder overheden.

De cypherpunks geloofden dat de doorbraak van encryptie, samen met het internet en de computer, een solide basis vormde voor het creëren van gedecentraliseerde netwerken in de digitale ruimte, waardoor mensen privé en zonder tussenkomst van een centrale autoriteit op het internet konden communiceren en transacties konden doen.

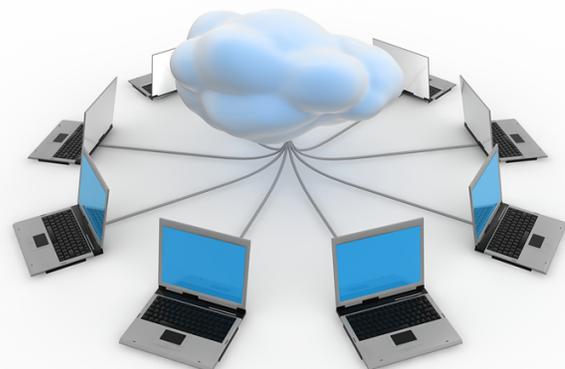
De cypherpunks waren op de goede weg naar een betere toekomst voor de mensheid, waarin technologie een hulpmiddel is om vrijheid te maximaliseren in plaats van een middel om controle uit te oefenen. Het enige wat nog ontbrak was een gedecentraliseerd netwerk en gedecentraliseerd geld.

5.3.2 Gecentraliseerde versus gedecentraliseerde systemen

Gecentraliseerde systemen: één heerser, veel problemen

In een gecentraliseerd systeem is alles om één hoofdautoriteit opgebouwd, zoals een wolkenkrabber in een stad, omringd door lage gebouwen. Deze autoriteit bepaalt hoe het systeem werkt. Denk bijvoorbeeld aan traditionele banken, waarbij een kleine groep alle beslissingen neemt.

 Voorbeeld uit de echte wereld: In 2022, tijdens vreedzame protesten in Canada, bevroren banken de rekeningen van demonstranten, waarmee ze lieten zien hoe de centrale autoriteit kon ingrijpen en controle heeft over de toegang tot financiële diensten.



Problemen met gecentraliseerde systemen:

- ☀ Centraal punt van falen: als er iets misgaat met de centrale autoriteit, kan het hele systeem instorten.
- ☀ Controle: een kleine groep aan de top heeft alle controle en macht en neemt vaak beslissingen die hen meer ten goede komen dan alle anderen.
- ☀ Inefficiëntie en tussenpersonen: net als verkeersopstoppingen in een stad kunnen gecentraliseerde systemen traag en duur worden door onnodige tussenpersonen en bureaucratie.
- ☀ Gebrek aan autonomie: mensen kunnen misschien niet hun eigen financiële keuzes maken; alles wordt bepaald door de hoogste autoriteit.
- ☀ Censuur en beperkingen: net zoals sommige delen van een stad kunnen worden geblokkeerd, kunnen gecentraliseerde systemen de toegang tot bepaalde financiële middelen blokkeren of beperken.
- ☀ Uitdagingen bij schaalvergroting: als meer mensen financiële diensten nodig hebben, kunnen gecentraliseerde systemen moeite hebben om het bij te benen.
- ☀ Veiligheidsrisico's: problemen met de centrale autoriteit kunnen het hele systeem in gevaar brengen in het geval van cyberaanvallen.
- ☀ Gebrek aan transparantie en vertrouwen: de interne werking van gecentraliseerde systemen kan intransparant zijn, waardoor mensen ze moeilijk kunnen vertrouwen.

Gedecentraliseerde systemen: mensen aan de macht

Zie een gedecentraliseerd systeem als een groot bos. Elke boom vertegenwoordigt een apart onderdeel van het geheel. In tegenstelling tot een stad met één centraal punt, is een gedecentraliseerd systeem meer zoals een veerkrachtig bos dat kan blijven gedijen, zelfs als één onderdeel problemen ondervindt.

- ☀ Voorbeeld uit de echte wereld: het tor netwerk en de tor browser creëren een gedecentraliseerd systeem waarbij mensen anoniem gebruik kunnen maken van het internet. Het tor netwerk is moeilijk te stoppen of te censureren.



Voordelen van gedecentraliseerde systemen:

- ☀ Verbeterde veerkracht en betrouwbaarheid: er is geen enkelvoudig punt van falen waardoor het systeem sterk is, zelfs als er problemen zijn.
- ☀ Verhoogde veiligheid: met de juiste encryptie/bescherming is een gedecentraliseerd systeem beter bestand tegen controle door een enkele autoriteit.

Hoe problemen tot oplossingen leiden

- ☀ Grotere soevereiniteit: mensen krijgen meer controle over hun geld, gegevens en beslissingen.
- ☀ Verbeterde transparantie: iedereen ziet dezelfde informatie, wat het systeem betrouwbaarder maakt.
- ☀ Toestemmingsvrij en grenzenloos: iedereen kan meedoen, waardoor het een inclusief systeem is.
- ☀ Gelijke kansen: iedereen heeft een eerlijke kans om bij te dragen en inspraak te hebben.
- ☀ Verbeterde privacy: gegevens worden verdeeld over meerdere deelnemers en zijn meestal pseudoniem, waardoor gedecentraliseerde systemen meer privacy bieden.

Hoewel gedecentraliseerde systemen veel voordelen hebben, kan het samen nemen van beslissingen een beetje lastig zijn. Het vereist dat iedereen samenwerkt.

Verschuiving van macht

In de wereld van gecentraliseerde en gedecentraliseerde systemen gaat het erom wie de macht heeft. Gecentraliseerde systemen geven macht aan een kleine groep, terwijl gedecentraliseerde systemen de macht verspreiden en iedereen inspraak geven. Deze verschuiving in macht betekent een eerlijkere en meer democratische financiële toekomst, waarin meer mensen invloed hebben op het systeem dat hun leven vormgeeft.

5.3.3 Korte geschiedenis van digitale valuta

Een van de belangrijkste concepten die de cypherpunks bespraken was digitaal geld. De cypherpunks realiseerden zich dat staat en geld gescheiden moesten worden om er zeker van te zijn dat de toekomst het algemeen belang ten goede zou komen. Het baanbrekende werk van David Chaum met betrekking tot cryptografische protocollen voor veilige en private transacties legde de basis. Het nadeel was dat dit protocol een centrale autoriteit nodig had om efficiënt te functioneren, wat zorgen opriep over een centraal punt van falen en mogelijke censuur.

In de jaren die volgden, probeerden meerdere cypherpunks elkaars ideeën te verbeteren om tot een werkbare oplossing te komen voor een digitale munt die vrij was van overheidscontrole. De tabel hieronder beschrijft een aantal belangrijke innovaties die de cypherpunks ontwikkelden in hun zoektocht naar digitaal geld:

Naam en datum	Beschrijving	Beperkingen
E-Cash (1982)	E-Cash van David Chaum was een vroeg concept van elektronisch geld, gericht op privacy door middel van cryptografische technieken.	Vereiste een centrale autoriteit, wat zorgen opriep over een enkelvoudig punt van falen en mogelijke censuur.
DigiCash (1990)	DigiCash, opgericht door David Chaum, wilde een digitale vorm van valuta creëren met de nadruk op privacy.	Het gecentraliseerde model droeg bij aan het uiteindelijke faillissement in 1998.

B-Money (1996)	B-Money, voorgesteld door Wei Dai, was een theoretisch voorstel voor een anoniem, gedistribueerd elektronisch geldsysteem.	Nooit geïmplementeerd, bleef een conceptueel idee. Ontbrak een praktische uitvoering.
HashCash (1998)	HashCash, ontwikkeld door Adam Back, was een proof-of-work systeem ontworpen om e-mailspam en denial-of-service aanvallen te beperken.	Adresseerde niet het probleem van dubbele uitgaven bij digitale valuta.
Bit Gold (1998)	Bit Gold, voorgesteld door Nick Szabo, beschreef een gedecentraliseerd systeem voor digitale valuta met elementen van proof-of-work.	Nooit geïmplementeerd, bleef een theoretisch concept.
e-Gold (2004)	e-Gold was een gecentraliseerde digitale valuta gedekt door fysiek goud, waarmee gebruikers e-Gold eenheden konden kopen en overdragen.	Juridische problemen leidden tot de sluiting in 2009 en benadrukten de uitdagingen van gecentraliseerde digitale valuta.

Ondanks de vele pogingen die cypherpunks in de loop van tientallen jaren hebben ondernomen om een digitale valuta te creëren die vrij is van de controle van een groep of overheid, stuitte hun inspanningen op praktische uitdagingen. De cypherpunks concludeerden dat het niet zo eenvoudig was om een digitale vorm van contant geld te maken die veilig was en de potentie had om op grote schaal te worden toegepast in de echte wereld.

Het verhaal neemt echter een wending wanneer een individu, lerend van de lessen van de cypherpunks, het concept van een gedecentraliseerde digitale valuta naar nieuwe hoogten tilt. In de volgende hoofdstukken onderzoeken we hoe de bijdrage van deze persoon, voortbouwend op 40 jaar aan eerder werk, uiteindelijk leidde tot de creatie van een functioneel systeem.

Hoofdstuk #6

Een introductie tot bitcoin

6.0 Satoshi Nakamoto en de creatie van bitcoin

6.1 Hoe werkt bitcoin?

6.1.1 Het Nakamoto consensus mechanisme

6.1.2 De spelers van het spel

Activiteit: consensusvorming in een peer-to-peer netwerk

6.2 Bitcoin als eerlijk digitaal geld

6.2.1 Inleiding

6.2.2 Kenmerken van bitcoin

Activiteit: discussie in de klas - Is bitcoin eerlijk geld?

6.2.3 Omarm persoonlijke verantwoordelijkheid

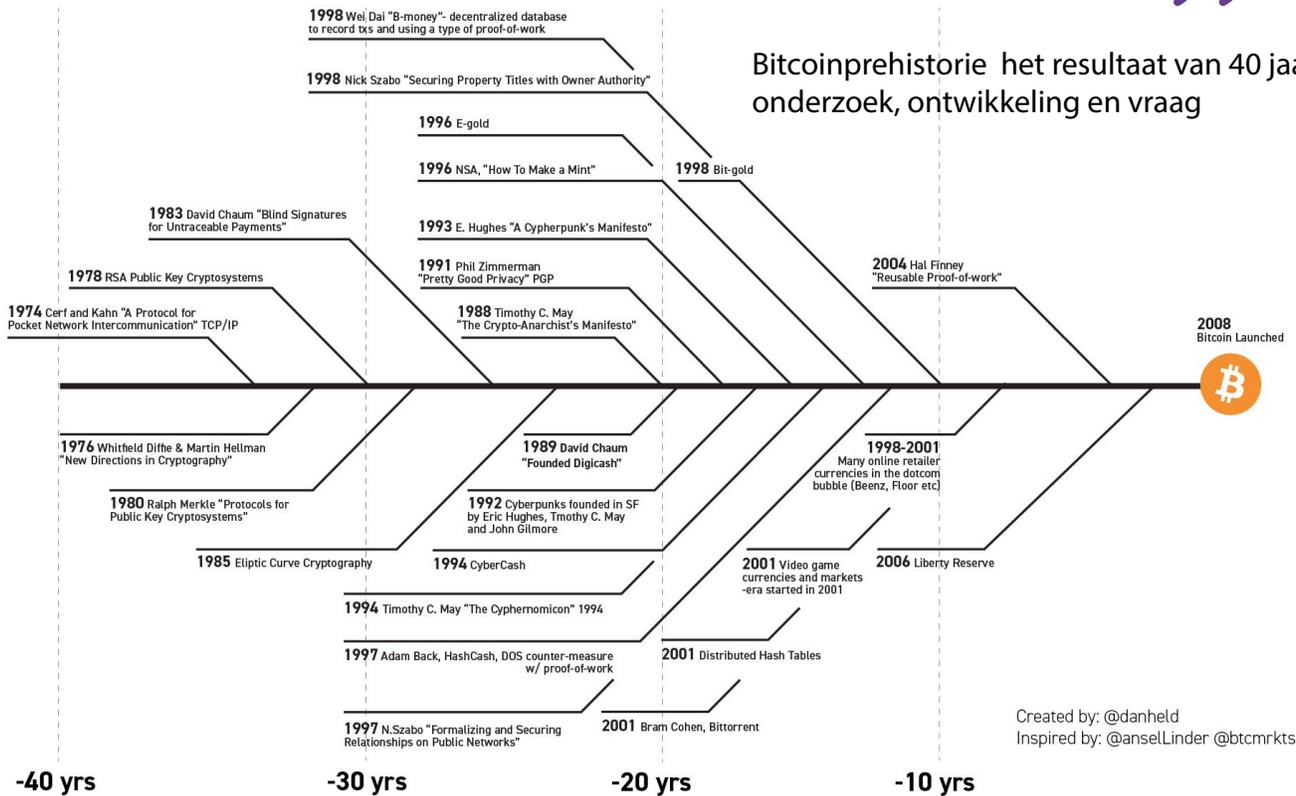
Een introductie tot bitcoin

6.0 Satoshi Nakamoto en de creatie van bitcoin

Veel mensen doen e-currency automatisch af als een verloren zaak vanwege alle bedrijven die sinds de jaren negentig failliet zijn gegaan. Ik hoop dat het duidelijk is dat het alleen de centraal gestuurde aard van die systemen was die hen hebben doen falen. Ik denk dat dit de eerste keer was dat we een gedecentraliseerd, niet-op-vertrouwen gebaseerd systeem proberen.

Satoshi Nakamoto

Bitcoinprehistorie het resultaat van 40 jaar onderzoek, ontwikkeling en vraag



Created by: @danheld
Inspired by: @anselLinder @btcmrks

Zoals je in het vorige hoofdstuk hebt kunnen lezen, probeerden meerdere cypherpunks een alternatief geldsysteem te creëren. Dit hoofdstuk gaat verder met het verhaal van één van hen: een visionaire geest met de naam "Satoshi Nakamoto". Deze anonieme persoon (man, vrouw of groep) maakte al lang voor de uitvinding van bitcoin deel uit van liefhebbers van cryptografie, zoals computerwetenschappers en hackers. Samen voerden ze discussies om praktische oplossingen te vinden ter vervanging van het fiatsysteem.



Een introductie tot bitcoin

In de jaren daarna begon bitcoin snel te groeien en werd het een symbool van hoop, kracht en weerbaarheid. Het daagde het fiatsysteem uit en bood een veilige, manier om financiële transacties uit te voeren, bestand tegen censuur. Bitcoin is een open-source protocol, wat betekent dat niemand er macht over controle over heeft. Het ontwerp is openbaar en iedereen kan eraan deelnemen.

Vandaag de dag leeft Nakamoto's droom van een grenzeloos, transparant en veilig financieel systeem voort en geeft het de wereldwijde vrijheidsrevolutie die we vandaag de dag zien. Elke dag kiezen gewone mensen ervoor om uit het fiatsysteem te stappen en in de wereld van bitcoin te stappen. Bitcoinhubs - de zogenaamde circulaire bitcoineconomieën - zijn gelanceerd door vrijheidsactivisten in regio's over de hele wereld. Zelfs hele landen die op zoek zijn naar een alternatieve weg, zoals El Salvador, beginnen op hun eigen manier bitcoin te gebruiken.

6.1 Hoe werkt bitcoin?

6.1.1 Het Nakamoto consensus mechanisme

Dus, hoe werkt bitcoin? Bitcoin heeft heel veel mogelijkheden en de "rabbit hole" gaat diep, heel diep. Gelukkig hoef je, als je je voor het eerst in de bitcoinwereld begeeft, niet perfect te begrijpen hoe het werkt voordat je het kan gebruiken. Hetzelfde geldt voor het gebruik van internet. De meeste mensen weten niet hoe het TCP/IP protocol werkt, maar toch versturen ze elke dag e-mails, berichten en plaatsen ze content op hun sociale media account. Hetzelfde geldt voor autorijden. De meeste mensen weten niet precies hoe een auto werkt, maar ze weten wel hoe ze moeten rijden.



Bitcoin is echter nog niet breed in gebruik. Het is nog steeds een vrij nieuwe technologie, zoals het internet dat was in de jaren '90. Daarom kan het handig zijn om de basis van bitcoin op een eenvoudige, minder technische manier te begrijpen.

Het belangrijkste idee achter de werking van bitcoin kan in één zin worden samengevat: bitcoin is een overeenkomst tussen mensen online. Je kunt het vergelijken met het spelen van een bordspel met vrienden. Als je een bordspel zoals Monopoly speelt, maak je afspraken met de andere spelers over bepaalde regels. Eén van de regels van Monopoly is dat alleen speciale "Monopoly biljetten" worden geaccepteerd. Als James (een van de spelers) tegen de regels ingaat door toiletpapier te gebruiken om een huis te kopen in plaats van Monopolybiljetten, dan zouden de andere spelers James vertellen dat hij een valsspeler is en gewoon stoppen met spelen. Kortom, om het spel te spelen moet je het met elkaar eens zijn over een aantal regels, en je wijkt niet af van die regels, anders word je afgewezen.

Zo kun je bitcoin ook zien. bitcoin is een netwerk van mensen die het eens zijn over dezelfde set regels. Deze regels zijn wiskundig gebonden, geschreven in computercode en direct geaccepteerd door alle mensen die de bitcoinsoftware draaien. De regels van bitcoin gelden in gelijke mate voor alle deelnemers, wat betekent dat iedereen ofwel de regels van het spel volgt, ofwel niet kan meespelen omdat ze dan door het netwerk worden afgewezen.

Een van de regels is bijvoorbeeld "Er zullen nooit meer dan 21 miljoen bitcoins zijn". Als sommige mensen 1 miljoen extra bitcoins voor zichzelf willen maken, hebben ze daar niets aan, omdat ze automatisch door alle anderen geïdentificeerd en geweigerd zouden worden. Dit is wat bitcoin zo robuust maakt.

Het maakt niet uit wie je bent of waar je vandaan komt, als je de bitcoinwereld betreedt, moet je met dezelfde regels spelen als ieder ander.

Dit geldt ook voor alle mensen en entiteiten die enorm veel controle en invloed hebben in de fiatwereld. In de bitcoinwereld is er geen ruimte voor bedrog of sabotage. Iedereen wordt gelijk behandeld en niemand kan daar iets aan doen.

Wist je dat bitcoin sinds 2009 meer dan tienduizenden pogingen heeft weerstaan om het te hacken, te manipuleren of te veranderen? Bitcoin heeft bewezen dat niemand het kan stoppen, controleren of manipuleren.



Een introductie tot bitcoin

6.1.2 De spelers van het spel

Om de decentralisatie van bitcoin beter te begrijpen, moeten we dieper ingaan op de verschillende rollen binnen het netwerk. In de bitcoinwereld spelen verschillende deelnemers verschillende maar harmonieuze rollen, die bijdragen aan het naadloos functioneren van het netwerk.

1. Miners: de architecten van de veiligheid

Miners zijn de ruggengraat van bitcoin. Dit zijn mensen of groepen mensen die achter de schermen werken om het netwerk te onderhouden en te beveiligen via een mechanisme dat Proof-of-Work (PoW) heet. Deze spelers hebben speciale computers met zware rekenkracht. Ze stellen hun hardware beschikbaar aan het bitcoin netwerk en concurreren met elkaar bij het vinden van complexe cryptografische getallen, het verifiëren van transacties en het toevoegen van nieuwe blokken met informatie over transacties aan het gedecentraliseerde kasboek van bitcoin (de zogenaamde blockchain). Hun inzet zorgt voor de onveranderlijkheid van het kasboek en beschermt tegen kwaadaardige aanvallen.



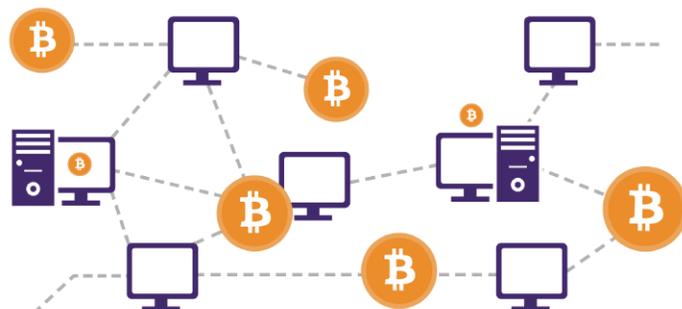
Door de gedecentraliseerde aard van mining kan iedereen met voldoende rekenkracht meedoen. Miners die door hun harde werk de puzzel het snelst oplossen worden beloond in de vorm van bitcoin.

Bitcoinminers zijn over de hele wereld verspreid en beschermen het netwerk tegen centralisatie en zorgen ervoor dat de veiligheid van bitcoin robuust en gedistribueerd blijft.

2. Nodes: poortwachters van validatie

Bitcoinnodes zijn computers van gewone mensen, verspreid over de hele planeet. Deze nodes vormen de poortwachters van het bitcoinnetwerk. De bitcoinsoftware op hun nodes houdt een kopie bij van het hele bitcoinkasboek. Nodes valideren transacties en zorgen ervoor dat alle deelnemers zich aan de consensusregels houden.

Door de verantwoordelijkheid voor de validatie te verdelen over een netwerk van nodes, blijft bitcoin bestand tegen aanvallen en behoudt het zijn vertrouwensloze karakter. Nodes spelen een cruciale rol in het handhaven van de integriteit van het Kasboek en dragen bij aan de decentralisatie van bitcoin.



3. Gebruikers: gerechtigde deelnemers

Gebruikers zijn de levensader van het bitcoinnetwerk. Het zijn individuen die transacties uitvoeren. Je kunt gebruikers zien als gewone mensen die doodnormaal hun leven leiden, maar die zichzelf ook op een bepaalde manier hebben versterkt door bitcoin erin te integreren. Sommige gebruikers sparen bijvoorbeeld hun geld in bitcoin. Anderen, zoals inwoners van El Salvador, gebruiken bitcoin als geld om boodschappen te doen en ontvangen bitcoin in de vorm van een salaris.

Bitcoin versterkt de macht van gebruikers door tussenpersonen zoals banken en overheden overbodig te maken. Dit digitale betaalmiddel maakt directe peer-to-peer transacties mogelijk, waardoor gebruikers rechtstreeks met elkaar handelen en volledige controle over hun geld behouden.

4. Ontwikkelaars en projecten: architecten van innovatie

Het monetaire systeem van de toekomst bouwt zichzelf niet vanzelf op en krijgt ook geen wereldwijd gebruik op een ethisch correcte manier zonder inspanning. Dat is waar bitcoin-ontwikkelaars en bitcoinprojecten om de hoek komen kijken.

Ontwikkelaars gebruiken hun technische expertise om het bitcoinprotocol te verbeteren en te innoveren. Deze mensen schrijven code, stellen verbeteringen voor en pakken kwetsbaarheden aan, zodat het netwerk zich ontwikkelt als reactie op allerlei uitdagingen. Het open-source karakter van bitcoin nodigt uit tot samenwerking, waardoor ontwikkelaars wereldwijd kunnen bijdragen aan de groei.

De schoonheid van deze gedecentraliseerde ontwikkeling voorkomt dat een enkele entiteit de controle over het protocol monopoliseert. Dit gebeurt door middel van een consensusgestuurd proces. Ontwikkelaars stellen ideeën en veranderingen voor en alleen degenen met de beste ideeën die aansluiten bij de bredere visie voor een betere wereld, krijgen steun van de gemeenschap. Dit zorgt voor een transparante en democratische evolutie van bitcoin totdat het klaar is voor 8 miljard mensen.

Bij bitcoinprojecten zijn verschillende groepen betrokken, van missiegedreven non-profit organisaties tot bedrijven, groepen en individuen die waardevolle inhoud creëren. Mensen die samenwerken aan een specifiek doel binnen de grotere bitcoinmissie naar collectieve vrijheid.

Bitcoinprojecten spelen een cruciale rol in het vormgeven en bevorderen van de adoptie van bitcoin, door te werken aan een toekomst die prioriteit geeft aan de vrijheid en kracht en de vrijheid van de mens.

Een introductie tot bitcoin

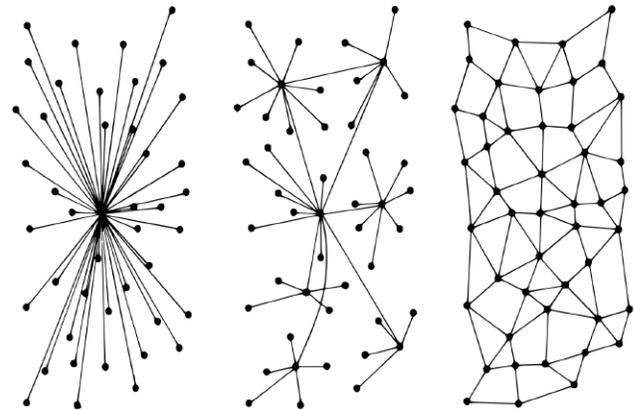
De symfonie

De decentralisatie van bitcoin kan worden gezien als een harmonieus muziekorkest, een evenwichtsoefening waarbij verschillende instrumentspelers samen de mooiste muziek maken. Er is geen baas in het bitcoinnetwerk, in plaats daarvan vervullen zowel miners, nodes, gebruikers, ontwikkelaars en projecten hun rol met autonomie en samenwerking.

Het gedecentraliseerde kasboek, onderhouden door nodes, garandeert transparantie, terwijl het proof-of-work mechanisme veiligheid biedt en centralisatie in mining tegengaat. Gebruikers hebben financiële soevereiniteit en zeggenschap, vrij van de controle van het fiatsysteem. Ontwikkelaars, zorgen ervoor dat het protocol zich aanpast aan de veranderende behoeften van de mensheid. Bitcoinprojecten dragen op hun eigen unieke manier bij aan collectieve vrijheid.

Zoals je ziet, heeft elke deelnemer een cruciale rol in het bevorderen van wereldwijde acceptatie van bitcoin en het versterken van de menselijke samenleving. Elke deelnemer draagt bij aan de veerkracht en levensduur van bitcoin en creëert een vertrouwensvrij, grenzeloos en mondig ecosysteem.

Samengevat resonanceert de symfonie van decentralisatie in bitcoin als een bewijs van Satoshi Nakamoto's visie en de immense passie van een wereldwijde gemeenschap op zoek naar vrijheid en kracht.



Gecentraliseerd

Gedecentraliseerd

Gedistribueerd

Activiteit in de klas: consensusvorming in een peer-to-peer netwerk



Doel

Begrijpen hoe consensus wordt bereikt in een groep, leren over cryptografie en de consensuslaag van bitcoin.



Materiaal

Bericht met versleutelde en onversleutelde instructies voor acties ("val aan" of "val niet aan").



Vorbereiding van de activiteit

De docent selecteert voor de les een groep van 3 of 4 studenten die kwaadaardige nodes spelen tijdens deze activiteit.

Oefening:

- 1 De docent selecteert een student als "initiator" en geeft die student stuk papier waar "ATTACK" op staat geschreven. De docent geeft aan een andere student een stuk papier met een serie getallen: "4-16-14-21-1-21-1-3-11-".
- 2 De studenten vormen een kring. Zorg ervoor dat de geselecteerde studenten, die de kwaadaardige nodes spelen, niet naast elkaar staan.



- 3 Zodra de groep een cirkel heeft gevormd, geeft de "initiator" het briefje door aan de persoon recht
- 4 Nadat iedereen het bericht heeft gelezen, geeft de "initiator" het signaal aan de groep door "Nu" te zeggen. De groep reageert tegelijkertijd op het bericht. Als de boodschap "ATTACK" luidt, zetten alle deelnemers een stap naar voren.
- 5 Na de eerste reactie zullen sommige studenten (degenen die het versleutelde bericht hebben ontvangen en het juist hebben geïnterpreteerd) stil blijven staan, terwijl de rest de oorspronkelijke instructie zal volgen, wat een gebrek aan consensus blootlegt.

Conclusie:

Bespreek waarom er geen consensus is bereikt, introduceer het concept van het Byzantijnse generaalsprobleem, hoe dit verband houdt met de behoefte aan een gemeenschappelijk doel en bespreek later hoe bitcoin een oplossing biedt voor dit probleem.

Een introductie tot bitcoin

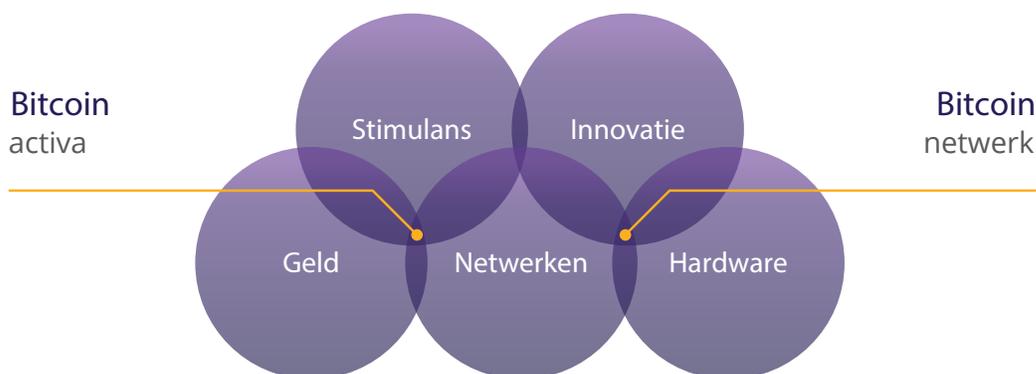
6.2 Bitcoin als eerlijk digitaal geld

6.2.1 Inleiding

Activiteit:
Bekijk deze
1,5 min.
durende
video,
"What is
bitcoin?"



Simpel gezegd. Bitcoin is geld, geen investeringsmiddel, maar een veilige manier om je zuurverdiende geld te bewaren. Het bezit van bitcoin maakt je niet automatisch rijk; je verzamelt immer niet meer bitcoins. De prijsstijging ten opzicht van fiatgeld komt door bitcoin's stijgende populariteit en de inflatie van fiatgeld.



Bitcoin is een nieuwe vorm van geld, het is "Het internet van geld", wat betekent dat iedereen zich kan aansluiten bij bitcoin en waarde kan gaan uitwisselen met andere bitcoingebruikers. Zelfs de meest geïsoleerde en arme gemeenschappen ter wereld hebben eindelijk toegang tot een monetair systeem. Net zoals dat iedereen met een telefoon en een internetverbinding een zoekmachine kan gebruiken, maakt bitcoin het voor iedereen met een telefoon en een internetverbinding mogelijk om toegang te krijgen tot een nieuw wereldwijd monetair systeem.



Snellere,
goedkopere
betalingen

Stuur geld over de hele wereld in slechts enkele minuten, tegen lage kosten.



Financiële
inclusiviteit

2,5 miljard mensen zonder bankrekening hebben toegang tot geld via een telefoon of computer.

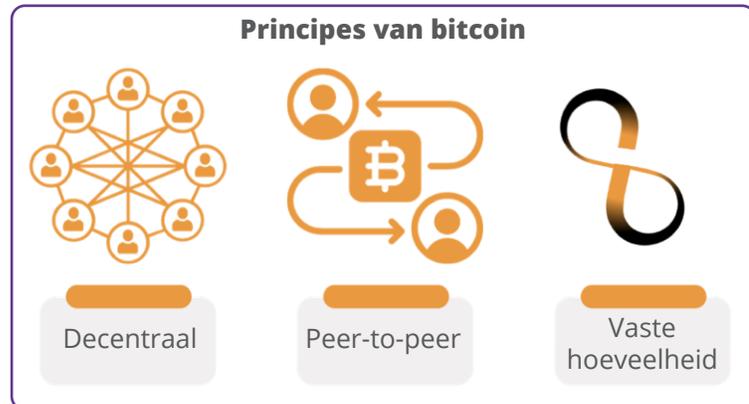


Meer
privacy

Bitcointransacties zijn openbaar, maar jouw identiteit niet.

Bitcoin is volledig digitaal en grenzeloos. Het maakt niet uit waar je je bevindt, want het leeft op computers en smartphones van mensen die over de hele wereld verspreid zijn. Veel gebruikers over de hele wereld gebruiken de bitcoinsoftware en een kopie van het bitcoinkasboek. De kans dat deze software en het register van alle transacties verdwijnt, is heel klein omdat er talloze kopieën van zijn. Om het uit te schakelen, zou je het hele internet voorgoed moeten afsluiten, wat hoogst onwaarschijnlijk is.

En tot slot is bitcoin schaars, wat betekent dat de hoeveelheid bitcointokens die kunnen bestaan absoluut beperkt is. Niemand kan bitcoin namaken. Zelfs de machtigste overheden en financiële instellingen niet.



6.2.2 Kenmerken van bitcoin

De evolutie van eerlijk geld

Zoals je in hoofdstuk 2 hebt geleerd, doorloopt de levenscyclus van eerlijk geld drie stadia om algemeen geaccepteerd te worden door de menselijke samenleving: van spaarmiddel naar ruilmiddel en uiteindelijk rekeneenheid.

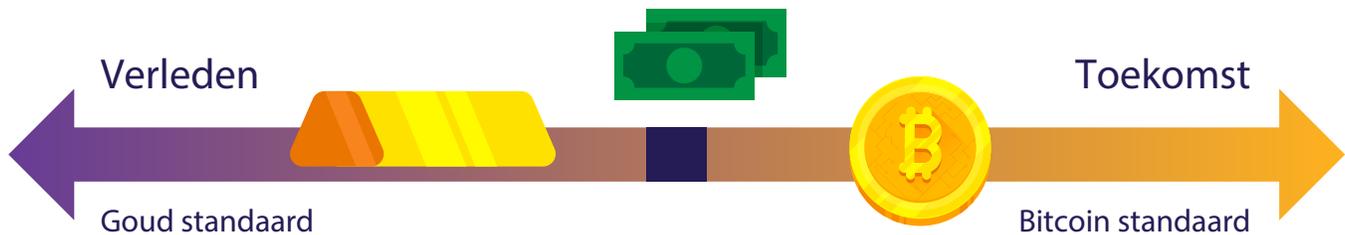
De eerste fase van geld, een spaarmiddel, is wanneer een goed na verloop van tijd het vertrouwen begint te krijgen als een waardevast (of toenemend) activum. Mensen die dit vroeg herkennen, proberen hun welvaart te beschermen door het op te slaan in deze vorm van geld, vooral in een tijd van geopolitieke en macro-economische onzekerheden.

Sommige groepen, zoals de media, noemen bitcoin een vorm van "digitaal goud". Dit komt omdat bitcoin zich in het afgelopen decennium stevig heeft gevestigd als spaarmiddel. Elke dag beginnen meer en meer mensen bitcoin te zien als middel om zich te beschermen tegen de nadelen van inflatie, zoals goud dat deed doorheen de geschiedenis van de mensheid.

De volgende fase is wanneer het vertrouwen in de stabiliteit van een geldsoort groeit. Dit is het moment waarop het geld verandert in een ruilmiddel, dat transacties in het dagelijks leven van mensen vergemakkelijkt. In dit stadium wordt het geld algemeen geaccepteerd voor het uitwisselen van goederen en diensten.

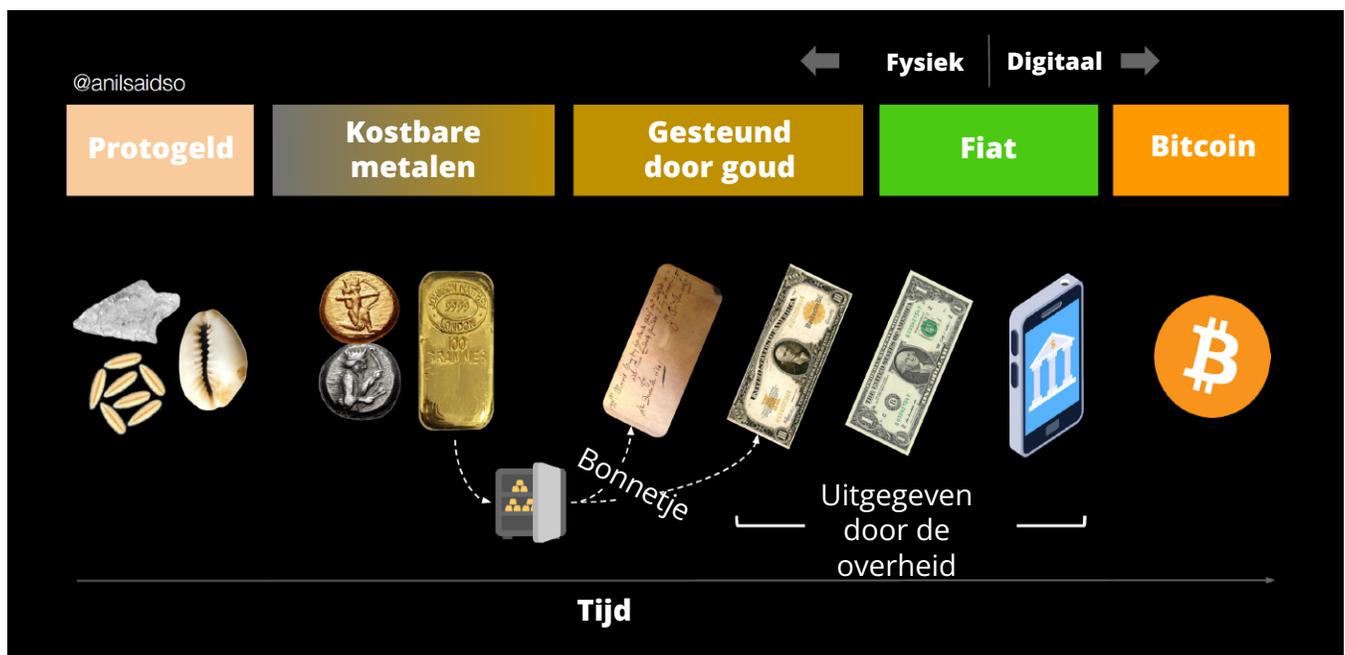
Bitcoin wordt steeds meer een ruilmiddel. Met de groeiende acceptatie door handelaren en de ontwikkeling van het protocol worden bitcointransacties steeds efficiënter en gebruikelijker in de dagelijkse handel. Een voorbeeld hiervan is El Salvador, waar bitcoin officieel erkend is als wettig betaalmiddel. Elke dag beginnen steeds meer gewone burgers en bedrijven bitcoin te gebruiken als ruilmiddel.

Een introductie tot bitcoin



In het laatste stadium bereikt een valuta de status van rekeneenheid, die dient als gemeenschappelijke maatstaf voor het prijzen van goederen en diensten. Dit is het stadium waarin het de standaard metriek wordt waaraan alle andere waarden worden afgemeten.

De evolutie tot het worden van een rekeneenheid is een lange proces. Op dit moment meet de wereld goederen en diensten alleen in fiatvaluta, en daarom moet bitcoin breder geaccepteerd en geïntegreerd worden in verschillende financiële systemen. De basis is echter al gelegd nu bedrijven en particulieren de prijzen van goederen en diensten in bitcoin beginnen aan te geven.



Zoals je kunt zien, is bitcoin goed op weg in deze evolutionaire cyclus van eerlijk geld. Als bitcoin volledig geïntegreerd is in het wereldwijde financiële systeem, kan het een standaard-rekeneenheid worden, die het hele wereldwijde monetaire systeem een nieuwe vorm geeft.

Eigenschappen van geld

Zoals je in hoofdstuk 2 hebt geleerd, is de mensheid er in de loop der tijd achter gekomen dat echt eerlijk geld bepaalde eigenschappen moet bezitten om effectief te zijn. Deze eigenschappen zijn duurzaam, deelbaar, draagbaar, aanvaardbaar, schaars en uitwisselbaar.

Laten we eens kijken of bitcoin de test doorstaat.

Duurzaam: bitcoin is een puur digitaal en kan dus niet degraderen.

Deelbaar: ter vergelijking: de euro kan worden opgedeeld tot op de cent (€0,01). Bitcoin kan worden onderverdeeld in wat bekend staat als een satoshi of sat (0,00000001 BTC). Door het digitale karakter van bitcoin kan het in de toekomst nog verder worden opgedeeld als de mensheid dat nodig heeft. Bitcoin is momenteel het meest deelbare goed ter wereld.

Draagbaar: in april 2020 werd \$1,1 miljard overgemaakt in slechts een paar minuten, en het kostte maar 68 cent. Geen enkele andere manier van betalen kan zoveel geld verplaatsen, tegen zulke lage kosten, zo snel, en zonder tussenkomst van derde partijen. Dit maakt bitcoin de gemakkelijkst verplaatsbare vorm van geld ter wereld.

Aanvaardbaar: Als ruilmiddel staat bitcoin staat nog in de kinderschoenen om een ruilmiddel te worden en vergeleken met fiatgeld is de acceptatie van bitcoin op dit moment laag.

Schaars: er zullen maar maximaal 21 miljoen bitcoins bestaan. De code is zo geschreven dat dit aantal nooit zal worden overschreden, wat betekent dat bitcoin niet alleen schaars is, maar zelfs het schaarste goed ter wereld.

Uitwisselbaar: elke eenheid bitcoin is hetzelfde als elke andere eenheid bitcoin en kan worden uitgewisseld en verhandeld via het bitcoinprotocol als gelijke eenheid, wat het tot een onderling verwisselbaar goed maakt.

Een introductie tot bitcoin

Bitcoin versus goud versus fiat

Eigenschappen van geld	Goud	Fiat	Bitcoin
Duurzaam	Hoog	Gemiddeld	Hoog
Draagbaar	Gemiddeld	Hoog	Hoog
Deelbaar	Gemiddeld	Gemiddeld	Hoog
Vervangbaar	Hoog	Hoog	Hoog
Schaars	Gemiddeld	Laag	High
Verifieerbaar	Gemiddeld	Gemiddeld	Hoog
Gevestigde geschiedenis	Hoog	Gemiddeld	Laag
Resistent tegen censuur	Gemiddeld	Gemiddeld	Hoog
Slim/programmeerbaar	Laag	Gemiddeld	Hoog

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

Bitcoin is een soort slim geld dat programmeerbaar is, niet afgepakt kan worden en beschikt over eigenschappen die het uitermate geschikt maken om als spaarmiddel te dienen.

Omdat het een transparant digitaal kasboek is, kan bitcoin super efficiënt zijn in het opsporen van fraude en het ontdekken van risico's in zijn diensten. Het heeft de goede kanten van goud, zoals dat er maar een beperkte hoeveelheid van is, maar het heeft ook de voordelen van fiatvaluta omdat je het kunt opdelen en gemakkelijk kunt meenemen. Bovendien biedt het nieuwe functies die handig zijn in onze digitale wereld.

Wat vind jij? Bitcoin is nog niet algemeen erkend en geaccepteerd, maar is bitcoin eerlijk geld?

Activiteit: discussie in de klas - Is bitcoin eerlijk geld?

Laten we, nu we bitcoin in meer detail hebben besproken, nog eens kijken naar onze geldvergelijkingstabel uit hoofdstuk 2 en kijken hoe bitcoin zich verhoudt tot andere vormen van geld:

Karakteristieken van eerlijk geld	 Koeien	 Cigaretten	 Diamanten	 Euros	 Bitcoin
Duurzaam					
Draagbaar					
Uniform					
Geaccepteerd					
Schaars					
Deelbaar					
Total					

6.2.3 Omarm persoonlijke verantwoordelijkheid

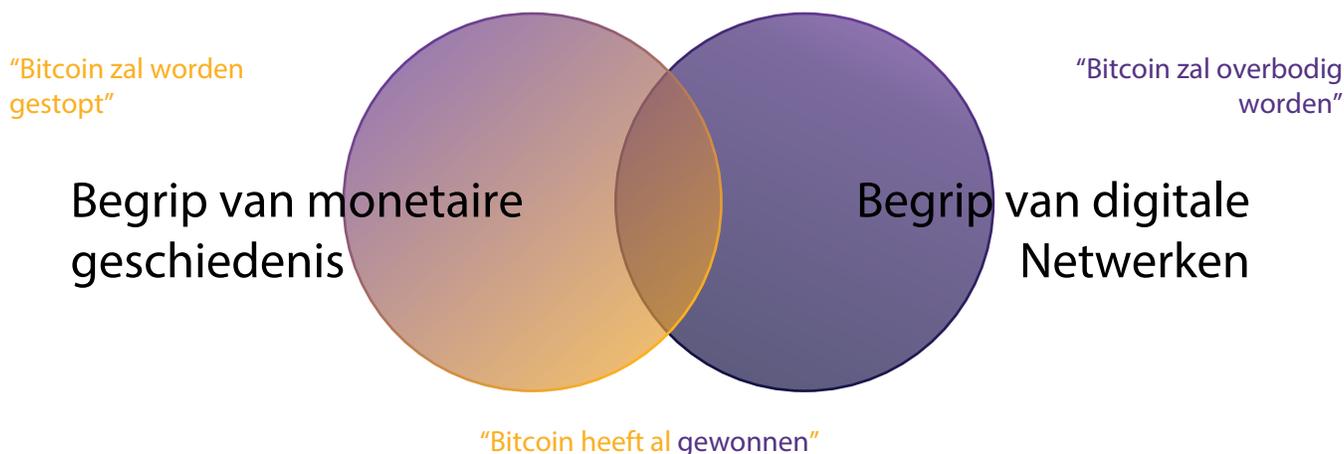
Het resultaat is een gedistribueerd systeem zonder enkelvoudig punt van falen. Gebruikers hebben de cryptografische sleutels van hun eigen geld en doen rechtstreeks transacties met elkaar, met behulp van het peer-to-peer netwerk dat controleert op op dubbele uitgave.

Satoshi Nakamoto

Een introductie tot bitcoin

In de fiatwereld vertrouwen mensen op overheden, banken en gevestigde leveranciers van betalingsdiensten. De hoofden van deze (financiële) instellingen bepalen de regels van het netwerk en de deelnemers, meestal gewone burgers, moeten zich aan deze regels houden. Het maakt niet uit waar je woont, er zijn altijd een aantal standaardprocedures die je instrueren wat je moet doen en hoe je het moet doen. Na verloop van tijd leidde dit tot een periode vol ontberingen, vooral voor gezinnen die worstelen met de toenemende uitdagingen van het dagelijks leven.

Door dit systeem zijn mensen gewend om de verantwoordelijkheid voor hun financiën in de handen van anderen te leggen. De meeste mensen vertrouwen er bijvoorbeeld op dat iemand anders hen helpt, vooral als er iets misgaat (zoals het verlies van toegang tot je bankrekening).



Het monetaire systeem van bitcoin is, zoals je weet, heel anders. Bitcoin werkt op een specifieke manier en heersers zijn vervangen door een autonoom systeem van regels. Er is geen dictator of leider, wat ook betekent dat er niemand is die jou gaat voorschrijven wat je moet doen. Als je de nieuwe vrijheid en macht van bitcoin wilt, zul je moeten leren hoe het werkt en de technologie moeten integreren op een manier die voor jou persoonlijk werkt.

	<div data-bbox="483 1499 781 1591">Eenheid</div> Cent 0.01	<div data-bbox="829 1499 1127 1591">(de)centralisatie</div> 	<div data-bbox="1179 1499 1476 1591">Uitgevende partij</div> 
	Sat 0.00000001		

Met bitcoin heb je volledige controle over je geld, maar met deze extra controle komt ook een grotere verantwoordelijkheid. Als je bijvoorbeeld de toegang tot je bitcoin verliest door je sleutels van je digitale wallet te verliezen, ben je je spaargeld voorgoed kwijt. Er is geen klantenservice of iemand die je kunt bellen als er een probleem is. Je moet er zelf voor zorgen.

Gelukkig zal dit niet gebeuren met de individuen die besluiten om volledige verantwoordelijkheid te nemen over hun eigen leven. Het gebruik van bitcoin is niet per definitie ingewikkeld; het is gewoon een nieuw concept. Eventuele ongemakkelijkheid ontstaat omdat het onbekend is, maar als je bereid bent om te leren hoe je bitcoin het beste kunt gebruiken en om de verantwoordelijkheid om je welvaart veilig te stellen volledig te omarmen, wordt bitcoin een machtig instrument, omdat je de controle hebt en niemand je rijkdom in beslag kan nemen.

Samengevat ligt de sleutel in het begrijpen van de werking van bitcoin en de vrijheid om het implementeren volgens jouw unieke behoeften en levensfilosofie.

In het volgende hoofdstuk beginnen we met het gebruik van bitcoin door een bitcoinwallet in te richten, onze eerste transacties te verzenden en te ontvangen en de beste beveiligingsmethoden te bespreken.

Hoofdstuk #7

Hoe gebruik ik bitcoin?

7.0 Inleiding

7.1 Bitcoin verkrijgen en ruilen

7.1.1 P2P: persoonlijk in de echte wereld

7.1.2 P2P: online

7.1.3 Gecentraliseerde exchanges

7.2 Bitcoinwallets, een introductie

7.2.1 Self-custodial vs custodial wallets

7.2.2 Verschillende typen bitcoinwallets

7.2.3 Open-source vs closed-source

Activiteit: evaluatie van bitcoinwallets

7.3 Een mobiele bitcoinwallet instellen

Activiteit: een bitcoinwallet opzetten/herstellen

7.4 Transacties ontvangen en versturen

Activiteit: bitcointransacties in de praktijk

7.5 Sparen in bitcoin

7.6 Don't trust, verify

Hoe gebruik ik bitcoin?

7.0 Inleiding

Waarom zou iemand nergeld in plaats van centralebankgeld vertrouwen? Nerds brachten jullie het internet. Banken brachten je de grote depressie.

Andreas M. Antonopoulos

Nu we beter begrijpen wat bitcoin is en waar het voor dient, is het tijd om te leren hoe je het in de praktijk kunt gebruiken. In dit hoofdstuk begeleiden we je stap voor stap door het proces van het verkrijgen van bitcoin, verkennen we de verschillende soorten wallets die beschikbaar zijn, helpen we je bij het opzetten van je eigen bitcoinwallet en oefenen we zelfs met het versturen en volgen van een bitcointransactie op het netwerk. Het is tijd om je kennis toe te passen.

7.1 Bitcoin verkrijgen en ruilen

Er zijn veel manieren om bitcoin te verwerven en te spenderen. Je kunt bijvoorbeeld:

- betaald krijgen in bitcoin in ruil voor je werk, en ermee betalen voor producten en diensten van anderen. (Meer hierover in hoofdstuk 8)
- bitcoin minen (meer daarover in hoofdstuk 9)
- met iemand persoonlijk je fiatgeld omruilen voor bitcoin, of andersom.
- je fiatgeld online omwisselen voor bitcoin, of andersom



Hieronder zullen we het omwisselen van fiatgeld voor bitcoin en vice versa bespreken, zowel via persoonlijke transacties als online methoden, omdat dit de meest voorkomende opties zijn.

7.1.1 Peer-to-peer: persoonlijk in de echte wereld

Bij peer-to-peer (P2P) aan- of verkooptransacties van bitcoin ruil je fiatgeld (of een ander goed of dienst) direct voor bitcoin met een ander individu, zonder tussenkomst van een bank of een andere partij.

Beide partijen bepalen samen het wisselbedrag en de koers. De ene persoon levert het fiatgeld, de andere draagt de bitcoin over en de transactie is afgerond. Hoewel het gemakkelijker is om peer-to-peer transacties fysiek uit te voeren door de andere persoon rechtstreeks in de echte wereld te ontmoeten, kun je dit dankzij het internet ook vrijwel overal doen.



7.1.2 Peer-to-Peer: online

Maak kennis met peer-to-peer platformen, waar kopers en verkopers van bitcoin elkaar ontmoeten om rechtstreeks transacties met elkaar uit te voeren zonder tussenpersonen.

Bij zulke platformen hoef je niemand je informatie of geld toe te vertrouwen, je kunt andere peers ontmoeten en rechtstreeks met hen handelen.



Op de meeste peer-to-peer platformen moeten peers een deel van het geld in “escrow” plaatsen om er zeker van te zijn dat ze hun deel van de deal nakomen. Escrow betekent dat het geld tijdelijk op een veilige plaats wordt vastgezet, in beheer van het platform. Als een van de partijen niet meewerkt met de deal, krijgt de ander zijn vastgezette bedrag terug. Het is als een vertrouwde vriend die de spullen bewaart tot aan de afgesproken voorwaarden is voldaan

7.1.3 Gecentraliseerde exchanges

Het gebruik van gecentraliseerde exchanges is voor velen de gemakkelijkste manier om bitcoin te kopen en verkopen, maar het brengt ook aanzienlijke nadelen met zich mee. Gecentraliseerde exchanges zijn bedrijven die klanten toestaan om bitcoin direct via hen te kopen en verkopen. Aan dit gemak hangt echter een prijskaartje.



Gecentraliseerd

Afwegingen bij gecentraliseerde exchanges

Het is belangrijk om te weten dat als je bitcoin koopt via een gecentraliseerde exchange, je vaak persoonlijke informatie moet verstrekken en je identiteit moet verifiëren. Dit creëert een risico op identiteitsdiefstal en stelt je persoonlijke informatie bloot aan potentiële bedreigingen. Bovendien bewaren gecentraliseerde exchanges je bitcoin, wat betekent dat je geen controle hebt over je geld totdat je het bij hen opneemt.

Erger nog, gecentraliseerde exchanges kunnen het geld van gebruikers verduisteren of meer bitcoin uitlenen dan ze aan reserves hebben, totdat ze instorten. Ja, net als banken! Maar in de bitcoinwereld is er geen centrale bank die frauduleuze banken kan redden door meer geld bij te drukken, want bitcoin kan niet worden bijgedrukt!

Hoe gebruik ik bitcoin?

7.2 Bitcoinwallets, een introductie

In tegenstelling tot fysiek geld zijn bitcoins niet daadwerkelijk aanwezig in een bitcoinwallet. Ze leven in het gedistribueerde kasboek (ledger) dat het bitcoinnetwerk voortdurend verifieert en beveiligt. Dus hoe kun je dan bitcoin bezitten?

Je bent pas eigenaar van je bitcoin als je de private keys (privésleutels) bezit waarmee je transacties kunt ondertekenen, want met deze private keys kan je het eigendom van jouw bitcoin aan iemand anders overdragen. Dit is het versturen van bitcoin.

Laten we, met dat in gedachten, eens kijken naar 2 concepten die we beschrijven als we de term "wallet" gebruiken:



- Een master private key (wat lijkt op een wachtwoord) waarmee je public keys (publieke sleutels) genereert die je met anderen kan delen om bitcoins te ontvangen en versturen.
- De mobiele of desktop-interface waarmee je kunt communiceren met het bitcoinnetwerk om je bitcoinsaldo op te vragen, transacties te versturen of ontvangen, en om ze te presenteren aan het netwerk. In de volgende paragraaf worden verschillende soorten wallets beschreven, samen met hun voor- en nadelen.

7.2.1 Self-custodial vs custodial wallets

Voordat we ingaan op de details van de verschillende soorten bitcoinwallets en hun kenmerken, maken we een belangrijk onderscheid tussen self-custodial en custodial wallets. Self-custodial wil zeggen dat de gebruiker de private keys bezit en dus dat de bitcoin echt zijn/haar bezit is. Bij een custodial wallet bezit een derde partij de bitcoin. De onderstaande tabel benoemt de voordelen en risico's van elk type wallet.

Wallet type	Who beheert mijn bitcoin?	Voordelen	Risico's
Self-custodial wallets	De gebruiker	Volledige controle over tegoeden en transacties, geen goedkeuringsproces of bevroering van rekeningen mogelijk, geen controle door bedrijven of overheden, beschermd tegen willekeurige inbeslagname, alsof je je geld thuis bewaart.	Geen herstel als de herstelzin verloren gaat, minder klantenondersteuning, de volledige verantwoordelijkheid ligt bij de gebruiker.
Custodial wallets	Een derde partij	Eenvoudig herstel als de toegang verloren is gegaan, eenvoudigere klantenondersteuning	Tegoeden zijn altijd verbonden met het internet en dus kwetsbaarder voor hacking en inbreuken. Beheerders kunnen rekeningen bevriezen.

Bij een self-custodial wallet (ook wel non-custodial genoemd) ben jij de enige met de sleutels van de wallet en heb je daarmee de volledige controle. Bij een custodial wallet heeft iemand anders de sleutels in bezit en heeft men toegang tot de inhoud van je wallet.

-  Self-custody is alsof je je eigen bank bent. Transacties zijn niet onderworpen aan controle door een overheid of bedrijf, maar het betekent ook dat je de volledige verantwoordelijkheid draagt voor het veilig houden van je bitcoin.
-  Self-custody zorgt ervoor dat anderen je bitcoin niet in beslag kunnen nemen zonder je medewerking.
-  Self-custody geeft gemoedsrust in tijden van onzekerheid, omdat je weet dat je bitcoin veilig is.

Het is belangrijk om het juiste type wallet te kiezen voor je persoonlijke behoeften. Soms vinden mensen het moeilijk om onderscheid te maken tussen een self-custodial of een custodial wallet. Deze tabel laat de verschillen in het installatieproces zien.

Wallet type	Stap 1: kies een wallet	Stap 2: installeer de wallet	Stap 3: maak een nieuwe wallet	Stap 4: beveilig je herstelzin	Stap 5: gebruik je wallet
Self custodial wallets	Kies een self-custodial walletaanbieder	Volg de instructies van de walletaanbieder	Genereer een herstelzin (seed phrase) en ten minste één private key	Bewaar de herstelzin (seed phrase) op een veilige locatie	Gebruik je wallet om bitcoin te ontvangen en te versturen
Custodial wallets	Kies een custodial walletaanbieder	Volg de instructies van de walletaanbieder	Maak een account aan bij de walletaanbieder	n.v.t. (de walletaanbieder beheert immers de private keys)	Gebruik je wallet om bitcoin te ontvangen en te versturen



"Not your keys, not your coins" is een populair gezegde onder bitcoinbezitters. Het verwijst naar het idee dat, als je geen directe controle hebt over de private keys die gekoppeld zijn aan je bitcoinwallet, je niet echt de eigenaar bent van die bitcoin.

Wie toegang krijgt tot je private keys wordt eigenaar van je bitcoin. Daarom is het van het grootste belang om ze te beschermen en ze weg te houden van nieuwsgierige ogen! We zullen later in het boek een paar manieren bespreken waarop je dat kunt doen.

In het vervolg hebben we het alleen nog over self-custodial wallets, waarbij je zelf eigenaar bent van de sleutels en waarbij je zelf de volledige controle hebt over je bitcoin.

Maak je geen zorgen als het ingewikkeld wordt of als je niet alles begrijpt. Dit is een reis en je zult meer begrijpen naarmate je bitcoin meer gaat gebruiken!

Hoe gebruik ik bitcoin?

7.2.2 Verschillende typen bitcoinwallets

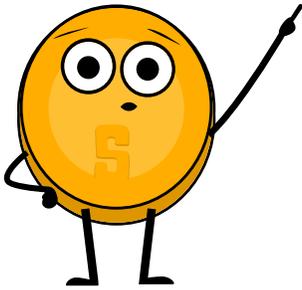
Afhankelijk van waar je private key is gemaakt en opgeslagen, gebruiken we vaak verschillende namen om bitcoinwallets te beschrijven.

Als de sleutels worden opgeslagen op je smartphone, noemen we het een "mobile wallet". Als ze veilig worden opgeslagen op een speciaal apparaat, dan noemen we het een "hardware wallet". Als de sleutel alleen op papier wordt opgeslagen, dan noemen we het een "paper wallet".

De verschillende namen die we aan bitcoinwallets geven, zijn afhankelijk van hoe ze gebruikt worden:

Wallet type	Beschrijving	Voordelen	Nadelen	Wanneer te gebruiken?
Online wallet	Een wallet die toegankelijk is via een webbrowser.	Toegankelijk vanaf elk apparaat met internet. Gemakkelijk te gebruiken.	Minder veilig. Kan worden gehackt.	Iemand die vaak bij zijn wallet moet en daar niet veel waarde in opslaat.
Mobile wallet	Een wallet die op een mobiel apparaat wordt geïnstalleerd.	Gemakkelijk. Overal toegankelijk	Kan verloren gaan als het apparaat zoekraakt, wordt gestolen of wordt gehackt.	Iemand die onderweg transacties moet doen en daar niet veel waarde in opslaat.
Desktop wallet	Een wallet die op een desktop computer wordt geïnstalleerd.	Veiliger dan online wallets. Kan ook offline worden gebruikt.	Kan worden gehackt als de computer is geïnfecteerd met malware.	Iemand die een grote hoeveelheid bitcoin wil opslaan en zich comfortabel voelt met een desktopcomputer.
Hardware wallet	Een fysiek apparaat dat bitcoin opslaat zonder verbonden te zijn met het internet.	Heel veilig. Kan ook offline worden gebruikt.	Bitcoin kan verloren gaan als het apparaat verloren gaat of wordt gestolen.	Iemand die een grote hoeveelheid bitcoin wil opslaan en bereid is te betalen voor de extra veiligheid van een hardware wallet.
Paper wallet	Een fysieke registratie van de private en public keys van een bitcoinwallet.	Heel veilig. Kan ook offline worden gebruikt.	Kan verloren gaan of gestolen worden als de fysieke registratie verloren gaat of gestolen wordt.	Iemand die een grote hoeveelheid bitcoin wil opslaan en extra voorzorgsmaatregelen wil nemen om de veiligheid te garanderen.

Omdat de keys (sleutels) van het ene apparaat naar het andere verplaatst kunnen worden, is de "status" van je bitcoinwallet niet definitief. Als ik bijvoorbeeld de keys van mijn bitcoinwallet genereer op een computer en ze later upload naar mijn telefoon, dan wordt de "desktop wallet" een "mobiele wallet".



Als het gaat om het opslaan van je bitcoin, gaat het er niet alleen om wie er controle over heeft - er zijn ook veel andere risico's waar je rekening mee moet houden. Daarom is het belangrijk om een opslagoplossing te vinden die zowel veilig als handig is.

Als je de afwegingen van de verschillende soorten wallets analyseert, zul je ontdekken dat er geen ideale wallet is die aan alle behoeften voldoet.

Bij het kiezen van een bitcoinwallet moet je hier rekening mee houden:

-  **Beveiliging:** zorg ervoor dat de wallet sterke beveiligingsmaatregelen heeft, zoals 2-Factor authenticatie en een veilig wachtwoordbeleid.
-  **Privacy:** onderzoek of de wallet je toestaat anoniem te blijven, of dat er persoonlijke informatie nodig is om een account aan te maken.
-  **Gebruiksgemak:** kies een wallet die makkelijk te gebruiken is, vooral als je nieuw bent met bitcoin.
-  **Compatibiliteit:** controleer of de wallet compatibel is met je apparaat en besturingssysteem.
-  **Fees:** vergelijk de kosten die verschillende wallets in rekening brengen. Waar krijg je de beste deal?
-  **Reputatie:** onderzoek de reputatie van de wallet en de makers om een idee te krijgen van de betrouwbaarheid.
-  **Controle:** sommige wallets geven je meer controle over je private keys, wat een veiligheidsvoordeel kan zijn.

Bedenk of je een wallet wilt die je volledige controle geeft, of eentje die gebruiksvriendelijker is maar misschien wat minder controle biedt.

7.2.3 Open-source vs closed-source

Een andere belangrijke factor om in gedachten te houden bij het kiezen van een bitcoinwallet is de keuze tussen open-source of closed-source.

Open-source code is erg belangrijk, omdat het de gemeenschap in staat stelt de broncode van de wallet te inspecteren en door te gaan met de ontwikkeling van het project, mocht het team stoppen.

Oefening in de klas. Optie 1. Download een nieuwe wallet.



Je herstelzin

Je herstelzin wordt gebruikt om je account aan te maken en te herstellen

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

Sla aub deze 12 woorden veilig op. De volgorde is belangrijk. Deze herstelzin stelt je in staat je account te herstellen

Hoe maak je en gebruik je een bitcoinwallet.

- 1 Zoek naar de app in de App Store (iOS) of Google Play Store (Android).
- 2 Open de app en maak een nieuwe wallet aan. Nu zie je 12 of 24 woorden die de herstelzin vormen (ook wel een seed phrase genoemd). Zorg ervoor dat je deze opschrijft en op een veilige plek bewaart! Met deze herstelzin kun je indien nodig weer volledige toegang krijgen tot je bitcoins.

Onthoud dat als je deze reeks woorden verliest of vergeet, je geen toegang meer hebt tot je bitcoin als je de toegang tot je wallet verliest!

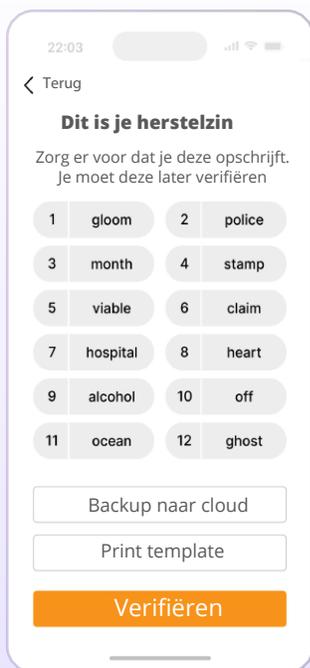
- 3 Je moet dan bevestigen dat je je herstelzin goed hebt opgeslagen. Om dit te doen, moet je opnieuw jouw herstelzin invoeren.
- 4 Als extra beveiligingsmaatregel kun je bij sommige wallets aanvullend nog een wachtwoord kiezen. Je private key en eerste bitcoinadres worden nu automatisch voor je aangemaakt door je wallet.

Je kunt bitcoinadres(sen) vergelijken met je e-mailadres - dit kan je delen met anderen zodat ze je bitcoin naar je kunnen sturen, of in het geval van een e-mailadres, een e-mail.

Je private key is vergelijkbaar met het wachtwoord van je e-mailaccount. Dit wil je met niemand delen omdat ze dan toegang krijgen tot je e-mail.

- 5 Nu kun je bitcoins ontvangen op je bitcoinadres. Met een self-custodial wallet kun je niet altijd direct bitcoin kopen met fiatgeld, dus moet je het misschien eerst kopen bij een exchange en dan overboeken naar je wallet.

Hoe gebruik ik bitcoin?



Oefening in de klas. Optie 2. Wallet herstellen (bij beperkte tijd).

Maak per student een wallet aan en voeg wat satoshis toe.

Geef elke student de herstelzin om deze wallet te herstellen.

Begeleid studenten stap voor stap:

- 1 Wanneer je je wallet voor het eerst start, zie je meestal meerdere methoden om een wallet aan te maken. We gaan nu een bestaande wallet herstellen middels een herstelzin. Tik op [importeer een bestaande wallet] Je ziet nu een introductiescherm, tik op [herstellen met herstelzin].
- 2 Voer de 12 of 24 woorden van de herstelzin één voor één in, in de juiste volgorde.
- 3 Klik op [verifiëren] om de invoer te controleren en daarna op [herstellen] om je wallet te herstellen.
- 4 Je ziet vervolgens "importeren succesvol" als de herstelzin succesvol is geïmporteerd. De wallet is nu hersteld.

7.4 Transacties ontvangen en versturen

Een bitcointransactie is een eigendoms-overdracht van een bestaande hoeveelheid bitcoin naar een nieuwe eigenaar. Maar in plaats van daadwerkelijke munten over te dragen, werken alle nodes in het netwerk hun lokale kopie van het openbare kasboek bij om de verandering in eigendom weer te geven.

Bij het versturen van een bitcointransactie ondertekent de verzender een bericht dat alleen hij kan ondertekenen met zijn privésleutel, waarmee hij aan het netwerk doorgeeft dat het eigendom van de bitcoin wordt overgedragen aan de ontvanger.

Dat wil zeggen dat de bitcoin nu wordt gekoppeld aan een adres vanwaar alleen de nieuwe eigenaar bitcoins kan versturen, waardoor hij of zij eigenaar wordt van de bitcoin.

Kasboek

Eigenaar	Waarde
Sam	2,50
Adam	3,00
Michael	6,00
Jim	1,50
Robert	2,00
Eliana	1,75
Daniel	5,25

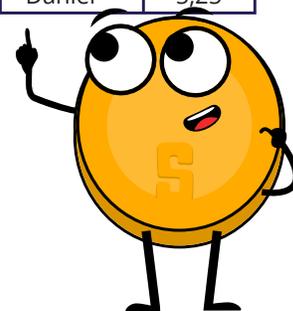


Kasboek

Eigenaar	Waarde
Sam	2,50
Adam	3,00
Michael	6,00
Jim	1,00
Robert	2,00
Eliana	2,25
Daniel	5,25

Nieuwe bitcointransacties worden geïnitieerd vanuit wallets over de hele wereld, maar er is geen centrale betalingsverwerker. In plaats daarvan concurreren miners over de hele wereld om transacties vast te leggen in het kasboek.

In bovenstaande voorbeeld maakt Jim 0,5 BTC over naar Eliana.



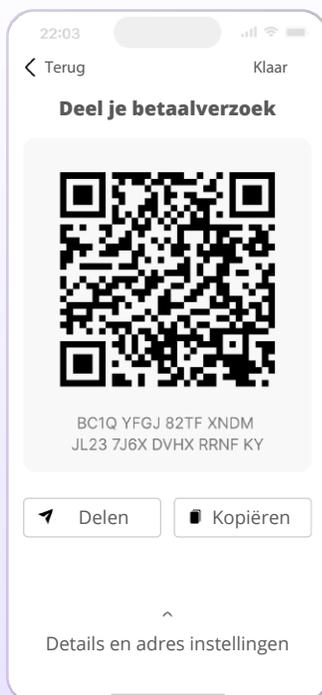
- 1 Eliana deelt haar bitcoinadres met Jim.
- 2 Jim gebruikt zijn wallet om de transactie aan te maken. Deze transactie bevat het bitcoinadres van Eliana, het bedrag (0,5 BTC) en een vergoeding voor de miner.
- 3 Na het ondertekenen van de transactie wordt deze naar het bitcoinnetwerk gestuurd waar deze wordt geverifieerd door de nodes. Nodes controleren de transactie op geldigheid en controleren of Jim genoeg bitcoin heeft. Als dat niet zo is, verwerpen ze de transactie onmiddellijk.
- 4 Zodra de transactie is geverifieerd, wordt deze door miners toegevoegd aan de blockchain en wordt de bitcoin overgemaakt naar het adres van Eliana.
- 5 Eliana kan dan haar private key gebruiken om toegang te krijgen tot de overgemaakte bitcoin in haar wallet.

Het is belangrijk om te weten dat transacties niet meer kunnen worden teruggedraaid.

Hoe een bitcointransactie werkt



Bitcointransacties ontvangen:



Om bitcoin te ontvangen, moet de afzender je bitcoinadres weten. Dit is een unieke reeks letters en cijfers die je wallet aanmaakt en is uniek op het bitcoinnetwerk. Je kunt je bitcoinadres vinden door in te loggen op je bitcoinwallet en te zoeken naar een optie om bitcoin te "Ontvangen" of "Versturen".

Je kan op verschillende manieren je bitcoinadres delen met de afzender:

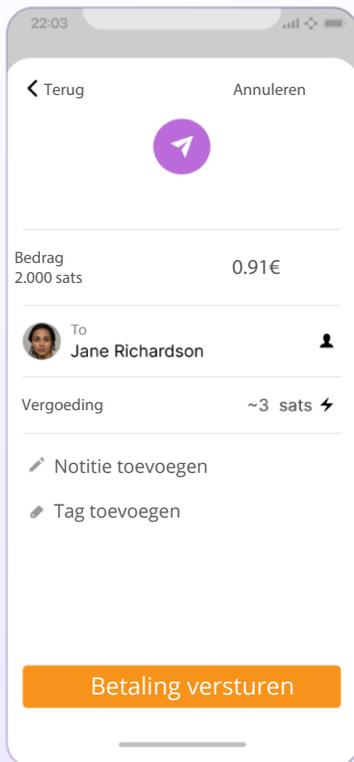
- 1 Kopieer en plak het adres: Je kunt het adres kopiëren door het te markeren en op "CTRL+C" op je toetsenbord te drukken, en het vervolgens te plakken via CTRL+V in een e-mail of bericht aan de afzender.
- 2 Deel een link naar je bitcoinwallet: Bij sommige bitcoinwallets kun je via een link je bitcoinadres delen met de verzender.
- 3 Deel een QR-code: Als de afzender een smartphone heeft met een bitcoinwallet app, kan hij de QR-code scannen om jouw bitcoinadres te krijgen.

Hoe gebruik ik bitcoin?

Zodra de verzender je bitcoinadres heeft, kan hij bitcoin naar je sturen door dit adres en het bedrag in te voeren en de transactie te starten. De bitcoin wordt dan naar je wallet gestuurd en is zichtbaar zodra de transactie is bevestigd op het bitcoinnetwerk. Dit duurt meestal een paar minuten, afhankelijk van de drukte op het bitcoinnetwerk.

Hieronder kijken we hoe het versturen van bitcointransacties via een wallet verloopt.

Bitcointransacties versturen:



Om bitcoin te versturen heb je een paar dingen nodig: een bitcoinwallet, het adres van de ontvanger en de hoeveelheid bitcoin.

- 1 Open je bitcoinwallet. Soms wordt er ter controle een SMS naar je telefoonnummer gestuurd met een code die je moet invoeren in het dialoogvenster. Als je Google 2FA hebt ingeschakeld, moet je de zescijferige code van de Google Authenticator app invoeren.
- 2 Kopieer het bitcoinadres van de ontvanger. Navigeer naar de functie "Versturen" of "Verzenden".
- 3 Plak het bitcoinadres van de ontvanger in het veld "Aan".
- 4 Voer het bedrag in dat je wilt versturen in het veld "Bedrag".
- 5 Controleer het adres van de ontvanger en het te versturen bedrag.
- 6 Voordat je op "Betaling versturen" klikt, raden we je aan om de transactiegegevens nog een keer te controleren om er zeker van te zijn dat je het juiste bedrag naar het juiste bitcoinadres stuurt.
- 7 Verstuur de transactie en wacht tot het bitcoinnetwerk de transactie bevestigt.

Nu weet je hoe je een self-custodial bitcoinwallet moet beoordelen, selecteren en gebruiken. Bitcoin versturen van de ene wallet naar de andere op het bitcoinnetwerk wordt een "on-chain-transactie" genoemd. Dit komt omdat de transactie plaatsvindt op de blockchain van het bitcoinnetwerk. On-chain-transacties zijn de veiligste manier om transacties te doen met bitcoin, maar de transacties zijn duurder en langzamer dan andere opties die we zullen bespreken in hoofdstuk 8.

Activiteit: bitcointransacties in de praktijk

Doel: de onderliggende concepten en mechanismen van peer-to-peer bitcointransacties begrijpen.

Hieronder een korte herinnering aan de hoofdrolspelers in een bitcointransactie:

- Afzenders en ontvangers zijn de partijen die transacties met elkaar willen doen.
- Nodes valideren transacties en slaan een volledige kopie van de blockchain op.
- Miners zijn verantwoordelijk voor het toevoegen van nieuwe transacties aan de blockchain.

In deze oefening krijg je een van de volgende rollen toegewezen: verzender, ontvanger, node of miner.

-  Verzenders zijn verantwoordelijk voor het maken en broadcasten van transacties.
-  Ontvangers zijn verantwoordelijk voor het ontvangen en verifiëren van transacties.
-  Nodes valideren de transacties door te controleren of de transactie geldig is.
-  Miners zijn verantwoordelijk voor het toevoegen van de transacties aan de blockchain.

Zowel nodes als ontvangers moeten transacties verifiëren

 Een verzender: jij maakt een transactie aan.

Volg deze stappen om een transactie aan te maken: neem een transactienota en schrijf het aantal munten op dat je wilt versturen en de naam of initialen van de ontvanger. Onderteken het briefje met je naam of initialen, waarmee je een private key simuleert. Geef het transactiebriefje aan de ontvanger.

 Een ontvanger: jij bent verantwoordelijk voor het verifiëren van de transacties.

-  Controleer op de transactienota of het juiste aantal munten en de naam of initialen van de ontvanger zijn geschreven.
-  Tel de ontvangen munten en vergelijk ze met het aantal munten dat op het briefje staat.
-  Als de munten overeenkomen, vink je het goedkeuringsvakje aan. Als de munten niet overeenkomen of als je twijfelt, wijs de transactie dan af.

Munten verstuurd	Verzender	Verzender handtekening	Ontvanger	Datum & tijd	Ontvanger goedkeuring

 Een node: jij bent verantwoordelijk voor het verifiëren en valideren van de transacties.

-  Controleer of het adres van de afzender geldig is en of het adres van de ontvanger geldig is.
-  Controleer of de verzender genoeg munten heeft om de transactie te voltooien en of de transactie geen munten dubbel uitgeeft.

Munten verstuurd	Verzender	Verzender handtekening	Ontvanger	Datum & tijd	Node goedkeuring

Hoe gebruik ik bitcoin?

4 Een miner: jij bent verantwoordelijk voor het toevoegen van de transacties aan de blockchain.

- Controleer de transacties die zijn goedgekeurd door de ontvangers en gevalideerd door de nodes.
- Gooi de dobbelstenen en vergelijk de getallen met die van de andere miner. De miner met het kleinste getal voegt de transactie toe aan de blockchain.
- Voor je tijd, energie en moeite verdien je een punt. De miner met de meeste punten wint.

** Als een transactie eenmaal aan de blockchain is toegevoegd, kan deze niet meer worden veranderd of teruggedraaid.

5 Houd gedurende de activiteit je muntsaldo bij door de munten in je digitale wallet te tellen.

Munten verstuurd	Verzender	Verzender handtekening	Ontvanger	Datum & tijd	Goedkeuring

6 Bespreek de geleerde concepten met je klas.

7.5 Sparen in bitcoin

Bitcoin is een manier om je geld te beschermen tegen inflatie en, als je het goed doet, ook te beschermen tegen controle door iemand anders. Sparen in bitcoin is een middel om over de lange termijn waarde op te slaan en op te bouwen. Zoals je inmiddels begrijpt, is het soort geld dat je kiest om te sparen een van de belangrijkste beslissingen die je kunt nemen. Door verstandig te kiezen kun je een betere toekomst opbouwen voor jezelf en je naasten.



Gemoedsrust: Als bitcoin op de juiste manier wordt bewaard, is het de enige vorm van eigendom die niemand je kan afnemen



7.6 Don't trust, verify

Wat je ook doet in bitcoin, onthoud dit: "Don't Trust, Verify". Er zijn geen leiders in bitcoin. Je moet nooit blindelings iemands beweringen volgen. In plaats daarvan moet je altijd vragen stellen bij wat je verteld wordt en het voor jezelf verifiëren. Door dit mantra te volgen, bescherm je jezelf tegen het verliezen van je bitcoin. Dit geldt net zo goed voor beweringen als "dit is de volgende bitcoin", of voor "investeringsmogelijkheden" of beloften van "snelle en gemakkelijke winsten".

Samengevat heeft hoofdstuk 7 je de belangrijke vaardigheden gegeven om bitcoin in je dagelijks leven te gebruiken. Je hebt geleerd hoe je bitcoin op verschillende manieren kunt verkrijgen, ontvangen en versturen, en hoe je het veilig kunt bewaren met behulp van verschillende wallets.

Door je mobiele bitcoinwallet in te stellen en transacties met anderen uit te voeren, heb je nu praktijkervaring opgedaan om bitcoin vol vertrouwen dagelijks te gebruiken. Als je begrijpt dat bitcoin een manier is om geld te sparen en het idee van "Doe Je Eigen Onderzoek (DYOR) - Don't Trust, Verify" volgt, heb je nu controle over je geld.

In het volgende hoofdstuk verkennen we het lightningnetwerk. We bekijken hoe deze innovatieve technologie de manier verandert waarop mensen wereldwijd toegang hebben tot geld en hoe ze het gebruiken, van alledaagse transacties tot meer geavanceerde toepassingen. Je zult leren hoe het lightningnetwerk individuen, gemeenschappen en bedrijven in staat stelt om toegang te krijgen tot financiële diensten.

Hoofdstuk #8

Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

8.0 Inleiding

Activiteit: bekijk deze video over het lightningnetwerk

8.1 Het lightningnetwerk

8.2 Verschillende soorten lightningwallets

8.2.1 Self-custodial versus custodial wallets

8.2.2 Open-source versus closed-source

8.3 Een bitcoin lightningwallet opzetten

8.4 Ontvangen en versturen van lightningtransacties

Activiteit: lightningwalletestafette

8.5 Koffie en boodschappen kopen met bitcoin

8.5.1 Online: payment plugins - E-commerce

8.5.2 Persoonlijk: zoek een winkelier bij jou in de buurt

8.5.3 Overgangshulpmiddelen: vouchers, cadeaubonnen en betaalkaarten

8.5.4 Circulaire economieën en bitcoin als ruilmiddel

Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

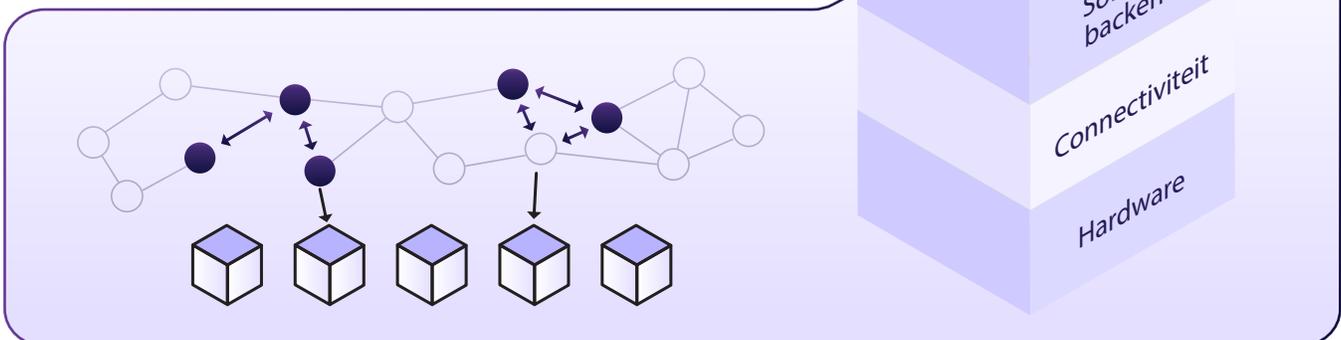
8.0 Inleiding

We bouwen het Visa-netwerk voor bitcoin. Maar wat ik er krachtig aan vind, is dat iedereen er op kan bouwen, in tegenstelling tot Visa

Elizabeth Stark

Technologieën groeien meestal in lagen, als een stapel. Denk aan je favoriete website, e-mail of sociale media: ze zijn gebouwd bovenop het internetprotocol, dat werd gebouwd bovenop computersystemen, die werden gebouwd bovenop het elektriciteitsnet, enzovoort. Deze technologieën begonnen met een heel eenvoudig ontwerp en werden in de loop der tijd steeds beter.

Bitcoin is geen uitzondering. Zoals Andreas Antonopoulos het beroemd zei: "bitcoin is het internet van geld". Het is de basislaag van eerlijk digitaal geld en biedt een solide basis waarop nieuwe technologie gebouwd zal worden.

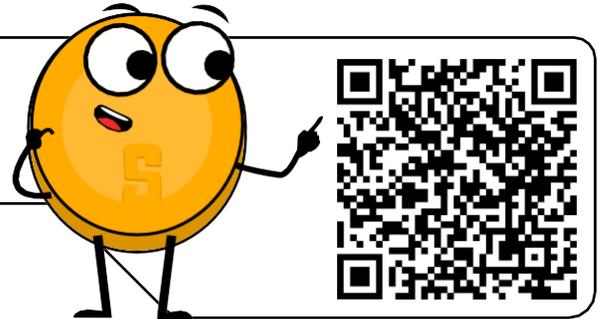


Een van deze lagen heet het lightningnetwerk. Het lightningnetwerk is als een supersnelle snelweg voor bitcoin. Het helpt mensen om bitcoin heel snel en tegen zeer lage kosten te versturen en te ontvangen. Het stelt gebruikers in staat om onmiddellijke, kleine transacties te doen bovenop het gewone bitcoinnetwerk. Dit maakt het kopen van een kopje koffie of het betalen van een vriend eenvoudig en snel!

Onthoud: Een satoshi is als de kleinste munt van bitcoin. Net zoals een euro opgesplitst kan worden in centen, kan een bitcoin worden opgesplitst in kleinere eenheden die satsoshis worden genoemd. Eén bitcoin is gelijk aan 100 miljoen satoshi's, waarbij een satoshi het kleinste stukje waarde in het bitcoinsysteem vertegenwoordigt. Wanneer we het hebben over het versturen van bitcoin via het bitcoin lightningnetwerk, dan noemen we het ook wel "sats versturen". Gewoon kleinere delen van een bitcoin.

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

Activiteit: Bekijk deze video over het lightningnetwerk



8.2 Het lightningnetwerk

Zoals we net hebben gezien, dient het bitcoin lightningnetwerk als een betalingssysteem dat snelle en goedkope transacties met bitcoin mogelijk maakt. Het werkt door het opzetten van een gedeelde wallet waarin beide partijen bitcoin bezitten. Ze kunnen onderling talloze transacties uitvoeren zonder dat ze die allemaal hoeven vast te leggen in het kasboek. Het eindsaldo wordt dan geregistreerd op het kasboek zodra de transacties zijn voltooid.



Het lightningnetwerk is een betalingssysteem waarmee gebruikers snel en goedkoop betalingen kunnen ontvangen en versturen met bitcoin. Het werkt door het opzetten van een gedeelde wallet waar beide mensen hun bitcoins opslaan en dan onbeperkt onderlinge transacties doen zonder de bitcoinblockchain te gebruiken. Als ze klaar zijn, wordt het eindsaldo geregistreerd op de blockchain.

Stel je een dag in een café voor. Met een verblijf van een hele dag in het vooruitzicht, open je een rekening en betaal je wat geld vooruit in plaats van elke keer te betalen als je iets bestelt. Als je aan het eind van de dag klaar bent om te vertrekken, bekijken jij en de eigenaar de rekening om af te rekenen. Als je meer hebt betaald dan je werkelijke consumptie, krijg je wat geld terug.

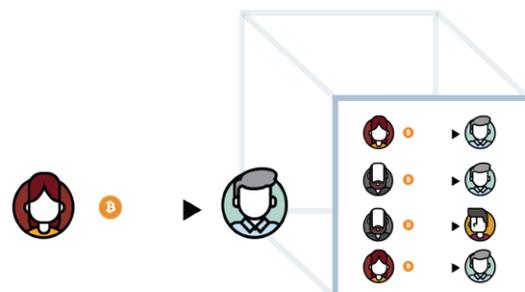
Stel je nu voor dat duizenden mensen tegelijkertijd hetzelfde doen en dat anderen hun rekeningen kunnen gebruiken om met meer mensen in contact te komen. Dat is het lightningnetwerk!

Met lightning kun je betalingen doen aan iedereen op het netwerk, niet alleen aan de persoon met wie je direct een rekening deelt. Je betaling kan door het netwerk navigeren totdat het zijn bestemming bereikt, zelfs als je geen open kanaal hebt met de ontvanger.

Laten we eens kijken naar het verschil tussen on-chain-transacties (het type dat we in hoofdstuk 7 hebben besproken) en off-chain-transacties (via het lightningnetwerk):

On-chain transacties

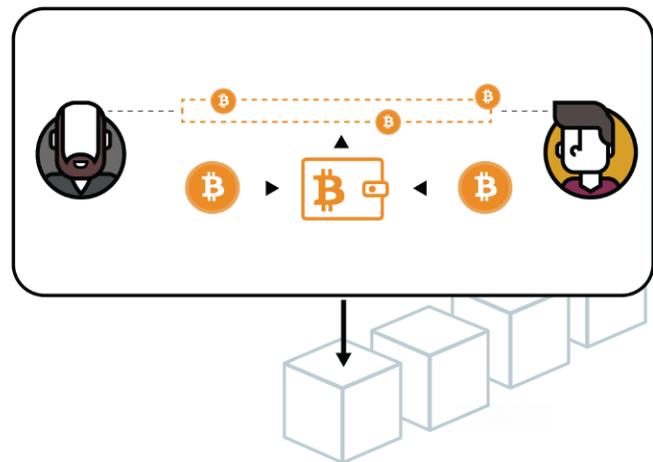
Dit zijn transacties die direct op de bitcoinblockchain plaatsvinden. Het duurt ongeveer 10 minuten om ze te bevestigen en de kosten zijn afhankelijk van de grootte van de transactie in bytes. Ze zijn veiliger maar langzamer.



Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

Off-chain-transacties (lightningnetwerk)

Deze transacties vinden plaats op een apart netwerk dat bovenop de bitcoinblockchain is gebouwd. Ze worden sneller en tegen lagere kosten afgehandeld. Ze worden vaak gebruikt waar regelgeving en wetten het gebruik ervan ondersteunen en waar eigenschappen als de snelheid en kosten van transacties belangrijker zijn. Vergeleken met transacties on-chain zijn ze minder veilig.



Betaal netwerk	Bitcoin netwerk	Lighting netwerk
Definitie	Een gedecentraliseerd digitaal netwerk dat cryptografie gebruikt om financiële transacties te beveiligen.	Een betalingsprotocol voor de tweede laag dat bovenop de bitcoin blockchain werkt en snellere en goedkopere transacties mogelijk maakt.
Voordelen	Gedecentraliseerd en veilig. Geen terugboekingen of fraude. Kan anoniem worden gebruikt. Wereldwijde acceptatie	Snellere en goedkopere Transacties. Verhoogde schaalbaarheid. Off-chain transacties voorkomen grote drukte op de blockchain.
Nadelen	Relatief trage transactietijden. Hoge kosten voor bepaalde soorten transacties. Complex voor beginners	Vereist vertrouwen in de beheerders van het kanaal. Nog experimenteel en weinig gebruikt. On-chain transacties nodig om kanalen te openen en te sluiten.

Samengevat: het lightningnetwerk maakt vrijwel onmiddellijke transacties mogelijk met extreem lage kosten, terwijl bitcointransacties erg veilig zijn, maar wel langzamer en duurder.

8.2 Verschillende soorten lightningwallets

Een lightningwallet is iets anders dan een bitcoinwallet, hoewel het dezelfde functie heeft: bitcoin ontvangen en versturen. Het verschil is dat je met een lightningwallet bitcoin kunt versturen op het lightningnetwerk, wat een tweede laag is bovenop het bitcoinnetwerk.

Net zoals we in het vorige hoofdstuk zagen met bitcoinwallets, hebben lightningwallets verschillende kenmerken waar je rekening mee moet houden voordat je er een kiest.

8.2.1 Self-custodial versus custodial wallets

Lightningwallets kunnen worden onderverdeeld in zeer specifieke categorieën, maar voor de eenvoud zullen we ze in tweeën delen: self-custodial en custodial wallets.

Net als bitcoinwallets is een self-custodial lightningwallet er een waarbij jij de keys van de wallet beheert, terwijl een custodial lightningwallet er een is waarbij iemand anders de sleutels beheert.

Als je een custodial wallet gebruikt, ben je afhankelijk van iemand anders voor toestemming om je geld te gebruiken. Je ruilt het eigendom van je geld voor gemak.

Dit kan acceptabel zijn voor kleine bedragen, maar het is aan te raden om een self-custodial wallet te gebruiken zodra je de technologie begrijpt.

Hieronder hebben we het alleen over Self-custodial lightningwallets.

8.2.2 Open-source versus closed-source

Net als de bitcoinwallets die we in het vorige hoofdstuk hebben gezien, kunnen lightningwallets open-source of closed-source zijn. Gebruik altijd open-source wallets, omdat deze volledig open zijn en kunnen worden doorgelicht door de gemeenschap.

Een open-source toepassing wil ook zeggen dat iedereen kan bijdragen aan de verbetering van de software, waardoor het een betere keuze kan zijn voor de gebruikers.

8.3 Een bitcoin lightningwallet opzetten

Het opzetten van een self-custodial bitcoin lightningwallet is hetzelfde als het opzetten van een self-custodial on-chain bitcoinwallet.

Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

Oefening in de klas. Optie 1. Download een nieuwe self-custodial wallet.

Hoe je een lightningwallet maakt en gebruikt.

- 1 Zoek naar de app in de App Store (iOS) of Google Play Store (Android).
- 2 Open de app en typ de 12 of 24 woorden van je herstelzin in (ook wel een seed phrase genoemd). Zorg ervoor dat je deze opschrijft en op een veilige plek bewaart! Met deze herstelzin kun je indien nodig weer volledige toegang krijgen tot je geld.

Onthoud dat als je deze reeks woorden verliest of vergeet, je geen toegang meer hebt tot je bitcoin als je de toegang tot je wallet verliest!

- 3 Bevestig dat je je herstelzin (seedphrase) goed hebt opgeslagen. Om dit te doen, moet je in dezelfde volgorde de woorden van je herstelzin invoeren.
- 4 Als extra beveiligingsmaatregel kun je bij sommige wallets een wachtwoord kiezen. Je private key en eerste bitcoinadres worden automatisch voor je aangemaakt door je wallet.
- 5 Genereer een lightninginvoice (soort van factuur), adres of QR-code om bitcoin te ontvangen. Met een self-custodial wallet kun je niet altijd direct bitcoin kopen met fiat, dus moet je het via bijvoorbeeld een exchange kopen en dan overboeken naar je wallet.

Je herstelzin

Je gebruikt je herstelzin om je account te genereren en te herstellen.

- | | | | | |
|----------|------------|----------|----------|-----------|
| 1 Issue | 2 Flame | 3 Sample | 4 Lyrics | 5 Find |
| 6 Vault | 7 Scissors | 8 Banner | 9 Cute | 10 Damage |
| 11 Civil | 12 Goat | | | |

Schrijf deze 12 woorden alsjeblieft op een stuk papier. De volgorde is belangrijk. Deze herstelzin maakt het mogelijk om je account te herstellen.

*Opgelet: als je een custodial wallet gebruikt, hoef je sommige stappen in paragraaf 8.3 niet te volgen. Het gebruik van een custodial wallet brengt risico's met zich mee, omdat je geen controle hebt over je private key, wat betekent dat je geen controle hebt over de bitcoins die je in je wallet bewaart.

Nu we onze bitcoinwallet hebben gecreëerd, gaan we kijken naar het ontvangen en versturen van lightningtransacties, en hoe deze verschillen van de on-chain transacties die we in hoofdstuk 7 hebben verstuurd.

8.4 Lightningtransacties ontvangen en versturen

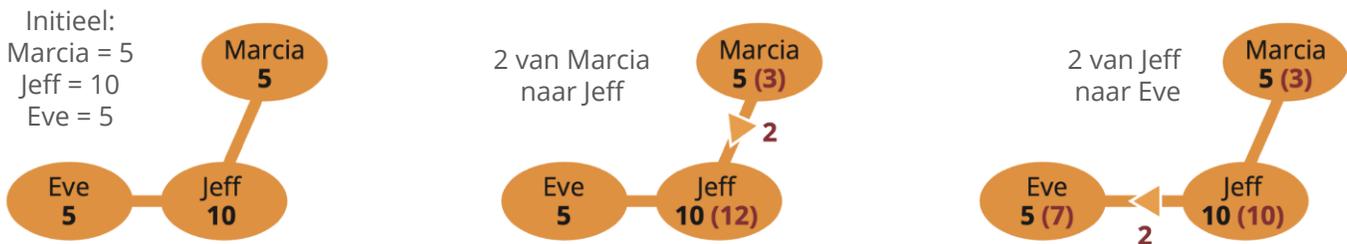
Met een lightningwallet is het gebruik van bitcoin snel, goedkoop en privé, waardoor transacties tussen mensen eenvoudig zijn. Je kunt snel bitcoin versturen en ontvangen voor alledaagse dingen zoals het kopen van koffie of winkelen.

Laten we eens kijken naar een paar voorbeelden van het lightningnetwerk in actie:

Voorbeeld 1:

Hieronder heeft Marcia 5 eenheden van een bepaalde valuta en Eve heeft ook 5 eenheden. Marcia wil 2 van haar eenheden naar Eve sturen, dus stuurt ze 2 eenheden naar Jeff. Jeff geeft vervolgens de 2 eenheden door aan Eve, die nu 7 eenheden heeft. Marcia heeft nu 3 eenheden. En dat is het! De transactie is voltooid.

Het belangrijkste punt hier is dat Marcia en Eve niet via een bank of andere tussenpersoon hoeven te gaan om de transactie te laten plaatsvinden.



Jeff treedt op als tussenpersoon of "vertrouwde derde partij" in dit scenario, waarin Marcia en Eve elkaar niet direct vertrouwen. Jeff ontvangt de 2 eenheden van Marcia en geeft ze door aan Eve, waardoor de transactie kan worden voltooid. Door Jeff als tussenpersoon te gebruiken, kunnen Marcia en Eve de transactie voltooien zonder tussenkomst van een bank of andere gecentraliseerde instelling, waardoor de transactie sneller, goedkoper en veiliger kan verlopen. Jeff faciliteert dit peer-to-peer transactieproces.

Als exploitant van een node in een lightningnetwerktransactie profiteert Jeff op verschillende manieren:



1 Transactie kosten (fees)

Jeff verdient een kleine vergoeding voor elke transactie die via zijn node verloopt. Dit compenseert hem voor de tijd en moeite die hij steekt in het onderhouden en draaiende houden van zijn node.



2 Netwerk participatie

Door een lightningnode te beheren, neemt Jeff deel aan het netwerk en helpt hij de decentralisatie, veiligheid en stabiliteit ervan te vergroten. Dit kan Jeffs reputatie en geloofwaardigheid als betrouwbare node operator vergroten, waardoor hij een geliefde tussenpersoon wordt voor toekomstige transacties.

Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven



Groei van het lightningnetwerk

Naarmate het lightningnetwerk groeit en meer mensen het gebruiken, neemt het aantal transacties dat via de node van Jeff loopt toe, wat resulteert in meer inkomsten uit transactiekosten.



Verhoging van de netwerkbeveiliging

Jeffs rol als tussenpersoon helpt de veiligheid van het netwerk te verhogen door een extra beschermingslaag toe te voegen tussen Marcia en Eve. Dit kan het vertrouwen van gebruikers in het netwerk vergroten en maakt het aantrekkelijker voor nieuwe gebruikers. Over het algemeen kan het exploiteren van een node in het lightningnetwerk aan Jeff een stabiele bron van inkomsten bieden, evenals de mogelijkheid om bij te dragen aan de groei en ontwikkeling van het netwerk.

Samengevat: on-chaintransacties zijn langzamer maar veiliger. Off-chaintransacties via het lightningnetwerk zijn sneller maar minder veilig. De afweging tussen veiligheid en snelheid is afhankelijk van je persoonlijke behoeften.

Voorbeeld 2:

Mina is een fan van McDonald's. Ze gaat er elke dag ontbijten, lunchen en dineren! Maar omdat er zoveel verschillende betalingsmogelijkheden zijn, weet ze niet zeker welke de beste keuze is. Gelukkig heeft ze wat geleerd over bitcoin en het lightningnetwerk. Na het vergelijken van de tabellen hieronder, twijfelt Mina er niet aan dat ze het beste via lightning kan betalen.

Het lightningnetwerk versus het traditionele bankensysteem

Voordelen	Lightning	Traditionele bankensysteem
Snelheid	Snel	Langzaam
Transparantie	Transparant	Niet transparant
Beveiliging	Veilig	Kwetsbaar
Transactie kosten	Laag	Hoog
Financiële inclusiviteit	Hoog	Beperkt

Voordelen	Lightning	Traditionele bankensysteem
Schaalbaarheid	Hoog	Laag
Privacy	Hoog	Gemiddeld
Interoperabiliteit	Hoog	Laag
Wettelijke naleving	Gemiddeld	Hoog
Kosten-effectiviteit	Hoog	Gemiddeld

VISA, Inc.

 Gemiddeld 1700 transacties per seconde
 Schaalbaar tot 65000 transacties per seconde

Bitcoin on-chain transacties

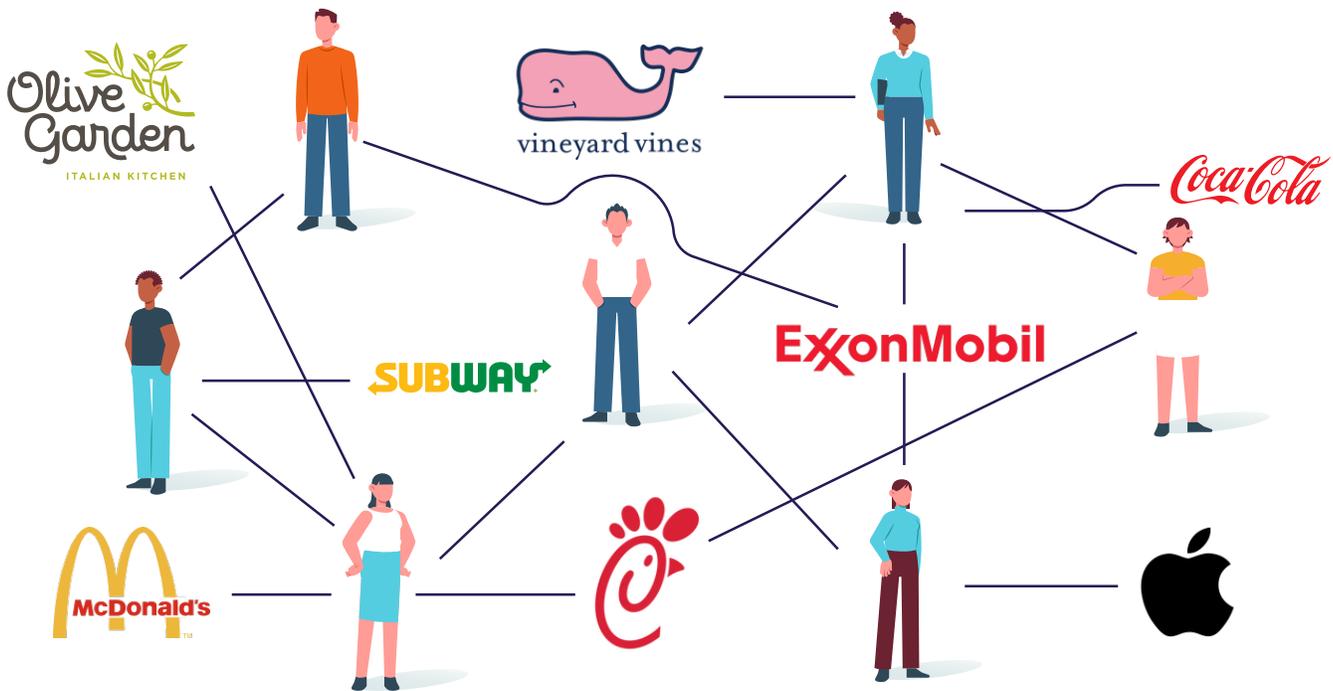
 Schaalbaar tot 7 transacties per seconde


Bitcoin lightningnetwerk

 Schaalbaar tot miljoenen transacties per seconde

Mina is een fan van snelle, veilige en voordelige transacties, dus besluit ze om lightning te gebruiken voor haar aankopen bij McDonald's. Met lightning kan ze nog meer van haar maaltijden genieten in de wetenschap dat haar betalingen onmiddellijk, veilig en tegen lage kosten worden verwerkt. En omdat het lightningnetwerk financiële inclusie biedt, kan Mina zelfs in een afgelegen gebied in El Salvador betalen.

Om te beginnen met lightning downloadt Mina een lightningwallet op haar telefoon. Vervolgens verstuurt ze wat bitcoin van haar gewone wallet naar haar lightningwallet. Dit proces wordt ook wel "funding" of "funding van je betalingskanaal" genoemd. Mina kan haar wallet vullen met elk bedrag aan bitcoin waar ze zich goed bij voelt. Het is belangrijk om te weten dat het bedrag aan bitcoin dat ze in haar lightningwallet opslaat niet kan worden gebruikt in haar on-chain transacties.



Zodra ze de bitcoin op haar lightningwallet heeft gestort, kan ze het gebruiken om betalingen te doen. McDonald's heeft een lightningnode, dus Mina kan een betalingskanaal met hen openen door een deel van haar bitcoin van haar bitcoinwallet naar een specifiek adres van McDonald's te sturen. Dit verplaatst haar bitcoin van de bitcoinblockchain naar een off-chain transactie op het lightningnetwerk.

Nu het betaalkanaal met één bitcoin open is, kan Mina aankopen doen bij McDonald's zonder een nieuw kanaal te hoeven openen of telkens hoge kosten te betalen. Het kanaal blijft open zolang zowel Mina als McDonald's het willen gebruiken. Als Mina bijvoorbeeld een hamburger koopt voor 0,0005 bitcoin, houdt het kanaal bij dat Mina nu 0,9995 bitcoin heeft. En als ze de volgende dag een milkshake koopt voor 0,0003 bitcoin, dan zit er nog maar 0,9992 bitcoin in het kanaal.

Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

Wanneer Mina besluit dat ze haar bitcoin voor iets anders wil gebruiken, sluit ze het kanaal door een sluitingstransactie te versturen naar het bitcoinnetwerk. Dit wordt gedaan door een afsluitende transactie te initiëren vanuit haar lightningwallet. Deze transactie bevat het eindsaldo van het kanaal dat door beide partijen is overeengekomen. De transactie wordt dan gedeeld met het bitcoinnetwerk en wanneer de transactie is bevestigd door een miner, wordt het kanaal gesloten en wordt de resterende bitcoin in het kanaal teruggegeven aan Mina en McDonald's.

Het is belangrijk om te weten dat het sluiten van een kanaal enige tijd kan duren voordat het bevestigd is op de blockchain. Tijdens deze wachtperiode zijn de fondsen vergrendeld in het kanaal en kunnen ze niet worden gebruikt voor on-chain transacties. Mina ontvangt een melding zodra de sluitingstransactie is bevestigd.

Nu we onze lightningwallet hebben ingesteld en hebben gelezen hoe je het lightningnetwerk kunt gebruiken om transacties te versturen, gaan we een spel spelen waarbij we satoshi's (de kleinste eenheden van bitcoin) naar andere studenten in de klas sturen via het lightningnetwerk.



Dit is een kaart van de hele wereld. Met het lightningnetwerk kun je satohis sturen naar elke gebruiker op het netwerk met een lightningwallet. De betaling komt binnen een paar seconden aan en kost maar een paar cent.

Bekijk het zelf:



Activiteit: Oefening in de klas, lightningwalletestafette

- 1 Als eerste moet je een lightningwallet downloaden op je telefoon of computer.
- 2 Volg de instructies voor het installeren van een wallet in paragraaf 8.3 van dit hoofdstuk.
- 3 Zodra de wallet is geïnstalleerd, open je hem en volg je de aanwijzingen om hem in te stellen. Dit kan inhouden dat je een nieuwe wallet aanmaakt of een bestaande wallet herstelt en beveiligt met een wachtwoord of andere vorm van authenticatie.
- 4 Genereer een lightninginvoice, -adres of -QR-code om bitcoin te ontvangen.
- 5 Zodra je wallet is ingesteld en je klaar bent om satoshis te ontvangen, geeft je docent je een startbedrag door ze naar je wallet te sturen.



- A Het doel is om de satoshis door te geven van de ene wallet naar de andere met behulp van het lightningnetwerk, totdat ze de laatste persoon in de groep bereiken.
- B Om satoshis naar iemand anders te sturen, open je je wallet en volg je de instructies voor het doen van een betaling. Je moet de lightninginvoice van de ontvanger opgeven of een QR-code scannen en het bedrag aan satoshis invoeren dat je wilt sturen.
- C Als jouw groep als eerste de satoshis naar de laatste persoon heeft gestuurd, heb je gewonnen! (en mag je de sats houden).

Bespreek eventuele moeilijkheden die je groep had met de activiteit. Was het verzenden van een transactie gemakkelijk, snel en goedkoop? Denk je dat het lightningnetwerk makkelijk te gebruiken en te begrijpen is?

Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

8.5 Koffie en boodschappen kopen met bitcoin

Heb je je ooit afgevraagd of je bitcoin kunt gebruiken om je dagelijkse kopje koffie te kopen of boodschappen in te slaan? Het kan! Er zijn veel opties om, zowel online als in winkels, met bitcoin te betalen. Laten we enkele van die opties bekijken, evenals tools die je kunnen helpen om lokale winkels te vinden waar je bitcoin kunt uitgeven.

Ook al lijkt betalen met een creditcard of een app makkelijk te begrijpen voor degene die betaalt, de verwerking van de betaling is eigenlijk heel complex en er zijn veel verschillende partijen bij betrokken. Hieronder volgt een overzicht van de verschillende partijen:



Bij elke digitale transactie zijn veel partijen betrokken en elke partij brengt kosten in rekening. Deze kosten kunnen voor winkeliers erg hoog zijn, zelfs meer dan 3% van de prijs.

En dan hebben we het nog niet eens over de wisselkosten als er geen lokale valuta wordt gebruikt!

Verwerkingskosten van Creditcards



Met bitcoin en het lightningnetwerk kunnen bedrijven zonder vertraging betalingen ontvangen van over de hele wereld via een open, veilig, internet-native, grenzeloos en censuurbestendig monetair systeem.

We zullen een paar manieren bekijken waarop winkeliers gemakkelijk betalingen in bitcoin kunnen accepteren.

8.5.1 Online: Plug-ins voor betalingen - E-commerce

BTCPayServer is een open-source betalingsverwerker waarmee webwinkeliers met weinig technische kennis betalingen in bitcoin kunnen accepteren. Het is helemaal gratis en rekent geen commissie.

Online bedrijven kunnen BTCPayServer naadloos integreren door de BTCPay plug-in toe te voegen aan hun website.



Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

Omdat BTCPay Server een open-source project is en geen bedrijf, kun je bijdragen aan het project als je meer weet over het project en programmeren.

Kijk op BTCPayServer
<https://btcpayserver.org> voor meer informatie over hoe je dit betaalsysteem kunt gebruiken voor je persoonlijke zaken of online business.

The infographic is titled 'BTCPay Server' and is divided into six colored sections, each with an icon and text describing a feature. The sections are: 1. 'Gratis en open-source' (blue background, green hand icon) - 'Gemaakt om gratis te zijn. MIT-licentie. Geen transactiekosten, abonnementskosten of verwerkingskosten. Volledig open-source. Betalingen zijn direct, peer-to-peer.' 2. 'Decentraal' (green background, network icon) - 'Iedereen kan een server opzetten. Word zelf een betalingsverwerker en ontvang betalingen direct in je wallet. Help je vrienden of gemeenschap en verwerk betalingen voor hen. Een ongelimiteerd aantal winkels kan gekoppeld worden aan één BTCPay Server.' 3. 'Privé, zonder tussenpersoon' (yellow background, people icon) - 'Vertrouwde derde partijen zijn veiligheidsgaten. BTCPay elimineert deze. Betalingen zijn P2P, direct. Gegevens worden niet gedeeld. Er is geen KYC/AML.' 4. 'Bestand tegen censuur' (red background, sad face icon) - 'Geen centraal punt van falen. Niemand heeft de controle behalve de gebruiker die de software runt. Je kunt het draaien op je eigen hardware.' 5. 'Veilig' (blue background, padlock icon) - 'Je private key is nooit vereist. Niet-beheerd. BTCPay heeft alleen de public key (publieke sleutel) nodig om facturen te genereren. Code is open-source en kan geïnspecteerd worden door veiligheidsauditors en ontwikkelaars.' Arrows connect the sections in a clockwise cycle.

BTCPay Server

- Gratis en open-source**
Gemaakt om gratis te zijn. MIT-licentie. Geen transactiekosten, abonnementskosten of verwerkingskosten. Volledig open-source. Betalingen zijn direct, peer-to-peer.
- Decentraal**
Iedereen kan een server opzetten. Word zelf een betalingsverwerker en ontvang betalingen direct in je wallet. Help je vrienden of gemeenschap en verwerk betalingen voor hen. Een ongelimiteerd aantal winkels kan gekoppeld worden aan één BTCPay Server.
- Privé, zonder tussenpersoon**
Vertrouwde derde partijen zijn veiligheidsgaten. BTCPay elimineert deze. Betalingen zijn P2P, direct. Gegevens worden niet gedeeld. Er is geen KYC/AML.
- Bestand tegen censuur**
Geen centraal punt van falen. Niemand heeft de controle behalve de gebruiker die de software runt. Je kunt het draaien op je eigen hardware.
- Veilig**
Je private key is nooit vereist. Niet-beheerd. BTCPay heeft alleen de public key (publieke sleutel) nodig om facturen te genereren. Code is open-source en kan geïnspecteerd worden door veiligheidsauditors en ontwikkelaars.

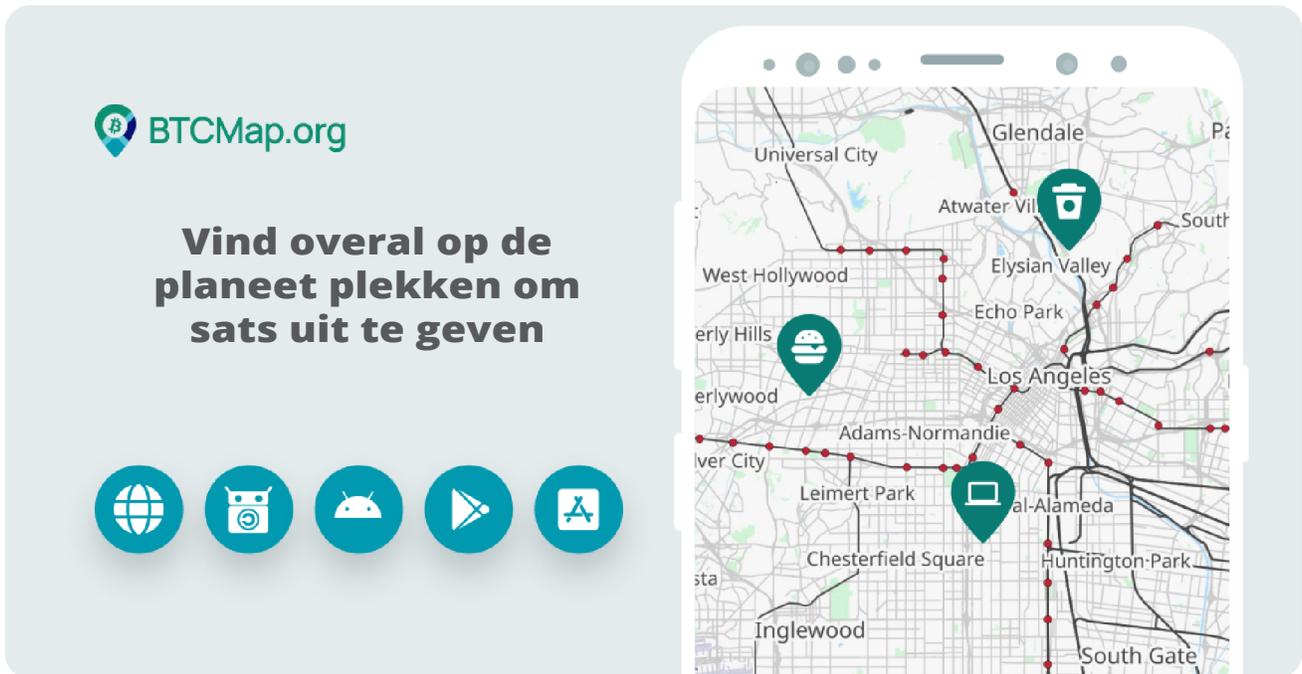
8.5.2 Zoek een winkelier bij jou in de buurt

Fysieke winkels kunnen ook een BTCPayServer gebruiken om betalingen te accepteren, of ze kunnen gewoon een bitcoinwallet downloaden en bitcoin betalingen zonder vertraging vanaf hun telefoon accepteren.



Om een handelaar te vinden die bitcoin accepteert in jouw omgeving, ga je naar BTCMap.org

BTCMap.org is een open-source kaart waarop handelaren die bitcoin accepteren hun bedrijven kunnen vermelden. Het is een handig hulpmiddel voor mensen die hun sats willen uitgeven.



8.5.3 Overgangshulpmiddelen: vouchers, cadeaubonnen en betaalkaarten

Om producten of diensten aan te schaffen bij bedrijven die bitcoin nog niet accepteren, is er een hulpmiddel dat je kunt gebruiken: cadeaubonnen.

Sommige bedrijven richten zich op het kopen en verkopen van cadeaubonnen. Dat betekent dat je met bitcoin een cadeaubon kunt kopen voor de winkel waar je naartoe wilt. Vervolgens kan je de cadeaubon direct uitgeven in die winkel.

Vliegtickets, hotels, games, simkaarten, je kunt bijna alles kopen met bitcoin en cadeaukaarten!

8.5.4 Circulaire economieën en bitcoin als ruilmiddel

Het begrip circulaire bitcoineconomie komt voort uit het idee om afval in een economie te minimaliseren door zoveel mogelijk producten en bijproducten te hergebruiken en te recyclen.

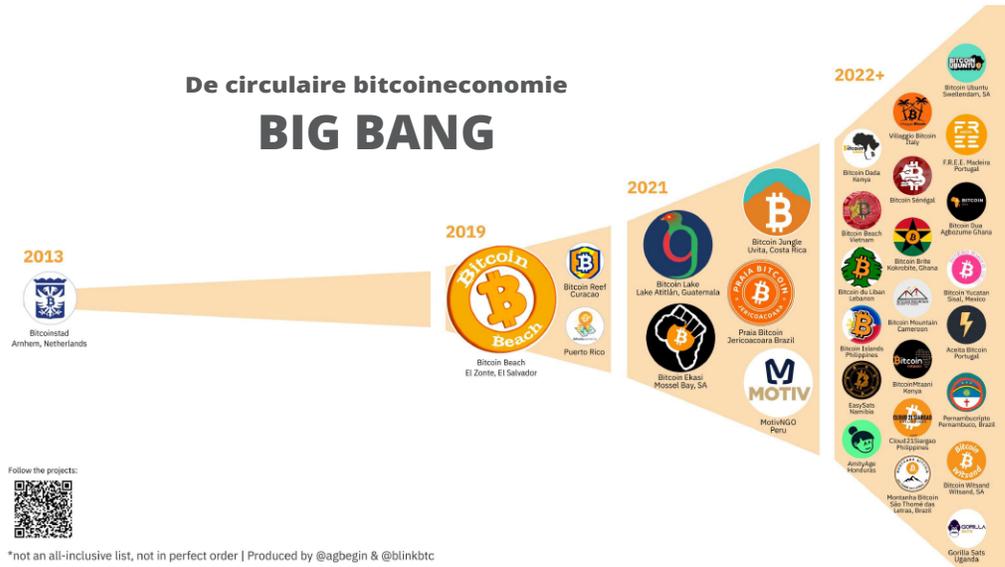
Op basis van dit concept is een circulaire bitcoineconomie er een waar de transacties worden gedaan in bitcoin en waar het geld in de vorm van bitcoin binnen de economie blijft en groeit, zodat individuen en bedrijven ervan kunnen profiteren.



Lightningnetwerk: bitcoin gebruiken in het dagelijkse leven

Dankzij het lightningnetwerk kunnen circulaire bitcoineconomieën overal ter wereld floreren, omdat transacties bijna onmiddellijk plaatsvinden met lage kosten

De eerste circulaire bitcoineconomie ooit werd gevestigd in Arnhem, Nederland. Het werd opgericht lang voordat het lightningnetwerk bestond, maar toen waren de on-chain vergoedingen echt laag!



De tweede was Bitcoin Beach, gevestigd in El Zonte, El Salvador. Het lightningnetwerk maakt het mogelijk dat inwoners zonder banrekening nu digitale betalingen kunnen verrichten via hun smartphones.

Vandaag de dag ontstaan er honderden circulaire economieën over de hele wereld, aangedreven door bitcoin, het lightningnetwerk en educatieve middelen.



Op BTCMap.org kun je ook bitcoingemeenschappen zoeken waar je andere bitcoingebuiters kunt ontmoeten en bedrijven kunt vinden die bitcoin accepteren. Sommige van onze docenten en studenten hebben daadwerkelijk bedrijven en circulaire economieën toegevoegd aan BTCmap.org, en als jij er klaar voor bent, kun jij dat ook!



Vind bitcoincommunities en plekken op de planeet om sats uit te geven



Bron: btcmap.org/communities

Nu we hoofdstuk 8 afsluiten, heb je inzicht gekregen in het gebruik van bitcoin in het dagelijks leven via het lightningnetwerk. Het lightningnetwerk maakt transacties sneller en toegankelijker en biedt een voorproefje van hoe bitcoin in lagen zal blijven veranderen en evolueren.

In hoofdstuk 9 onderzoeken we de technische kant van bitcoin. Van cryptografie tot nodes, miners en meer, maak je klaar om nader te bekijken hoe bitcoin echt werkt.

Hoofdstuk #9

Een introductie tot de technische kant van bitcoin

9.0 Inleiding

Activiteit: bekijk "Hoe bitcoin werkt onder de motorkap"

9.1 Public keys en private keys: beveiliging door cryptografie

9.1.1 Cryptografische public keys en private keys

9.1.2 Uitleg over hashing

Activiteit: genereer een SHA-256 hash

9.2 Het UTXO model

9.3 Bitcoinnodes en miners nader bekeken

9.3.1 Wat is een bitcoinnode en hoe zet ik er een op?

Activiteit: bekijk een video over bitcoinnodes

9.3.2 Wat is een bitcoinminer en hoe werkt mining?

9.4 Wat is de mempool?

Activiteit: mempool

9.5 Hoe bitcointransacties van begin tot eind werken

Activiteit: bitcointransacties in actie

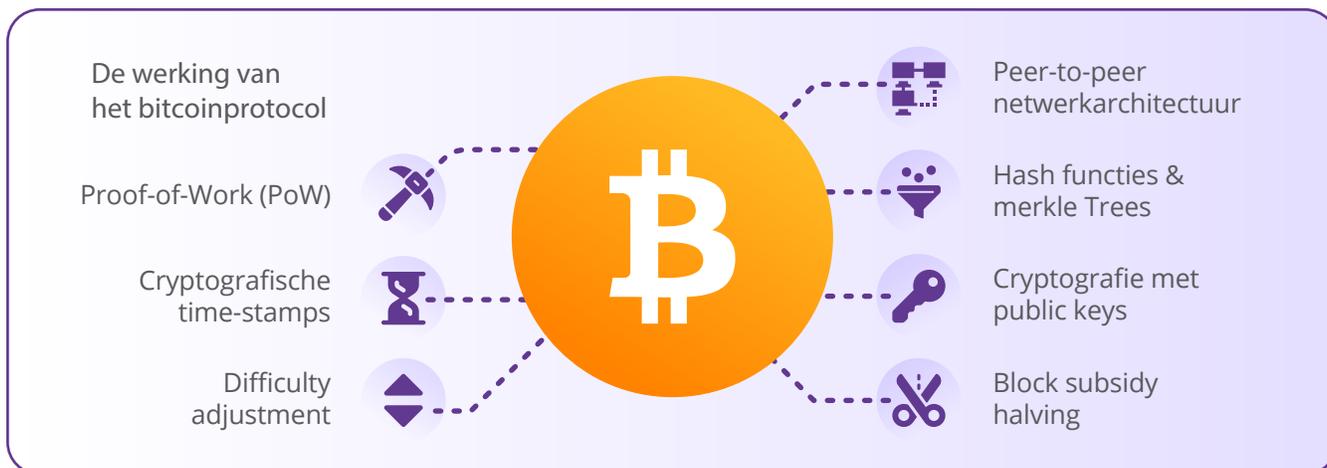
Een introductie tot de technische kant van bitcoin

9.0 Inleiding

Bitcoin is niet "ongereguleerd". Het wordt gereguleerd door een algoritme in plaats van dat het wordt gereguleerd door overheidsbureaucratieën, zonder corruptie.

Andreas M. Antonopoulos

In dit hoofdstuk gaan we dieper in op de technologie die ervoor zorgt dat het bitcoinnetwerk volledig gedecentraliseerd werkt. We leggen op een eenvoudige manier uit wat er gebeurt als je een bitcointransactie verstuurt, hoe deze transacties worden verwerkt en wat miners en nodes doen in het bitcoinnetwerk. We gaan in dit hoofdstuk een aantal uitdagende en technische concepten behandelen. Het is belangrijk om te onthouden dat veel mensen niet begrijpen hoe het internet werkt, maar dat ze het wel elke dag gebruiken om e-mails te versturen, contact te leggen met vrienden op sociale media en zelfs om hun rekeningen te betalen. Het leren van de technische kant van hoe bitcoin werkt is een lange reis die misschien niet iedereen wil maken, zelfs als ze besluiten om het als geld te gebruiken. We moedigen je aan om te blijven leren over de technische aspecten van bitcoin, al beperken we ons in dit hoofdstuk tot de belangrijkste basisbegrippen.



Als je een dieper technisch begrip wilt van hoe bitcoin werkt, hebben we achterin dit werkboek bronnen opgenomen. Je kunt je op onze website ook inschrijven voor Het Bitcoindiploma - Technische Editie om een bericht te krijgen als die meer technische cursus klaar is.

Laten we beginnen met het bekijken van een video die laat zien hoe het bitcoinnetwerk werkt.

Activiteit - bekijk "Hoe bitcoin werkt onder de motorkap".



Zoals je in de video hebt gezien, is het bitcoinnetwerk simpelweg een kasboek of registratie van transacties die is opgeslagen op meerdere computers die nodes worden genoemd. Het bitcoinkasboek is pseudoniem, wat betekent dat het geen persoonlijke gegevens bevat, alleen transactie- en adresinformatie. Het kasboek toont elke bitcoin en zijn bewegingen sinds de start van het netwerk op 3 januari 2009.

Nu gaan we dieper in op de technologie die dit systeem mogelijk maakt.

9.1 1 Public keys en private keys: beveiliging door cryptografie

Bitcoin geeft ons een harde belofte: het programma zal precies zo worden uitgevoerd als gespecificeerd.

Andreas M. Antonopoulos

9.1.1 1 Cryptografische public keys en private keys

Cryptografie is een manier om informatie geheim te houden door het te verhullen in code.



- Encryptie is het proces waarbij informatie wordt omgezet in een speciale code, waardoor het onleesbaar wordt voor iedereen die niet over de juiste decryptiemethode beschikt. Dit is vergelijkbaar met het vergrendelen van een kluis, waarbij alleen de persoon met de juiste sleutel of combinatie deze kan openen.
- Decryptie daarentegen is het proces waarbij de versleutelde informatie weer leesbaar wordt gemaakt, alsof je de kluis ontgrendelt en de toegang krijgt tot de inhoud ervan.

Laten we bijvoorbeeld zeggen dat John een geheim bericht wil sturen naar Peter dat niet bedoeld is voor anderen om te lezen. Ze spreken af om de Pigpen-code te gebruiken om het bericht te verhullen voordat ze het versturen. Alleen degenen met de code kunnen het bericht ontcijferen, waardoor het onleesbaar wordt voor anderen. Hoewel deze methode tegenwoordig niet meer als veilig wordt beschouwd, illustreert het wel het principe van cryptografie met private keys om berichten te versturen.

Hoe werkt cryptografie in bitcointransacties?

In traditionele cryptografie met private keys moeten John en Peter eerst een geheime sleutel delen, zoals een wachtwoord of de Pigpen-code. John zal dan deze sleutel gebruiken om zijn bericht te versleutelen voordat hij het naar Peter stuurt. Peter, die ook de geheime sleutel kent, kan dan dezelfde sleutel gebruiken om het bericht te ontcijferen.

Als iemand anders echter in het bezit is van deze sleutel en het bericht onderschept, kan hij dit bericht ook ontcijferen en lezen.

De Pigpen-code ontcijferen

Bij het oplossen van de Pigpen-code krijgt de speler een versleuteld bericht en een cijfer. Om het bericht te ontcijferen, moet de speler het symbool van het versleutelde bericht op de code vinden om de ontcijferde letter te vinden.

Voorbeeld van een versleuteld bericht:



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

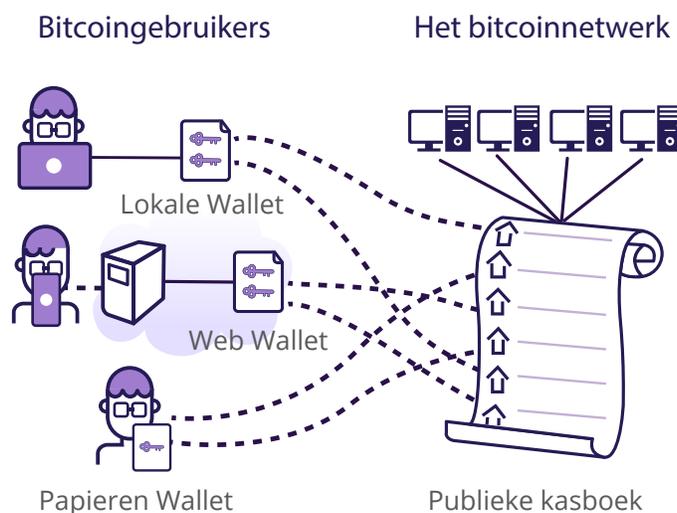
Een introductie tot de technische kant van bitcoin

Cryptografie met **public keys**, het type dat wordt gebruikt bij bitcointransacties, heeft dit probleem opgelost. Met cryptografie op basis van **public keys** hoeven John en Peter het wachtwoord of de versleutelmethode niet met elkaar te delen. In plaats daarvan hebben ze elk twee verschillende sleutels: een **public key** (die je veilig met iedereen kunt delen) en een **private key** (die je geheim moet houden).

In dit geval wil John een bericht naar Peter sturen. Hij gebruikt de **public key** van Peter om zijn eigen bericht te versleutelen voordat hij het naar Peter stuurt. Wanneer Peter het bericht ontvangt, kan alleen hij het ontsleutelen met zijn **private key**. Iemand anders kan het bericht niet lezen, zelfs niet als hij het onderschept. De kans is ook veel kleiner om de sleutel te stelen, omdat zelfs John en Peter de sleutel niet met elkaar hoeven te delen.

Het belangrijkste voordeel van cryptografie met **public keys** ten opzichte van cryptografie met een **private key** is dus dat het veilige communicatie mogelijk maakt zonder dat verzender en ontvanger eerst een geheime sleutel hoeven te delen (of een andere versleutelmethode zoals Pigpen-code), die door een derde partij onderschept zou kunnen worden.

Bij bitcoin wordt cryptografie met public keys niet gebruikt om versleutelde berichten te versturen. In plaats daarvan wordt het gebruikt om unieke **digitale handtekeningen** te maken die bitcointransacties onveranderbaar maken. Een **digitale handtekening** is een manier om de authenticiteit van een bitcointransactie aan te tonen, vergelijkbaar met een handtekening op een fysiek document.



Cryptografie met public keys (voor transacties tussen twee gebruikers):

Elke gebruiker heeft twee sleutels, een **private key** die geheim wordt gehouden en een **public key** die met anderen kan worden gedeeld.

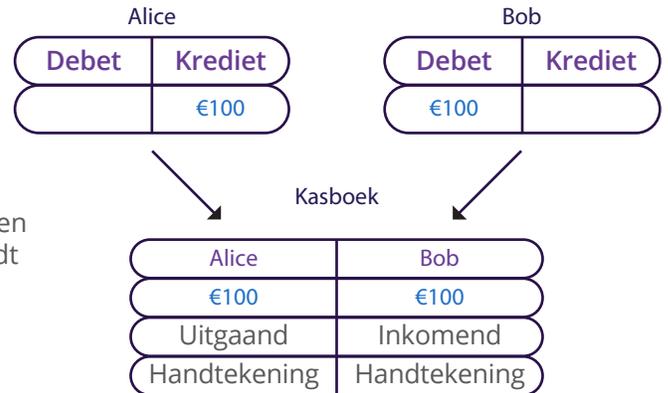
De **private key** dient als een vorm van identificatie en bewijs van eigendom en bevestigt "dit adres is van mij en ik heb er controle over".

Digitale handtekeningen worden gemaakt om unieke transacties te identificeren.

Digitale handtekening



- ☀ Een bitcointransactie houdt in dat iemand een bepaalde hoeveelheid bitcoin rechtstreeks overmaakt aan een ander.
- ☀ Encryptie wordt gebruikt om ervoor te zorgen dat alleen de echte eigenaar van de bitcoin de controle heeft om zijn geld naar iemand anders te sturen. Het zorgt ervoor dat het eigendom wordt beschermd tegen kwaadwillende actoren.
- ☀ Als extra beschermingsmaatregel krijgt elke transactie die je in bitcoin verstuurt automatisch een **unieke handtekening**. Deze **unieke handtekening** wordt mogelijk gemaakt door manipulatiebestendige technologie die het netwerk helpt te verifiëren dat de echte eigenaar van de bitcoin de bitcoin heeft verzonden, en niet iemand anders.



Hoe dit werkt in een echte bitcointransactie?:

- 1 **Bitcointransactie creëren:**
Een gebruiker initieert een bitcointransactie door bepaalde details op te geven zoals het adres van de ontvanger en de hoeveelheid bitcoin die verstuurd moet worden.
- 2 **Digitale handtekening genereren:**
De verzender genereert een unieke **digitale handtekening** met behulp van zijn private key. Deze handtekening is een unieke cryptografische code die de authenticiteit van de transactie bewijst.
- 3 **Transactie "broadcasten":**
De ondertekende transactie wordt als een broadcast verzonden naar het bitcoinnetwerk om aan te geven dat het eigendom van de bitcoin overgedragen moet worden aan de ontvanger.
- 4 **Verificatie op het netwerk:**
Nodes op het bitcoinnetwerk ontvangen de transactie en gebruiken de **public key** van de ontvanger om de transactie te ontsleutelen en de integriteit ervan te verifiëren. Tegelijkertijd gebruiken ze de **public key** van de verzender om de **digitale handtekening** te verifiëren.
- 5 **Bevestiging op het bitcoinnetwerk:**
Als de verificatie succesvol is, wordt de transactie toegevoegd aan het kasboek (ook wel ledger genoemd), dat dient als een veilige, transparante registratie van alle transacties. Na bevestiging is het eigendom van de bitcoin overgedragen van de verzender naar de ontvanger.



Samengevat: een **digitale handtekening** die je maakt met je **private key** dient als cryptografisch bewijs van authenticiteit en eigendom. Pas na ondertekening van een transactie met je **digitale handtekening** kan het bitcoinnetwerk de transactie verifiëren en vastleggen in het kasboek.

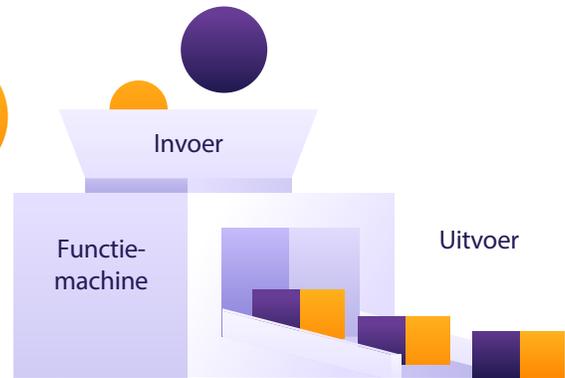
Een introductie tot de technische kant van bitcoin

9.1.2 Uitleg over hashing

Laat je alsjeblieft niet intimideren door de technische termen en wiskundige concepten die voor je liggen. We begrijpen dat niet iedereen gek is op wiskunde, maar misschien verras je jezelf en zie je dat zelfs de meest complexe ideeën met een beetje moeite te begrijpen zijn.

Wat is een functie?

Een functie is zoals een machine die bepaalde informatie verandert in iets nieuws. De informatie die je de functie geeft wordt de **invoer** genoemd. De nieuwe informatie die de functie maakt, wordt de **uitvoer** genoemd. Functies helpen computers om taken uit te voeren en problemen op te lossen.



Vergelijk het met een recept voor het maken van een salade. Het recept (of de functie) vertelt je welke ingrediënten je moet gebruiken en hoe je ze moet mengen om de salade te maken. Je kunt er andere ingrediënten in doen, maar het recept geeft je altijd een salade als resultaat. Functies kunnen worden gebruikt om dingen gemakkelijker en efficiënter te maken.

Dit recept is dus een functie die de ingrediënten als **invoer** neemt en de gemengde salade als **uitvoer** genereert.

In bitcoin worden functies gebruikt om transacties uit te voeren. We weten al dat transacties in bitcoin in wezen overdrachten van waarde (geld) van het ene adres naar het andere zijn. Om een transactie uit te voeren, worden een aantal cryptografische functies gebruikt om de transactie te valideren en het kasboek bij te werken.



De functies die gebruikt worden bij een bitcointransactie zijn onder andere het verifiëren van de authenticiteit van de transactie-invoer, controleren of de verzender voldoende geld heeft en het bijwerken van de tegoeden van de betrokken adressen. Zodra een transactie is geverifieerd en is toegevoegd aan een block in het kasboek, wordt deze onderdeel van de permanente registratie van alle transacties op het netwerk.

Wat is een is eenrichtingsfunctie?

Een eenrichtingsfunctie gebruikt een reeks instructies om de informatie te verwerken en verandert het in iets nieuws, zoals een smoothierecept ingrediënten verandert in een nieuw drankje. Maar net zoals je een smoothie niet kunt 'un-blenden' om de oorspronkelijke ingrediënten terug te krijgen, kun je de eenrichtingsfunctie niet omkeren om de oorspronkelijke informatie terug te krijgen.



Cryptografie met **private keys** en **public keys**, berust op het gebruik van eenrichtingsfuncties, waardoor het moeilijk is om de **private key** uit de public key te bepalen. In theorie is het niet helemaal "onmogelijk" om de **private key** uit de public key te achterhalen, maar het is extreem moeilijk om dit te doen en het zou een buitensporige hoeveelheid tijd en rekenkracht kosten.

Het vinden van een **private key** uit een public key in bitcoin is als het proberen te vinden van een naald in een hooiberg zo groot als een voetbalveld. De naald staat voor de **private key** en de hooiberg voor alle mogelijke **private keys**.

Op dezelfde manier zijn eenrichtingsfuncties ontworpen om onomkeerbaar te zijn en niet ontcijferd te kunnen worden.



Wat is een hashfunctie?

Hashing is als een vingerafdruk voor digitale gegevens. Het is een proces waarbij een digitaal bericht wordt omgezet in een code met een vaste lengte, die dient als een unieke identificatiecode.



Net zoals een vingerafdruk een persoon kan identificeren, kan een hash een digitaal bericht identificeren. Hashes worden in veel toepassingen gebruikt, waaronder bitcointransacties.

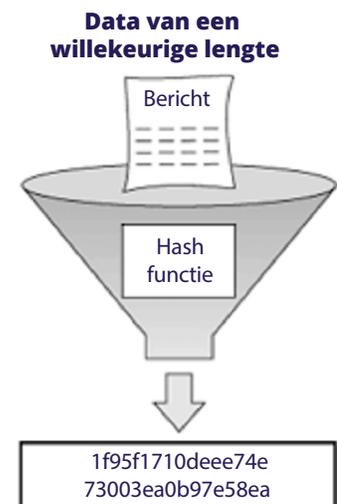
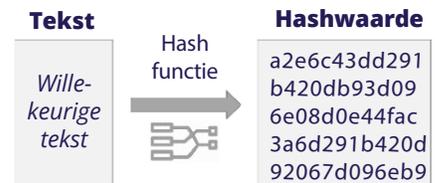
Hoe hashing wordt gebruikt in bitcointransacties

Elke bitcointransactie wordt gehasht voordat deze wordt toegevoegd aan het kasboek. De hash fungeert als handtekening voor de transactie en verifieert dat de transactie geldig is en dat er niet mee geknoeid is. Als iemand zelfs maar één letter in de transactie probeert te veranderen, zal de hash compleet anders zijn en zijn anderen gewaarschuwd.

De rol van hashing in beveiliging

Hashing is essentieel voor de veiligheid van het bitcoinnetwerk. Door hashes te gebruiken voor de identificatie van transacties, kan het netwerk elke poging tot verandering of manipulatie van een transactie detecteren. Dit helpt fraude te voorkomen en zorgt ervoor dat alle transacties nauwkeurig worden geregistreerd in het kasboek.

Een hashfunctie is een soort eenrichtingsfunctie die een **invoer** (aangeduid als het "bericht" of "gegevens") omzet in een uitvoer, in de vorm van een numerieke weergave die een "hash" wordt genoemd. Deze hash is uniek voor de specifieke invoergegevens die zijn gebruikt, dus zelfs een kleine verandering in de invoergegevens resulteert in een compleet andere hash.

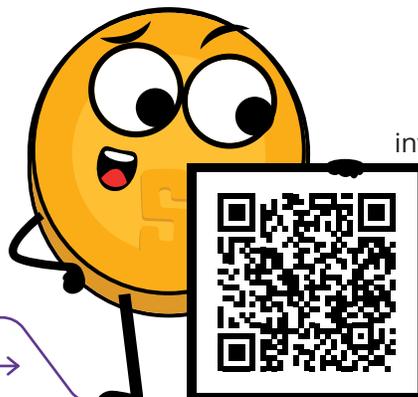


Een hash functie is als een machine die geheime code maakt. Het verandert een normaal **bericht** in een code.



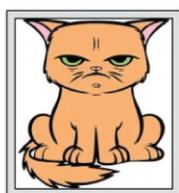
Een introductie tot de technische kant van bitcoin

De code ziet er altijd hetzelfde uit voor hetzelfde bericht. Als je het bericht ook maar een beetje verandert, ziet de code er compleet anders uit. Dit helpt computers dingen te onthouden en te controleren of er iets is veranderd.

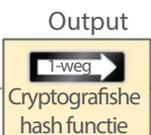


Direct een SHA-256 hash genereren van een willekeurige tekenreeks of invoerwaarde. Hash functies worden gebruikt als eenrichtingsmethoden.

Activiteit: genereer een SHA-256 Hash →



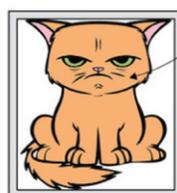
Input
cat.jpg 1.21MB



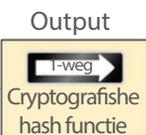
```
e40326f7aa7305  
500fea0a9a2b43  
9ebea93827ba21  
039404439fe33e
```

Een 32-byte hash

Er ontbreekt een
snorhaar in dit plaatje



Input
cat.jpg 1.21MB



```
664eaa3b78f7aa  
7305890e3aab53  
22a0a9a2048bef  
4f8342048b90e3
```

Een volledig andere hash
dan het vorige plaatje

Een 32-byte hash

De **uitvoer** van een hash functie is altijd even lang, ongeacht de lengte van de oorspronkelijke invoer.

Bitcoin gebruikt specifieke hashfuncties: SHA-256 en RIPEMD160. Hieronder een paar voorbeelden:

☀️ Merk op dat een "." in de tweede invoer de uitvoer volledig verandert ten opzichte van de eerste.

☀️ De derde invoer is een enorm bestand, maar de uitvoer heeft nog steeds dezelfde vaste lengte als de andere twee.

De SHA-256 waarde van "hello world"

```
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcded
```

De SHA-256 waarde van "hello world."

```
7ddb22731 5f423250fc67f3be69c544628dffe41752af91 cS0aeQa9c49faeb87
```

De SHA-256 waarde van een groot ISO bestand "Ubuntu 24.04"

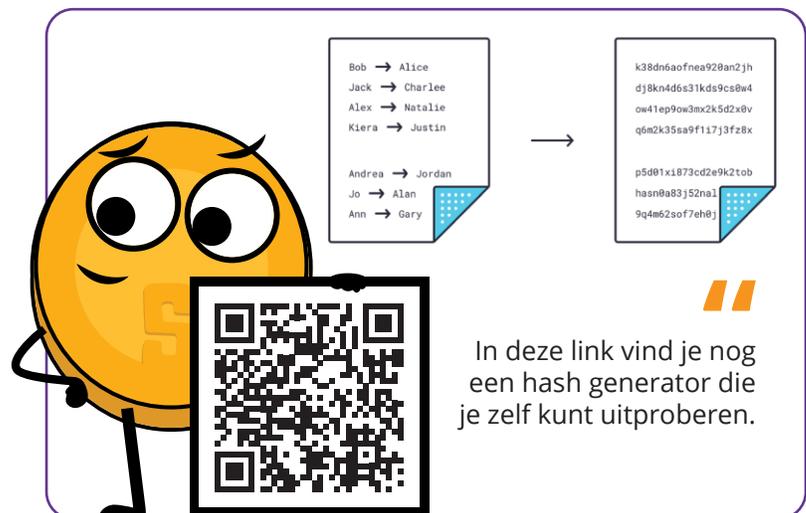
```
7b9f670c749f797a0f7481d61 9ce8807edac052c97e1 a0df3b130c95efae4765
```

Hashing kan ook gezien worden als een partituur die de essentie van een muziekstuk weergeeft. Net zoals dat een partituur een unieke weergave van een muziekstuk is, is een hashwaarde een unieke weergave van een stuk data. Door de partituur van een muziekstuk te vergelijken met de daadwerkelijke uitvoering, kan een muzikant bepalen of de uitvoering accuraat is. Op dezelfde manier kan het vergelijken van de hashwaarde bepalen of de gegevens tijdens de overdracht zijn gewijzigd.



Net zoals dat een kleine afwijking in een muziekuitvoering ervoor kan zorgen dat het vals klinkt, zal zelfs de kleinste verandering in de originele gegevens resulteren in een andere hashing waarde. Dit maakt hashing een krachtig hulpmiddel om de integriteit en authenticiteit van een bitcointransactie te garanderen.

Hashing van **public keys** wordt gebruikt om de veiligheid van informatie te verbeteren door deze om te zetten in een onleesbaar formaat met een vaste lengte. Bitcoin gebruikt de SHA-256 en Ripemd-160 algoritmen om openbare adressen te produceren. De resulterende output dient als een unieke identificatie voor de public key en helpt de integriteit en veiligheid van transacties die zijn opgeslagen in het kasboek te garanderen. Door de informatie op deze manier te versleutelen, wordt het voor onbevoegden moeilijker om toegang te krijgen tot de gegevens en ze te manipuleren.



- Deterministisch**
Dezelfde ingrediënten leveren altijd dezelfde smoothie op.
- Voorafbeeldingsbestendigheid**
Je kunt geen aardbeien meer maken van een smoothie door ze aan elkaar te lijmen.
- Correlatiebestendigheid**
Als je de ingrediënten een beetje verandert, krijg je een heel andere smoothie.
- Botsingbestendigheid**
Het is moeilijk om met andere ingrediënten precies dezelfde smoothie te maken.
- Snelheid en verifieerbaarheid**
Gooi fruit in de mixer. Het gaat snel en het resultaat is zeker een smoothie.

9.2 Het UTXO Model

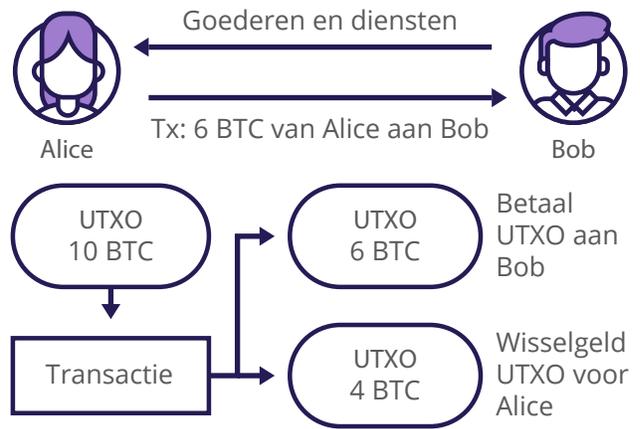


Een introductie tot de technische kant van bitcoin

Wat zijn UTXO's?

Bitcointransacties werken alsof je een groter stuk goud in kleinere stukjes breekt en deze kleinere stukjes zowel naar anderen als naar jezelf stuurt.

Je kunt UTXO's zien als bitcoin in verschillende stukjes, of als biljetten met verschillende waarden in je wallet. Als je een UTXO uitgeeft, wordt het omgezet in een nieuwe UTXO voor de ontvanger, en wat er over is wordt naar je teruggestuurd in een andere nieuwe UTXO die bekend staat als "het wisselgeld UTXO". Dit is net zo iets als wanneer je een biljet van €10 gebruikt om kopjes koffie te kopen voor €6. De winkelier houdt de €6 en geeft je €4 terug als wisselgeld.



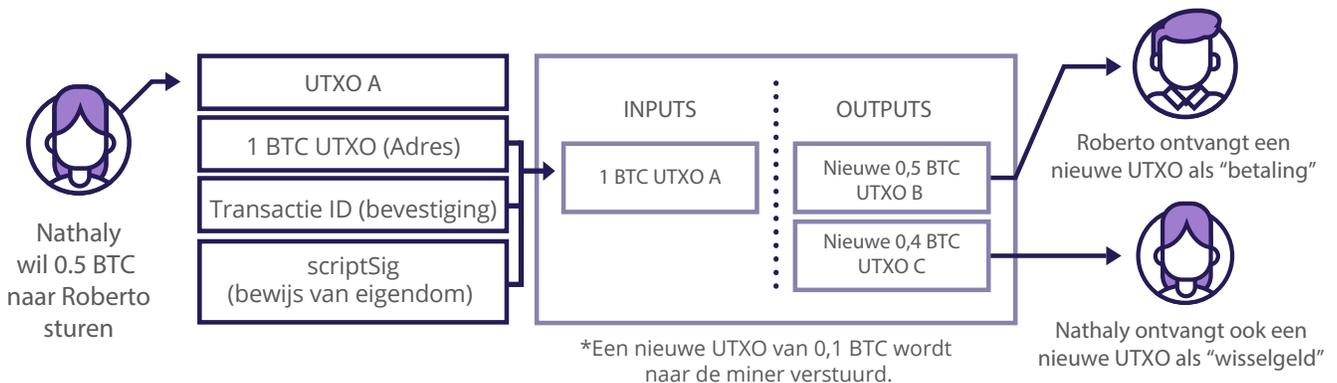
Als je bitcoin verstuurt, dan stuur je altijd het volledige bedrag van één (of meer) van je UTXO's in je wallet. Wat gebeurt er dan? Je stuurt een deel naar de ontvanger en je ontvangt het resterende bedrag terug als wisselgeld op een van de bitcoinadressen die je bezit. Het wisselgeld dat je terugkrijgt heet een UTXO (Unspent Transaction Output) en kan gebruikt worden als input voor een nieuwe toekomstige transactie.

Het saldo van je bitcoinwallet is de som van al je verschillende UTXO's. De som van je UTXO's is dus de som van de hoeveelheid bitcoin die je bezit.

Het is belangrijk om te weten dat je anderen niet op de hoogte moet stellen van je UTXO's, want als iemand je UTXO's kent, kan hij je bitcointransacties in het netwerk volgen en uiteindelijk weten hoeveel geld je bezit.



Samenvattend: elke keer dat je een transactie doet, gebruik je een of meerdere van je bestaande UTXO's om bitcoin uit te geven en worden er nieuwe UTXO's aangemaakt (voor zowel jou als de ontvanger).

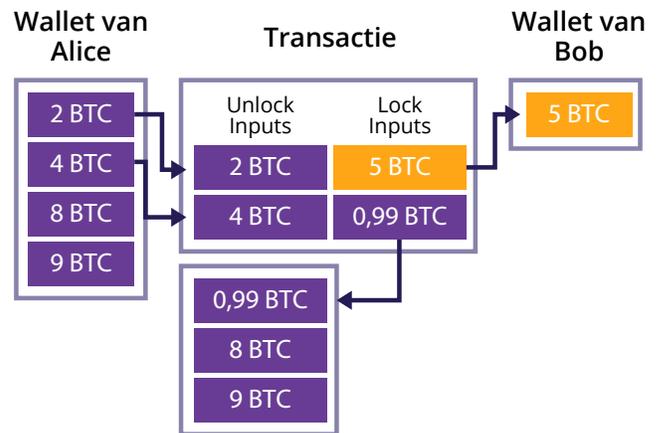


Bij elke transactie wordt de hoeveelheid bitcoin die wordt verzonden verdeeld in meerdere 'outputs', die elk worden gekoppeld aan een nieuw bitcoinadres (een nieuwe UTXO).

Als je naar iemand bitcoin verstuurt, gebruik je een of meerdere UTXO's als geldbron (input). Deze UTXO's worden, indien nodig, gecombineerd om nieuwe outputs te creëren die zowel aan de ontvanger van de transactie als aan jezelf zullen toebehoren. Deze nieuwe outputs, de UTXO's van de betaling zelf en van het wisselgeld, worden dan respectievelijk het eigendom van de ontvanger en dat van jou. Deze UTXO's kunnen dan worden gebruikt als tegoed in andere toekomstige transacties. Deze keten van UTXO's creëert een transparante en traceerbare geschiedenis van alle bitcointransacties in het bitcoinkasboek, vanaf het allereerste block (3 januari 2009).

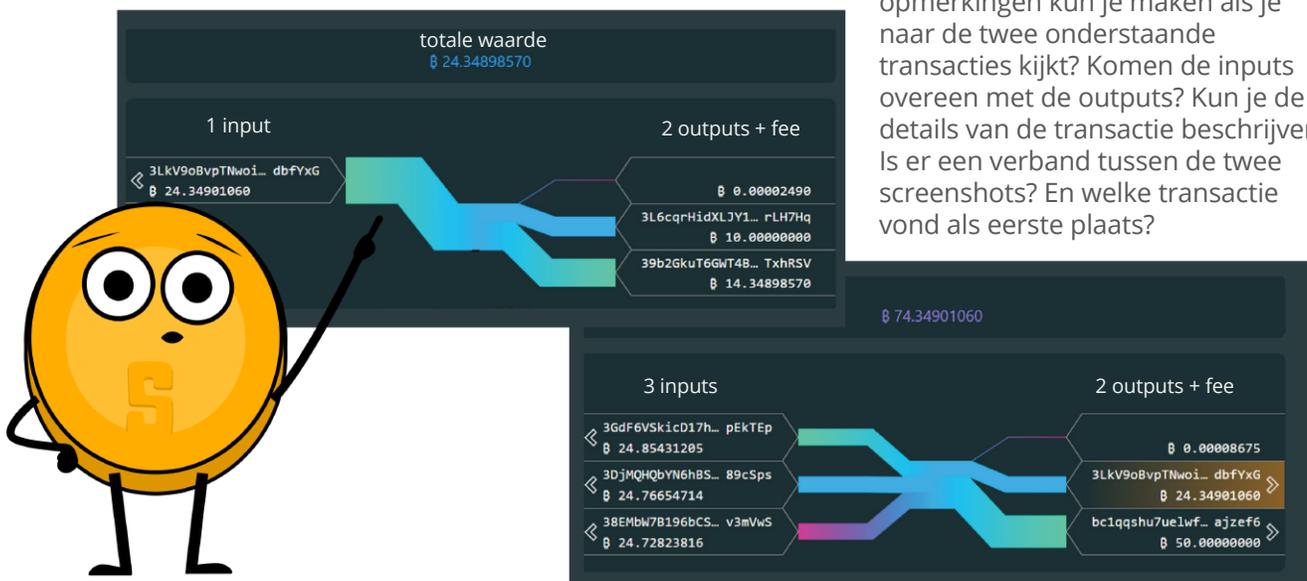
Hier nog een voorbeeld van hoe dit werkt: als je 2 bitcoin wilt versturen maar je hebt alleen een UTXO van 5 bitcoin, dan wordt het verschil van 3 bitcoin naar je teruggestuurd als "wisselgeld". Dit wisselgeld is een nieuwe UTXO voor jou, en je kunt die nieuwe UTXO in een toekomstige transactie uitgeven.

- 1 Alice wil naar Bob 5 bitcoin sturen
- 2 Ze voegt twee van haar UTXO's samen tot 6 BTC
- 3 Van deze UTXO's, stuurt ze 5 BTC naar Bob, ontvangt ze 0,99 bitcoins "wisselgeld", en moet ze 0,01 BTC transactiekosten betalen.
- 4 Na de bevestiging wordt de transactie toegevoegd aan het bitcoinkasboek op alle bitcoinnodes



Stel dat Alice probeert om een van haar al uitgegeven UTXO's te gebruiken om een andere transactie te doen, dan wordt dit automatisch afgewezen door de nodes. Dit komt omdat de nodes een kopie van het bitcoinkasboek (en alle transacties) bijhouden, zodat ze gemakkelijk het saldo van de UTXO's van Alice kunnen controleren en kunnen bevestigen dat de transactie niet geldig is.

Hieronder zie je een screenshot van een echte transactie met slechts één invoer. In een ander geval kan het startsaldo echter de som zijn van meerdere UTXO's. Welke opmerkingen kun je maken als je naar de twee onderstaande transacties kijkt? Komen de inputs overeen met de outputs? Kun je de details van de transactie beschrijven? Is er een verband tussen de twee screenshots? En welke transactie vond als eerste plaats?



Een introductie tot de technische kant van bitcoin

9.3 Bitcoinnodes en miners nader bekeken

In dit gedeelte gaan we dieper in op twee zeer belangrijke onderdelen (en deelnemers) van het bitcoinnetwerk die voor het eerst werden geïntroduceerd in Hoofdstuk 6. We zullen kijken naar:

1

Bitcoinnodes:

Dit zijn poortwachters van het bitcoinnetwerk houden een kopie bij van het bitcoinkasboek, zorgen ervoor dat alle transacties geldig zijn en dat iedereen dezelfde regels volgt.

Door deze taak over nodes wereldwijd te verspreiden, blijft bitcoin beschermd tegen potentiële problemen. Bitcoinnodes helpen het systeem betrouwbaar te houden en trouw te blijven aan het gedecentraliseerde idee, waarbij geen enkele persoon of groep te veel macht heeft.

2

Bitcoinminers:

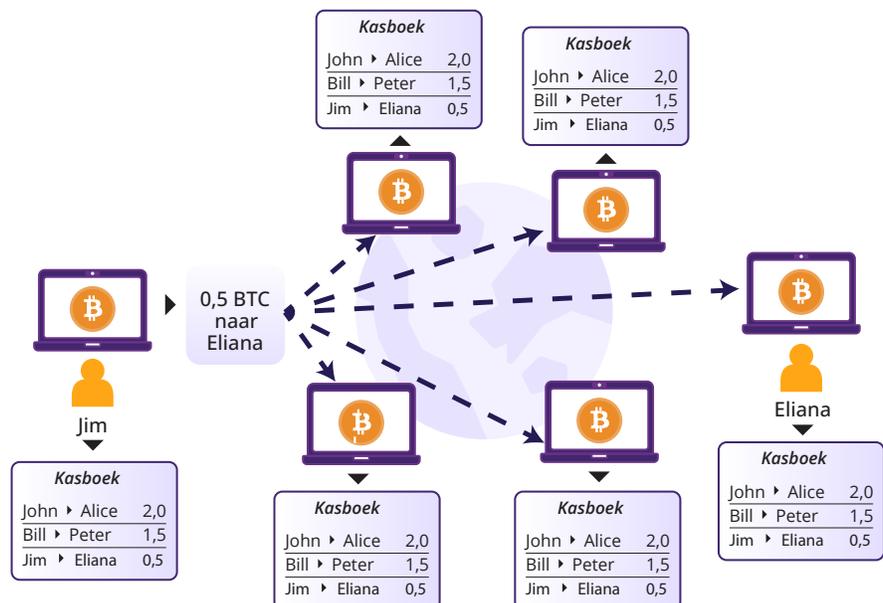
Dit zijn de architecten van de veiligheid en gebruiken krachtige computers en elektriciteit om transacties te controleren en te bevestigen, zodat het netwerk veilig gebruikt kan worden. Dit helpt het kasboek, of blockchain, bestand te maken tegen slechte actoren die de boel proberen te manipuleren.

Samen werken bitcoinnodes en -miners als een team om een gedecentraliseerd, veilig en sterk systeem in stand te houden - een nieuwe manier om met geld om te gaan waar mensen over de hele wereld op kunnen vertrouwen. Laten we deze rollen in meer detail bekijken om te begrijpen op welke manier ze bijdragen.

9.3.1 Wat is een bitcoinnode en hoe zet ik er een op?

Een bitcoinnode klinkt misschien technisch, maar het is gewoon een stukje software waarop een kopie van het bitcoinkasboek draait. Als je je eigen bitcoinnode draait, krijg je een stem in het vormgeven van de regels van het bitcoinnetwerk.

Stel je dit eens voor: als een groep mensen bitcoin probeert te veranderen, bijvoorbeeld door de totale hoeveelheid van bitcoin te veranderen, dan heb jij inspraak. Je kunt ervoor kiezen om de software van je node niet aan te passen aan het nieuwe systeem, wat hetzelfde is als stemmen voor de regels die jij wel ondersteunt.



Laten we ons een bitcoinnode voorstellen als een digitale verkeersagent met een aantal essentiële taken:

1

Poortwachters van de validatie:

Een bitcoinnode houdt een digitale kopie bij van de blockchain, wat een gedistribueerd kasboek is van alle bitcointransacties. Nodes over de hele wereld bewaren ditzelfde kasboek.

2

Communicatiehub:

Nodes verbinden zich met elkaar en creëren zo een uitgebreid communicatienetwerk. Ze delen informatie, vooral transacties die wachten om aan de blockchain te worden toegevoegd. Deze transacties worden opgeslagen in een digitale wachtkamer die "de mempool" wordt genoemd, tot een miner ze verwerkt in een block.

3

Kwaliteitschecker:

Elke toevoeging aan de blockchain wordt kritisch bekeken. Nodes controleren de geldigheid van transacties en wijzen ze af als ze niet voldoen aan de regels van het bitcoinnetwerk.

4

Blockchain Informant:

Andere software, zoals wallets, kunnen een node om informatie vragen over de blockchain, zoals bitcoin balansen. Nodes dienen hierbij als informatiehubs.

5

Nieuwe nodes verwelkomen:

Wanneer een nieuwe node zich wil aansluiten aan het netwerk, stellen al aangesloten nodes een kopie van de blockchain ter beschikking. De nieuwe node controleert onafhankelijk van de rest de geldigheid van elke transactie, wat een vertrouwensloos systeem benadrukt.

Activiteit: Bekijk een video over bitcoinnodes



Een van de opties om je eigen node te draaien is om de Bitcoin Core software te installeren en het wat tijd te geven om de hele blockchain te downloaden. Zodra dit proces voltooid is, kun je de software laten draaien, waarna er elke 10 minuten nieuwe blocks met transacties verschijnen. Je node controleert de geldigheid en voegt de nieuwe blocks toe aan je lokale kopie van de blockchain.

Bron:
Bitcoin Core
Software



Het runnen van een Node biedt soevereiniteit en onafhankelijkheid. Je bent niet afhankelijk van anderen; het is je eigen verkeersagent. In tegenstelling tot je bitcoinwallet, die geen kopie van de blockchain heeft, zorgt een node voor zelfvoorziening. In plaats van anderen te vertrouwen wat betreft je bitcoinbezit (en de staat van het bitcoinnetwerk), kan je wallet met je persoonlijke node communiceren, waardoor je digitale ervaring veiliger en betrouwbaarder is.

9.3.2. Wat is een bitcoinminer en hoe werkt mining?

Het doel van mining is niet het creëren van nieuwe bitcoin. Dat is de stimulans. Mining is het mechanisme waarmee de veiligheid van bitcoin wordt gedecentraliseerd

Andreas M. Antonopoulos

Een introductie tot de technische kant van bitcoin



Miners verzamelen onbevestigde transacties, vormen een block en besteden energie om een waardevolle sleutel te vinden waarmee het block aan de blockchain kan worden toegevoegd. Deze investering van energie beveiligt het netwerk tegen kwaadwillende actoren.

Miners racen tegen elkaar om het volgende block aan de blockchain toe te voegen. Ze zoeken de "juiste block hash," die slim verborgen is tussen miljarden anderen. Stel je een enorme hooiberg voor, gevuld met miljoenen sleutels die elk een unieke hash van een block vertegenwoordigen. Het protocol heeft één specifieke sleutel gekozen die een waardevolle beloning vrijspelt. Miners doorzoeken de hooiberg en testen elke sleutel om te zien of deze in het slot past, maar slechts één gelukkige miner zal als eerste de perfecte match ontdekken.

Zodra een miner de juiste block hash heeft gevonden, deelt hij deze met het netwerk samen met het door hem aangemaakte block met nieuwe transacties. Andere miners verifiëren de oplossing om er zeker van te zijn dat het klopt. Als alles klopt, wordt het block toegevoegd aan de blockchain, waardoor een veilig en openbaar kasboek ontstaat.

Miners verdienen op twee manieren beloningen voor hun inspanningen:



Block rewards



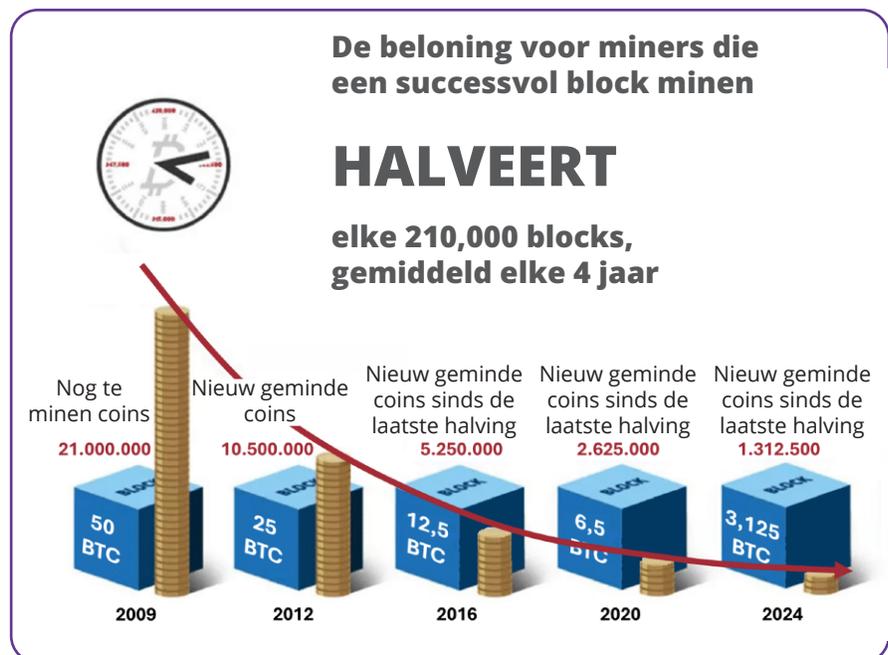
Transactievergoedingen

Block rewards zijn nieuwe bitcoin die in omloop worden gebracht bij elk block dat aan de blockchain wordt toegevoegd. Transactievergoedingen zijn kleine bitcoinbetalingen die gebruikers doen om hun transacties prioriteit te geven en sneller verwerkt te laten worden door miners. Miners kunnen kiezen welke transacties ze opnemen in het block dat ze minen, waarbij ze meestal de voorkeur geven aan transacties met hogere transactiekosten.

Bitcoin halvings

De bitcoin halving is cruciaal voor het behoud van de schaarste en waarde van bitcoin. Er bestaat een limiet van 21 miljoen bitcoins, die niet in één keer beschikbaar waren bij de lancering, maar geleidelijk vrijkomen. Satoshi Nakamoto ontwierp het ingenieuze systeem van de block reward om nieuwe bitcoins te verdelen zonder dat een centrale autoriteit dit kan manipuleren. In de begindagen van Bitcoin kregen miners een beloning van 50 bitcoins voor het minen van elk block, wat hen motiveerde om te investeren in krachtige apparatuur en de benodigde elektriciteit voor hun miningactiviteiten.

Om het netwerk stabiel te houden en het aanbod van nieuwe bitcoin onder controle te houden, wordt de block reward elke 210.000 blocks gehalveerd. Deze gebeurtenis, die "de halving" wordt genoemd, vermindert het aantal nieuwe bitcoin dat in omloop komt maar blijft miners motiveren om het netwerk te beschermen, en de decentralisatie in stand te houden. Historisch gezien hebben halvings geleid tot aanzienlijke prijsstijgingen op de bitcoinmarkt vanwege het verminderde aanbod van nieuwe bitcoins.

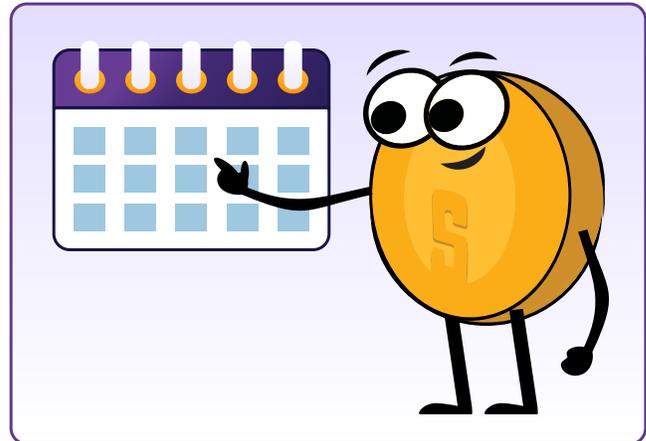




De omloopvoorraad (circulating supply) verwijst naar de totale hoeveelheid van een valuta die in circulatie is gebracht. Bij bitcoin is de omloopvoorraad het aantal munten dat is gemined en op een bepaald moment in omloop is, exclusief munten die voor altijd verloren zijn gegaan.

Na elke halving wordt door het protocol per block minder bitcoin in omloop gebracht, waardoor miners kleinere beloningen krijgen. Deze vermindering van de block reward betekent niet per se dat miners minder winst zullen maken, omdat ze ook transactiekosten kunnen verdienen voor het verifiëren van transacties en het toevoegen ervan aan de blockchain. Dit kan de vermindering van de block rewards compenseren.

Halvings zijn voorgeprogrammeerd in het bitcoinprotocol, waardoor het aanbodscha van bitcoin voorspelbaar en transparant is

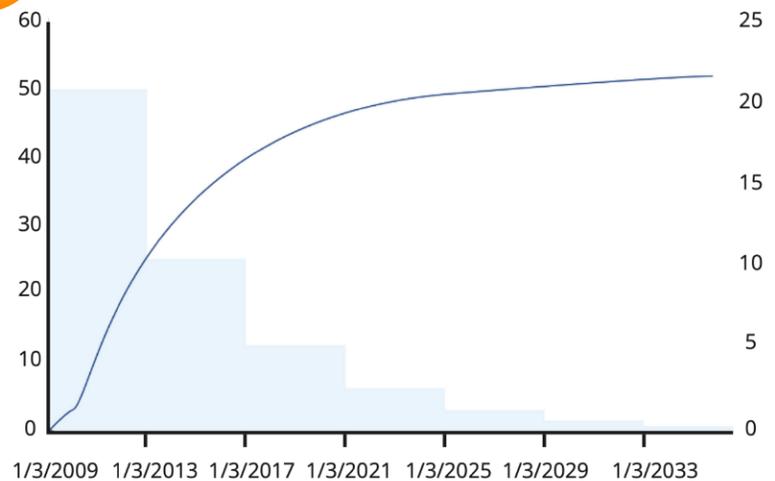


Het bitcoin aanbodscha is het vooraf bepaalde en openbare plan voor het in omloop brengen van nieuwe bitcoin, ontworpen om de schaarste van bitcoin in de loop van de tijd te handhaven.



De volgende tabel geeft een overzicht van de komende halvings voor bitcoin, de verwachte datum van de volgende halvingsgebeurtenis, het blocknummer waarop de halvingsgebeurtenis zal plaatsvinden, de block rewards (per gemined block) vanaf die halvingsgebeurtenis en het percentage van de voorraad dat minimaal gemined zal zijn.

Het bitcoin aanbodscha



Gebeurtenis	Verwachte datum	Block	Block Reward	Percentage gemined
Vierde halving	2024	840,000	3.125	96.875 %
Vijfde halving	2028	1,050,000	1.5625	98.4375 %
Zesde halving	2032	1,260,000	0.78125	99.21875 %

Een introductie tot de technische kant van bitcoin

Naarmate er meer bitcoin wordt gemined, zal de omloopvoorraad en het percentage van de totale voorraad dat gemined is, blijven toenemen totdat het totale aanbod van 21.000.000 is bereikt. Het afnemende aanbod van nieuwe coins, in combinatie met een stijgende vraag, kan de prijs van bitcoin (gemeten in euros) opdrijven. Dit is in het voordeel van vroege gebruikers (early adopters) en motiveert miners om door te gaan met het beveiligen van het netwerk en het inzetten van hun rekenkracht en middelen.

Percentage van de 21M geminde bitcoins



Wat is een geldige block hash in bitcoin?

In bitcoin is een geldige block hash als een speciale code die miners proberen te vinden. Het is een uniek nummer dat helpt bij het bijhouden van elk block in de blockchain, waarin informatie over transacties wordt opgeslagen. De blocks vormen zich in een keten, van het eerste (genesis block) tot het laatste block, waardoor een openbaar verslag ontstaat van alle transacties. Deze hashing van een block is cruciaal omdat het elk block koppelt aan het block ervoor, waardoor het voor iedereen mogelijk is om de geschiedenis van alle transacties te controleren. Het is een beetje zoals een vingerafdruk voor elk block, die ervoor zorgt dat de informatie correct en veilig is. Met andere woorden, de hash van het block is een manier om te bevestigen dat de gegevens in het block niet zijn veranderd.



Satoshi Nakamoto, de uitvinder van bitcoin, mineerde het eerste block, dat in totaal 50 bitcoins bevatte.

De race om een block te minen

Miners gaan een wedstrijd aan om de hash van het block te vinden die overeenkomt met het doel (een speciaal nummer) dat door het netwerk is ingesteld. De miner die als eerste met succes de juiste hash van het block ontdekt, krijgt de mogelijkheid om dat block aan de blockchain toe te voegen en het de bijbehorende hash ID te geven. Deze oplossing dient als validatie voor de authenticiteit van het block.

Mining kan vergeleken worden met een race waarbij het doel is om zo snel mogelijk de finish te bereiken. De moeilijkheid om de hash van het block te vinden, wordt periodiek aangepast, zodat elk block in ongeveer 10 minuten wordt gemined (om te compenseren voor een toe- of afnemend aantal miners) Dit mechanisme wordt de "difficulty adjustment" genoemd.



Laten we zeggen dat het doelgetal dat door het bitcoinprotocol is ingesteld 1000 is. De miners moeten dan hun rekenkracht en energie gebruiken om een block hash (een specifiek getal) te zoeken dat lager is dan 1000. De eerste miner die een block hash vindt dat lager is dan 1000 mag het nieuwe block toevoegen aan de blockchain en wordt beloond met bitcoin.

De moeilijkheidsgraad in bitcoinmining is een maat voor hoe moeilijk het is om een geldige hash van een block te vinden dat voldoet aan het doel dat het protocol heeft gesteld. De moeilijkheidsgraad wordt elke 2016 blocks aangepast, wat ongeveer elke twee weken is, om ervoor te zorgen dat blocks in een vast tempo aan de blockchain worden toegevoegd. Zonder deze difficulty adjustment zouden blocks steeds sneller gevonden worden naarmate meer miners naar de block hash gaan zoeken. De moeilijkheidsgraad wordt uitgedrukt als een getal en hoe hoger de moeilijkheidsgraad, hoe moeilijker het is om een geldige hash van een block te vinden.



Neem bijvoorbeeld deze twee verschillende hashes:

-  Hash 1: 0000A1mINgF0RbL0cK5wltHth3hAy5tAcK
Moeilijkheidsgraad: 1
-  Hash 2: 00000000A1mINgF0RbL0cK5wltHth3hAy5tAcK
Moeilijkheidsgraad: 2

In dit voorbeeld heeft Hash 2 een hogere moeilijkheidsgraad dan Hash 1, omdat het een langere hash is met meer nullen aan het begin. Het is moeilijker voor miners om Hash 2 te vinden omdat hun computers meer werk moeten verrichten.

Door een geldige hash van een block te vinden, bewijst een miner dat hij het werk heeft gedaan dat nodig is om het nieuwe block aan de blockchain toe te voegen en krijgt hij een beloning in bitcoin, plus transactiekosten voor zijn inspanning. Deze methode die het bitcoinnetwerk gebruikt om transacties te valideren en nieuwe blocks aan de blockchain toe te voegen heet Proof-of-Work (PoW).

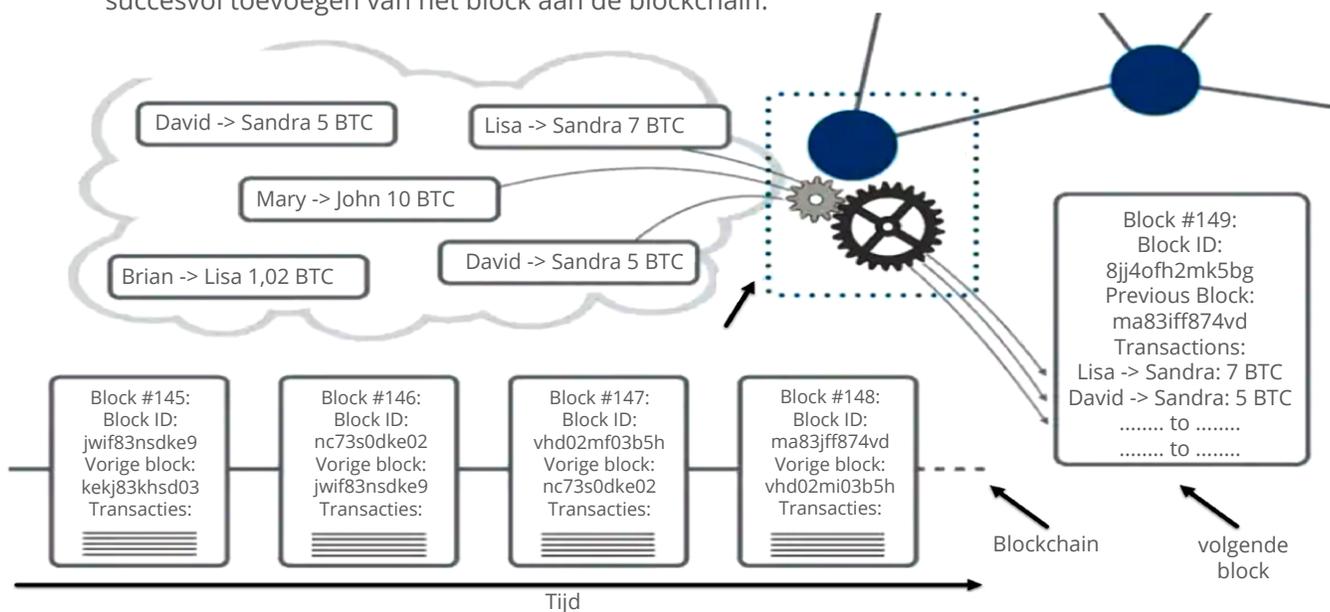


Een introductie tot de technische kant van bitcoin

PoW maakt bitcoin veilig door het moeilijk te maken voor iemand met kwade bedoelingen om de controle over te nemen, waardoor het bitcoinnetwerk veilig te gebruiken is.

Samengevat bestaan de taken van miners uit:

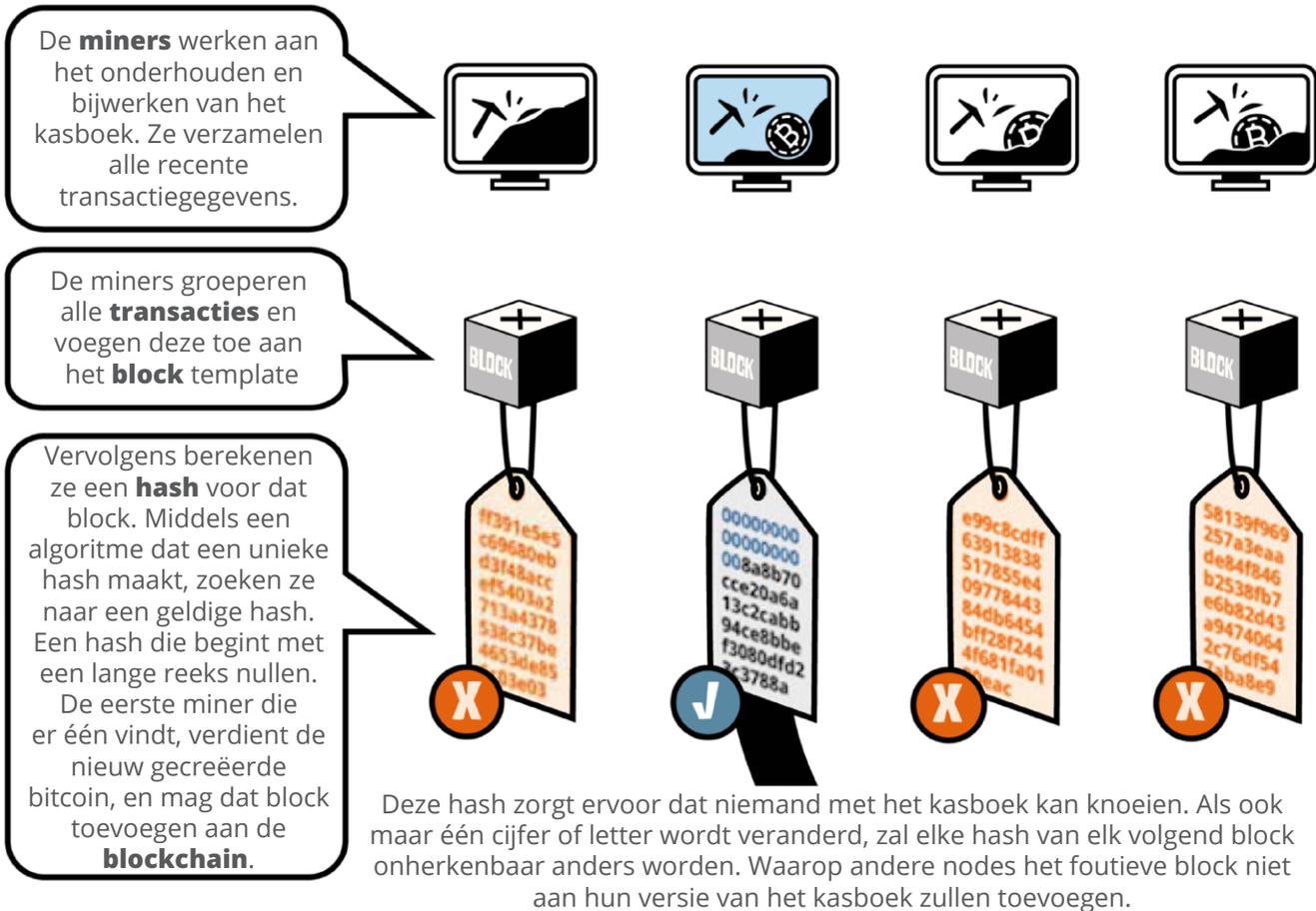
- 1 Het bundelen van transacties in blocks:
Nodes verifiëren nieuw aangemaakte transacties die wachten in de mempool. De miners selecteren een subset hiervan om op te nemen in een toekomstig te minen "block template".
- 2 Proof-of-Work:
Miners concurreren met elkaar om de geldige hash van het block te vinden.
- 3 Geldige blocks broadcasten:
Na het vinden van de geldige blockhash, zenden miners het nieuwe block uit naar het netwerk
- 4 Beloningen verdienen:
Tot slot ontvangen miners nieuw gecreëerde bitcoins (block subsidy) en transactiekosten voor het succesvol toevoegen van het block aan de blockchain.



Meerdere miners werken tegelijkertijd aan het creëren van nieuwe blocks. De eerste miner die een block hash ontdekt die voldoet aan de eisen van het netwerk, deelt dit met het netwerk. De andere miners controleren dan de transacties in het template block van die miner om er zeker van te zijn dat ze geldig zijn. Als de transacties inderdaad geldig zijn, wordt het block toegevoegd aan de blockchain. De andere blocks die op dat moment door de andere miners zijn gemaakt worden weggegooid. Dit proces helpt de consensus binnen het netwerk te behouden en voorkomt "dubbel uitgeven" van UTXO's.

Een template block is een block met een set transacties dat overwogen wordt om aan de blockchain toegevoegd te worden, maar nog niet toegevoegd is.





9.4 Wat is de mempool?

De "Mempool" of Memory Pool is als een wachtkamer voor transacties in het bitcoinnetwerk. Wanneer je een transactie doet, wordt deze eerst uitgezonden naar de mempool en kunnen miners besluiten of ze deze transactie toevoegen aan een nieuw block. Vervolgens controleren de bitcoinnodes of de transacties in dit nieuwe block voldoen aan de consensusregels.

Stel je voor dat je in de rij staat bij een restaurant en je naam wordt toegevoegd aan een lijst van mensen die staan te wachten. Als er een tafel vrijkomt, roept de gastheer je naam en geeft je een plaats. Op dezelfde manier komt een bitcointransactie in de mempool. De transactie wordt toegevoegd aan de blockchain wanneer een miner besluit deze op te nemen in een block.

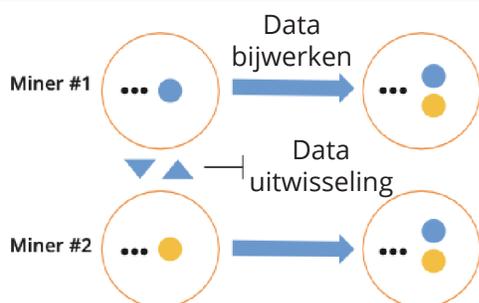
Een introductie tot de technische kant van bitcoin

In de **mempool** wachten transacties tot ze worden bevestigd in een block.



Wanneer een node een transactie ontvangt van een peer, moet deze eerst verifiëren of de transactie legitiem is.

Mempoolsynchronisatie stelt nodes in staat om hun transacties te delen met andere nodes door ze een bericht te versturen met een lijst van geverifieerde transacties in de mempool.



Het belangrijkste doel van een mempool is om:

1 Niet-bevestigde transacties door te geven



2 Miners transacties te geven om te minen.



De Accept To Memory Pool (ATMP) stelt nodes in staat om transacties te ontvangen, te valideren en toe te voegen aan hun mempool. Het controleert:

- Heb ik deze transactie al?
- Is er een conflict met een andere transactie in de mempool?
- Komen de ingaande en uitgaande hoeveelheid bitcoin overeen?
- Bewijzen de handtekeningen dat de vorige UTXO kan worden uitgegeven?
- Is de vergoeding (fee) hoog genoeg?

Hoe worden transacties geverifieerd en toegevoegd aan de mempool?

Wanneer nieuwe transacties worden verzonden naar het bitcoinnetwerk, verifiëren nodes deze transacties om er zeker van te zijn dat ze geldig zijn en dat het geld niet eerder is uitgegeven. Zodra deze transacties zijn geverifieerd, voegen de nodes ze toe aan hun mempool. Vervolgens delen de nodes de transacties met andere nodes om ze dubbel te controleren. Als de meerderheid van de nodes akkoord gaat, worden de transacties beschikbaar gesteld aan miners, die kunnen selecteren welke transacties ze opnemen in een block.

Soms komt het voor dat transacties niet bevestigd of geweigerd worden. Dit kan veroorzaakt worden door:

- 1 Te lage transactiekosten:
Transacties met een lage vergoeding worden mogelijk niet snel genoeg verwerkt, omdat miners geneigd zijn om de transacties met hogere vergoedingen eerder op te nemen in hun blocks.
- 2 Netwerkgestoe: Bij een overbelast netwerk kan het bevestigen van transacties traag zijn, zelfs bij een hoge vergoeding.
- 3 Poging tot double spend:
Als een kwaadwillende een 'double spend' tracht uit te voeren, kan die transactie worden geweigerd.
- 4 Onjuiste of onvolledige gegevens:
Als een transactie onjuiste of onvolledige gegevens bevat, kan deze worden geweigerd.
- 5 Misvormde transactie:
Als een transactie incorrecte gegevens bevat, kan deze geweigerd worden door het netwerk.

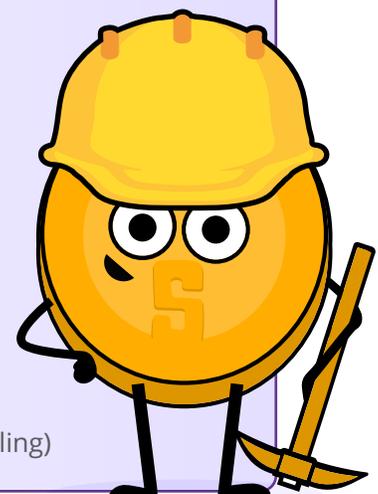
Om te voorkomen dat transacties worden geweigerd, is het aan te raden om een vergoeding aan te bieden die hoog genoeg is zodat de transactie tijdig wordt verwerkt. Controleer ook altijd minstens twee keer of alle gegevens in de transactie correct zijn voordat je deze verstuurt.

Activiteit: mempool

- 1 Scan de volgende QR code:
- 2 Bekijk de verschillende elementen die op de pagina worden weergegeven, waaronder de laatste blocks, bevestigde transacties, het aantal transacties, geheugengebruik en de geschatte waarde van het hele block. Beantwoord de vragen:



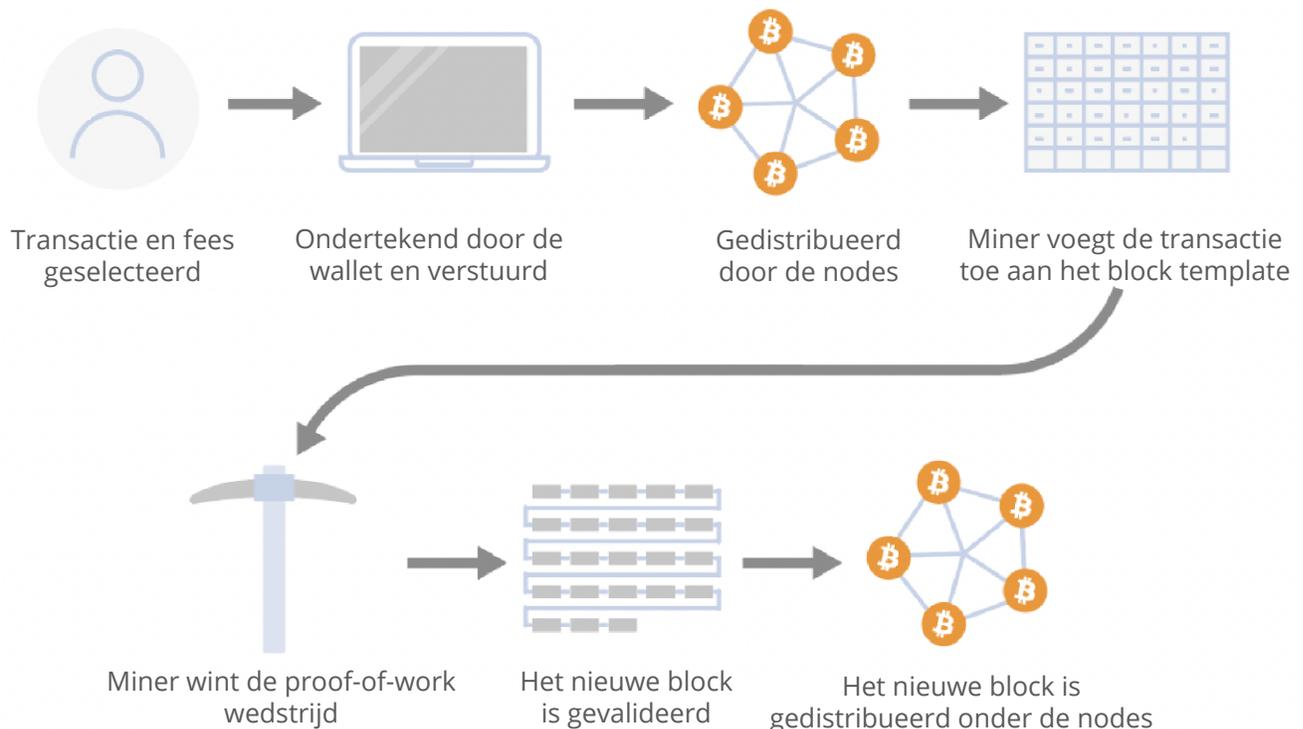
- ☀ Wat was het laatst geminede block?
- ☀ Hoeveel transacties zaten er in dat block?
- ☀ Wat is de totale waarde die in bitcoin wordt verhandeld?
- ☀ Wat was de grootte van het block in megabytes?
- ☀ Hoeveel bitcoin heeft de miner in totaal verdiend?
- ☀ Wat was de totale waarde van de vergoedingen die de miner ontving voor het toevoegen van de transacties aan het netwerk?
- ☀ Kies de transactie met de hoogste waarde.
Over hoeveel bitcoinadressen werd het bedrag verdeeld?
- ☀ Met hoeveel nullen begint de nonce van het block?
(De nonce is een willekeurig getal dat aan een block header wordt toegevoegd om een hash te maken die voldoet aan de moeilijkheidsdoelstelling)



Een introductie tot de technische kant van bitcoin

9.5 Hoe bitcointransacties van begin tot eind werken

- 1 Adam wil bitcoin naar Peter sturen. Hij kiest een van zijn UTXO's, maakt een transactie aan en voegt alle benodigde details toe, waaronder de hoeveelheid bitcoin die hij wil versturen, Peter's ontvangende adres en een bovengemiddeld bedrag aan transactiekosten.
- 2 Na een laatste controle of alle details kloppen, gebruikt Adam zijn private key om de transactie te ondertekenen.
- 3 Adam verzendt (broadcast) de transactie naar het bitcoinnetwerk



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

- 4 De nodes op het netwerk ontvangen de transactie en verifiëren de geldigheid ervan volgens de consensusregels (zoals de geldigheid van Adams handtekening en of hij voldoende bitcoin heeft om de transactie uit te voeren).
- 5 De transactie wordt als geldig gemarkeerd en de nodes propageren het naar andere nodes op het netwerk, waarna ze het toevoegen aan de mempool.
- 6 Omdat Adam een transactievergoeding (fee) heeft gekozen die hoog genoeg is, nemen bijna alle miners zijn transactie op in hun blocks.

7

Proof-of-work: miners proberen hun block te minen door de geldige hash van het block als eerste te vinden. Een van de miners vindt de hash en zendt zijn block uit naar het netwerk.

8

De nodes ontvangen het nieuwe block en verifiëren de geldigheid ervan. Dit houdt in dat alle transacties in het block worden gevalideerd en dat het proof-of-work wordt gecontroleerd.

9

De meerderheid van de nodes is het ermee eens dat het block geldig is en voegt het toe aan de blockchain. Peter ontvangt de bevestigde (confirmed) bitcoin op zijn ontvangstadres.

10

Naarmate er in het daaropvolgende uur meer blocks aan de blockchain worden toegevoegd, groeit het aantal bevestigingen van de transactie. Naarmate het aantal bevestigingen toeneemt, krijgt Peter meer vertrouwen dat het gelukt is en dat de transactie niet meer omkeerbaar is.



Samengevat ondertekent de verzender de transactie met zijn private key, de nodes verifiëren de transactie-UTXO's en de miners voegen de geverifieerde transactie toe aan de blockchain. De ontvanger heeft dan toegang tot de bitcoin met zijn of haar private key. Zodra een block is gemined, worden alle transacties die er deel van uitmaken als bevestigd beschouwd en de UTXO's die als inputs in deze transacties zijn gebruikt, worden als uitgegeven beschouwd en zullen niet opnieuw worden gebruikt.

In dit hoofdstuk heb je waardevolle inzichten gekregen over de fundamentele concepten van de werking van bitcoin. We hebben essentiële aspecten behandeld, van de basis van geld tot de technische kant van de bitcointechnologie. Laten we het nu allemaal samenvoegen in hoofdstuk 10, waarin we dieper ingaan op de belangrijke vraag: "Waarom bitcoin?"

Hoofdstuk #10

Waarom Bitcoin?

10.0 Inleiding

Activiteit: hoe zou een toekomst met bitcoin eruit kunnen zien?

10.1 Wat is digitaal centralebankgeld en wie beheert het?

10.2 De filosofie van bitcoin

Activiteit: discussie in de klas - heb je het recht om over je eigen geld te beschikken?

10.3 De voordelen van bitcoin

10.4 Een zelfredzame toekomst

Activiteit: discussie in de klas - hoe is je perspectief veranderd?

Waarom Bitcoin?

Bitcoin is meer dan een valuta; het is een revolutie die de macht teruggeeft aan de mensen, een voorproefje van vrede en vrijheid in een wereld die verlangt naar zelfbeschikking.

Mijn eerste Bitcoin

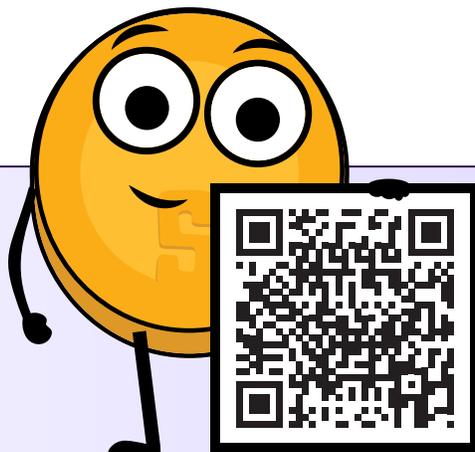
In dit afsluitende hoofdstuk vatten we de lessen samen die we hebben geleerd tijdens onze reis, behandelen we een paar belangrijke vragen en verkennen we de toekomst van bitcoin.

Bitcoin is niet zomaar een technologie, het is een soort netwerk dat een nieuwe vorm van geld mogelijk maakt waarvan de voorraad door geen enkele partij kan worden veranderd. De mensheid heeft nog nooit een vorm van geld gehad met een vaste voorraad en zonder gecentraliseerde controle. Als bitcoin op grote schaal wordt gebruikt, is het een instrument dat een beweging voor positieve verandering ontketent die het leven van mensen over de hele wereld kan veranderen. Bitcoin vertegenwoordigt een vreedzame revolutie naar collectieve vrijheid en gelijkheid, en opent nieuwe mogelijkheden voor de mensheid door het creëren van een gedeeld wereldwijd monetair systeem.

Als gedecentraliseerd wereldwijd systeem maakt bitcoin grotere financiële vrijheid mogelijk en verschuift de macht van enkelen naar velen. Het biedt een veilig en censuurbestendig platform voor het opslaan en overdragen van waarde, waardoor individuen controle krijgen over hun vermogen en hun koopkracht kunnen beschermen. Dit is vooral belangrijk in het huidige onzekere economische klimaat, waarin het traditionele financiële systeem voor ongekende uitdagingen staat.

Activiteit: hoe zou een toekomst met bitcoin eruit kunnen zien?

De mogelijkheden voor positieve verandering zijn enorm en daarom nodigen we je uit om deze video te bekijken voor meer informatie.



Vervolgens kijken we naar een andere vorm van digitale valuta, namelijk digitaal centralebankgeld (ook wel de digitale Euro of CBDC) genaamd, en evalueren we hoe dit vergelijkbaar maar ook verschillend is van bitcoin.

10.1 Wat is digitaal centralebankgeld en wie beheert het?

Digitaal centralebankgeld zoals de digitale Euro, is een digitale versie van gewoon fiatgeld en volgt dezelfde principes. Een centrale autoriteit, zoals de overheid, kan meer aanbod creëren en is daardoor in staat om de koopkracht van mensen te verminderen. Digitaal centralebankgeld geeft overheden echter de controle over hoe dat geld wordt gebruikt door mensen over de hele wereld. Volgens het onderzoek van de Human Rights Foundation (HRF) zijn 119 van de 193 regeringen wereldwijd digitaal centralebankgeld aan het onderzoeken, testen of gebruiken.

Je kunt controleren of jouw land digitaal centralebankgeld aan het testen is op de tracker van de Human Rights Foundation op:

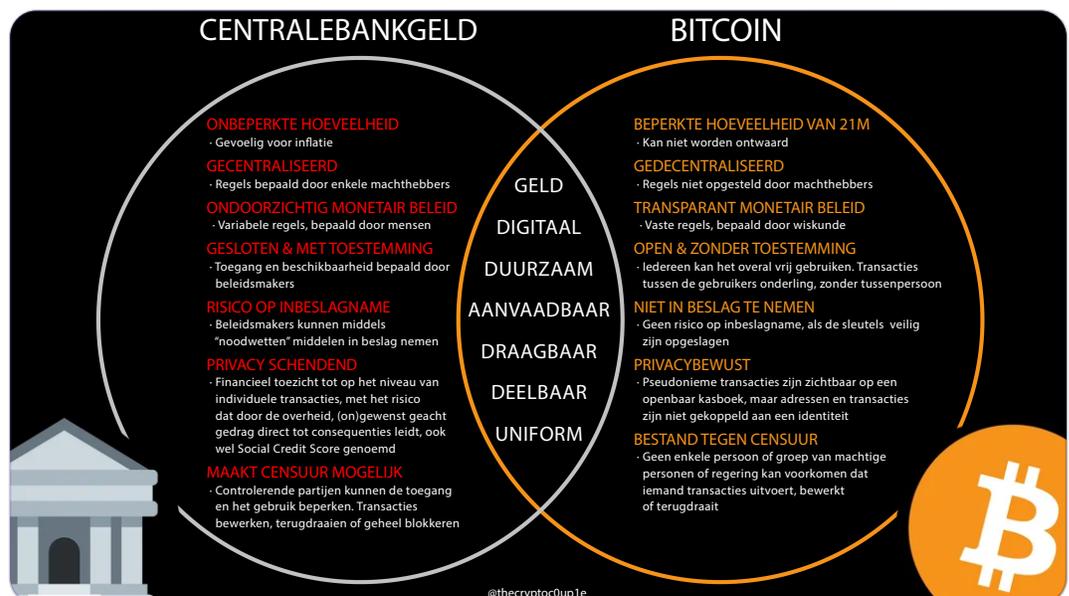
<https://cbdctracker.hrf.org/home> or
<https://cbdctracker.org/>



Wat maakt digitaal centralebankgeld anders dan gewoon fiatgeld, behalve dat het digitaal is? Het is cruciaal om te begrijpen dat digitaal centralebankgeld, in tegenstelling tot gewoon fiatgeld in de vorm van briefgeld, munten of een normale bankrekening, de overheid in staat stelt elke transactie wereldwijd rechtstreeks te volgen en te controleren. Dit betekent dat de overheid bepaalde transacties kan stoppen of zelfs je rekening kan bevriezen als het ze niet bevalt hoe jij je geld gebruikt. Stel je bijvoorbeeld voor dat je geld wilt sturen naar een familielid in een land dat hulp nodig heeft, maar je lokale overheid weigert je transactie omdat ze het niet eens zijn met de leiders van dat land. Of stel je voor dat je naar de winkel gaat om iets te kopen wat je leuk vindt, maar dat je dat niet kunt omdat je je mening op sociale media hebt geuit.

Digitaal centralebankgeld geeft regeringen vrijwel onbeperkte macht om te bepalen hoe geld over de hele wereld wordt gebruikt. Ze kunnen de mogelijkheden van individuen om geld uit te geven op basis van hun eigen keuzes beperken. Sommigen beweren zelfs dat digitaal centralebankgeld machtige regeringen in staat zal stellen om wereldwijd dictatoriaal beleid af te dwingen - met één druk op de knop - zonder dat daar menselijke handhavers voor nodig zijn.

Zowel digitaal centralebankgeld als bitcoin zijn digitaal, maar afgezien van deze overeenkomst vertegenwoordigen ze zeer verschillende vormen van geld met verschillende filosofieën, wat leidt tot verschillende resultaten voor de mensheid.



Waarom Bitcoin?

10.2 De filosofie van bitcoin

In hoofdstuk 6 en 9 ontdekten we dat mensen die een bitcoinnode runnen, helpen om de regels van bitcoin te handhaven. Dit is belangrijk, want voor de allereerste keer kunnen mensen zoals wij ervoor zorgen dat de regels van ons monetaire systeem beschermd worden. Deze regels zijn onder andere dat er maar een beperkte hoeveelheid geld kan zijn en dat een enkele entiteit deze regels niet zomaar kan veranderen. Het is een bijzondere kans voor gewone mensen om mee te helpen aan de veiligheid en betrouwbaarheid van het geld.

De filosofie van bitcoin gaat over zelfredzaamheid, vrijheid, financiële onafhankelijkheid, kritisch denken en het concept dat we allemaal inspraak zouden moeten hebben in de regels van het systeem dat we voor onszelf kiezen. In tegenstelling tot het fiatsysteem dat beheerd wordt door machtige centrale partijen, werkt bitcoin op een netwerk waar geen enkele partij de volledige controle heeft. Dit betekent dat, in tegenstelling tot andere soorten geld, zoals digitaal centralebankgeld, niemand je eigendommen kan afpakken of je ervan kan weerhouden je geld uit te geven zoals jij wilt.

In de fiatwereld vertaalt meer rijkdom zich direct naar meer invloed en controle. Bitcoin geeft de macht daarentegen aan het volk. Het is als een teamprestatie waarbij iedereen, ongeacht hoeveel geld hij of zij heeft, een cruciale rol speelt in het systeem. Stel het je voor als een collectieve kracht, waarbij je financiële omvang niet automatisch betekent dat je controle hebt over alles. Bitcoin is gebouwd op onveranderlijke regels en in deze harmonie is het alsof de mensheid zelf de controle heeft over het systeem. Er zijn geen hoge piefen die de lakens uitdelen; we werken allemaal samen als een veerkrachtige gemeenschap die de koers van bitcoin bepaalt, zonder dat een enkele autoriteit zegt wat het moet doen.

Terwijl in het fiatsysteem de machthebbers de regels dicteren, is het in het bitcoinecosysteem de collectieve kracht van individuen die het netwerk in stand houdt. Geen enkele entiteit, ongeacht haar rijkdom, kan het pad van het bitcoinecosysteem dicteren. Het is een omkering van de traditionele machtsdynamiek, waarbij de veerkracht van het systeem niet in de handen van enkelen ligt, maar in de collectieve kracht van elke deelnemer.

Het belangrijkste doel is om een veilig, duidelijk en eerlijk systeem te creëren waarbij iedereen in gelijke mate toegang heeft tot mondiaal geld.

Activiteit: discussie in de klas - heb je het recht om over je eigen geld te beschikken?

- 1 Is het bezit van geld een menselijke noodzaak en een mensenrecht? Waarom?
- 2 Als je je geld niet kunt uitgeven zoals je zelf wilt, het niet kunt overdragen aan wie je wilt of het niet mee kunt nemen naar een nieuw land, is het dan echt van jou? Waarom wel/niet?
- 3 Waarom wordt ruilhandel niet veel meer gebruikt? Wat is het probleem van de samenvallende behoeften?
- 4 Waarom is het voor iedereen vandaag de dag belangrijk om de Nixon-schok en de relevantie ervan te begrijpen?
- 5 Hoe verschilt geld met een vaste voorraad van traditioneel fiatgeld?

- 6 Wanneer is bitcoin ontstaan, door wie, met welk doel en hoe definieert dit doel het concept van een gedecentraliseerd systeem?
- 7 Wat is het verschil tussen een custodial en een non-custodial wallet? Wat was jouw favoriete wallet?
- 8 Wat begrijp je van het lightningnetwerk? Voor wat voor soort transacties zou je het gebruiken?
- 9 Op welke manier ondersteun je het bitcoinnetwerk door het draaien van je eigen node?
- 10 Hoe kan controle over je eigen geld bijdragen aan je dagelijks leven en je toekomstplannen?
- 11 Op welke manieren kan financiële vrijheid je vermogen om een positieve bijdrage te leveren aan je gemeenschap of samenleving vergroten?

10.3 De voordelen van bitcoin

"Hyperbitcoinization" is een potentiële toekomst waarin bitcoin het dominante wereldwijde monetaire systeem wordt. Dit zou betekenen dat bitcoin door iedereen, overal en voor alles wordt gebruikt - van het kopen van koffie tot het betalen van rekeningen en zelfs om een huis te kopen.

De groeiende interesse in bitcoin van individuen, bedrijven, landen en overheden benadrukt de potentiële impact van een wijdverspreide toepassing op de economie en maatschappij. Hier zijn enkele voordelen van een hyperbitcoinwereld:

- 1 Een zelfsoevereine toekomst:
Dit is een toekomst waarin individuen wereldwijd volledige controle hebben over hun eigen digitale identiteit en bezittingen. Dit kan leiden tot meer financiële inclusie, vrijheid, privacy en veiligheid, wat bijdraagt aan een verbeterd menselijk welzijn, welvaart en algemeen geluk.
- 2 Een betrouwbaar spaarmiddel:
De digitale schaarsheid van bitcoin maakt het een betrouwbaar spaarmiddel, wat meer mensen zou kunnen aanmoedigen om het te gebruiken als een middel om te sparen voor de toekomst.
- 3 Veranderingen in monetair beleid:
Als bitcoin op grote schaal wordt gebruikt, zou dat het vermogen van overheden om de geldhoeveelheid te manipuleren met traditionele monetaire beleidsinstrumenten teniet doen. Een massale invoering van bitcoin zou de koopkracht van mensen kunnen vergroten en de maatschappij kunnen stimuleren om over te stappen op activiteiten met een lage tijdsvoorkeur.
- 4 Meer transparantie en traceerbaarheid:
De fraudebestendige en onveranderlijke registratie van alle transacties op de blockchain vergroot de transparantie en controleerbaarheid in verschillende industrieën en sectoren. Op dit moment hebben machtige entiteiten de mogelijkheid om biljoenen dollars over de wereld te verplaatsen zonder dat duidelijk zichtbaar is waar deze middelen naartoe gaan of hoe ze worden gebruikt. Door een open en verifieerbare registratie van financiële transacties te bieden, kan bitcoin ervoor zorgen dat de beweging van kapitaal beter controleerbaar en toegankelijker wordt voor het publiek.

Waarom Bitcoin?



Een revolutie in de markt voor geldoverboekingen:

Dit bestaat uit het overboeken van geld van de ene partij naar de andere, vaak over internationale grenzen heen. Ondanks de dalende kosten blijven deze overboekingen relatief duur in vergelijking met binnenlandse bankoverschrijvingen, vooral voor kleinere bedragen. Het lightningnetwerk biedt snelle en goedkope transacties, waardoor het zeer geschikt is voor het overmaken van geld en een oplossing biedt voor de hoge kosten en andere uitdagingen die hiermee gepaard gaan, zoals trage vereffeningstijden en beperkingen buiten de kantooruren.



Overvloedige energie:

Als betaalbare energie makkelijk verkrijgbaar is, geniet de samenleving van grote welvaart en kan aan de toenemende behoefte aan stroom voor huizen, bedrijven en nieuwe technologieën worden voldaan. Bitcoinmining stimuleert het gebruik van overtollige energie uit duurzame energiebronnen zoals zonne-, wind- en waterkracht die normaal gesproken verloren zou gaan. Bitcoin miners gebruiken deze overtollige energie om nieuwe bitcoin te creëren door middel van mining, wat het netwerk beveiligt. Wanneer de energiemaatschappij de energie nodig heeft voor haar klanten, zullen de miners hun activiteiten afschalen en de energie ter beschikking stellen.

10.4 Een zelfredzame toekomst

Bitcoin is geld.

Mensen communiceren via het uitgeven van geld welke activiteiten, goederen en diensten in de samenleving zij het belangrijkste vinden. Zoals we in deze cursus hebben gezien, wordt geld vrijwel altijd gemanipuleerd als onder controle is van gecentraliseerde autoriteiten.

Een van de fouten die de mensheid door de geschiedenis heen blijft herhalen is het manipuleren van geld, wat vervolgens een negatief effect heeft op individuen, gezinnen, bedrijven, regeringen en uiteindelijk op de wereldwijde menselijke welvaart.

Door de controle over geld uit handen te nemen van gecentraliseerde partijen en in plaats daarvan geld te gebruiken met een vaste voorraad die geen enkele partij kan veranderen, creëren we een andere wereld. Een wereld waarin we er niet op hoeven te vertrouwen dat de mens het juiste zal doen, maar waarin de mens niet in staat is het verkeerde te doen.

Dit is een fundamenteel andere wereld.

En jij, beste student, kunt een deel zijn van het creëren van deze wereld. Door bitcoin te gebruiken, je eigen node te runnen en je medemens te helpen meer te leren over de toekomst van geld, stem je voor een andere wereld.

Activiteit: discussie in de klas - hoe is je perspectief veranderd?

Beantwoord de 5 vragen hieronder:



Waarom hebben we geld nodig?

Wat is geld?

Waarom Bitcoin?

Wie beheert het geld?

Wat geeft geld zijn "waarde"?

Schrijf de vragen op die de studenten tijdens hoofdstuk 1 hebben gesteld en beantwoord ze hier.

1

Ga terug naar de eerste activiteit in hoofdstuk 1 en vergelijk je nieuwe antwoorden met je oude antwoorden

2

Vergelijk en bespreek de oorspronkelijke antwoorden en vragen. Is er iets veranderd?

3

Stel jezelf deze laatste vraag: wat is mijn volgende stap? En hoe kan ik deze nieuwe kennis gebruiken om mezelf te versterken?



Als je klaar bent om de volgende stap te zetten, bekijk dan de volgende sectie "Additionele bronnen", waarvoor we de beste bronnen hebben geselecteerd om verder mee te leren. Succes!

Aanvullende bronnen

1. Waarom bitcoin gebruiken?

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

In dit boek wordt beargumenteerd waarom bitcoin waardevol is en de potentie heeft om een dominante wereldwijde valuta te worden. De auteur behandelt de technische en economische aspecten van bitcoin.

b "Why Bitcoin Matters" door Aleks Svetski (1 uur):

Deze video gaat over het belang van bitcoin als gedecentraliseerd digitaal geld en hoe het het huidige financiële systeem kan beïnvloeden. De spreker onderzoekt het potentieel van bitcoin om financiële vrijheid te bieden aan mensen over de hele wereld.

c "Why Bitcoin" door Wiz:

Dit artikel geeft een overzicht van de voordelen van het gebruik van bitcoin als digitaal geld en spaarmiddel. Het benadrukt het gedecentraliseerde karakter van bitcoin en hoe dit zorgt voor meer financiële vrijheid en veiligheid.

2. Wat is bitcoin?

a "How Bitcoin Works Under the Hood" door CuriousInventor:

<https://www.youtube.com/watch?v=Lx9zgZCMqXE>

Deze video geeft een gedetailleerde uitleg van de technische aspecten van bitcoin en hoe het werkt.

b "What Is Bitcoin" door Greg Walker:

Dit artikel geeft een uitgebreide uitleg over wat bitcoin is, inclusief de geschiedenis, technologie en hoe het verschilt van traditioneel geld.

c "Bitcoin - The Genesis" door RT (30 minuten):

Deze video gaat over het ontstaan en de begindagen van bitcoin. Het onderzoekt de beweegredenen van de mysterieuze maker, Satoshi Nakamoto, en hoe het concept van bitcoin zich ontwikkelde.

3. Verder leren:

a "The Bitcoin Standard" (1 uur 40 minuten):

Dit luisterboek verkent de economische en historische context die heeft geleid tot het ontstaan van bitcoin. Het behandelt de voordelen van gedecentraliseerd geld en het potentieel voor bitcoin om een wereldwijde standaard te worden.

c "Bitcoin Babies"

by Naomi Wambui - <https://bitcoinbabies.com/>
Twitter: @btcbabies - @ngachanaomi1

A free PDF resource that aims to empower mothers with essential knowledge encompassing nutrition, bitcoin, and overall mental well-being.

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

Dit audio college gaat over de Oostenrijkse school en hoe deze zich verhoudt tot het concept van bitcoin. Het biedt een diepgaande blik op de economische principes achter bitcoin en hoe deze aansluiten bij het gedachtegoed van de Oostenrijkse school.

d BTC Sessions

Een YouTube-kanaal voor alleen bitcoinonderwijs met nuttige tutorials en gidsen:
<https://www.youtube.com/@BTCSessions>

4. Cursussen:

a De zomer van Bitcoin

<https://www.summerofbitcoin.org> Een wereldwijd, online zomerstageprogramma gericht op het laten kennismaken van universiteitsstudenten met open-source bitcoinontwikkeling en -ontwerp.

Chaincode Labs

<https://learning.chaincode.com/#FOSS> - online cursussen waarmee studenten leren hoe ze mee kunnen helpen aan de ontwikkeling van het bitcoinprotocol.

Saylor Academy

Gratis onderwijs in meerdere disciplines:
<https://www.saylor.org/>

5. Belangrijke auteurs

-  Alex Gladstein: *Check Your Financial Privilege*
-  Alex Swan: *Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications*
-  Amanda Cavaleri: *Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide*
-  Anita Posch: *Learn Bitcoin: Become Financially Sovereign*
-  Eric Yakes: *The 7th Property: Bitcoin and the Monetary Revolution*
-  Jeff Booth: *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future*
-  Jimmy Song: *The Little bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future*
-  Nik Bhatia: *Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies*
-  Robert Breedlove: *Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money*
-  Lyn Alden: *Broken Money*

6. Geciteerde auteurs

 Curious Inventor:
<https://www.youtube.com/@CuriousInventor>

 Anil Patel:
Twitter: @anilsaidso

7. Andere bronnen:

-  **Bitcoin.org**: De officiële website van het bitcoinprotocol.
-  **Bitcointalk.org**: Bitcointalk is een forum waar gebruikers bitcoin gerelateerde onderwerpen kunnen bespreken, vragen kunnen stellen en informatie kunnen delen. Het is een geweldige plek om te leren van andere bitcoin enthousiastelingen en -experts.
-  **Bitcoincore.org**: Dit is de oorspronkelijke bitcoinsoftware en wordt nog steeds veel gebruikt door veel gebruikers en ontwikkelaars. Het biedt een krachtige set gereedschappen voor interactie met het Bitcoinnetwerk en het bouwen van bitcointoepassingen.
-  **Bitcoinwiki.org**: Dit is een community-gedreven bron die een uitgebreide gids biedt voor alles wat met Bitcoin te maken heeft. Alles komt aan bod, van de technische aspecten van Bitcoin tot de geschiedenis en het gebruik ervan.
-  **Bitcoinmagazine.com**: Dit is een online publicatie met nieuws en inzichten over bitcoin en andere cryptocurrencies. Het is een geweldige manier om op de hoogte te blijven van de laatste ontwikkelingen in het bitcoinecosysteem.
-  **Bitcoin.Design**: Een open-source opslagplaats van Bitcoin gerelateerde ontwerpbestanden voor illustraties, websites, sjablonen en pictogrammen.
-  **NOSTR**: <https://nostr.com/> - sociale media waar je daadwerkelijk eigenaar bent van je gegevens.
-  **Simple X**: <https://simplex.chat/> - een persoonlijk, gedecentraliseerd applicatieprotocol
-  **Een bitcoinnode opzetten: Raspberry Pi DIY door Keith Mukai**: https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?ab=README-ov-file
-  **Hoe kies je een bitcoin wallet**: <https://bitcoin.org/en/choose-your-wallet> - gebruik je nieuw verworven kennis om de juiste wallet voor jou te kiezen.
-  **Bitcoincons.com**: <https://bitcoincons.com/> - Een verzameling gratis bitcoin pictogrammen.
-  **Bitcoin voor bedrijven**: <https://bitcoinforlocalbusiness.com/> - Een set flyers om je te helpen de waarde van Bitcoin te delen met je favoriete lokale bedrijven.
-  **Mempool.Space**: <https://mempool.space/> - Een open-source mempoolproject dat ook gegevens en grafieken van het lightning netwerk bevat

Lesdoelen

Hoofdstuk 1:

Cursus introductie:

Ontdek de cursusdoelen en verwachtingen voor het bitcoindiploma

Reflectieve activiteit - geld definiëren:

Doe een reflectieoefening door vijf antwoorden te geven op belangrijke vragen over geld.

Discussie in de klas - waarom hebben we geld nodig?

 Neem deel aan een klassikale discussie over de fundamentele noodzaak van geld.

 Deel en vergelijk individuele perspectieven op het belang van geld.

 Leg de basis voor het begrijpen van de rol van geld in economische systemen

Hoofdstuk 2:

Geld begrijpen:

 Verken de fundamentele definitie en het concept van geld.

 Bespreek de verschillende perspectieven in de klas om de veelzijdige aard van geld te begrijpen.

Psychologie van geld:

 De psychologische aspecten begrijpen van geld, waaronder schaarste, tijdsvoorkeur en economische afwegingen.

 Doe de activiteit "tijdsvoorkeur" om psychologische elementen te koppelen aan levensechte scenario's.

Functies, eigenschappen en typen geld:

 Verdiep je in de functies, eigenschappen en soorten geld.

 Herken het belang van deze aspecten bij het definiëren en gebruiken van geld.

Hoofdstuk 3:

Introductie tot de geschiedenis en evolutie van geld:

Verken de geschiedenis en evolutie van geld. Begrijp hoe oude handelsvormen hebben geleid tot de ontwikkeling van de valuta die we vandaag de dag gebruiken.

De revolutie van digitaal geld

 Ontdek het huidige hoogtepunt in de evolutie van geld - digitale valuta.

 Begrijp de elektronische ervan en hoe het wereldwijd onmiddellijke, goedkope transacties mogelijk maakt.

 Lees meer over de belangrijke rol die bitcoin speelde bij het oplossen van de eerste uitdagingen van digitaal geld, en de voorbereiding voor wereldwijd gebruik.

De evolutie van geld:

Verken de overgang van oude vormen zoals schelpen en kralen naar het ontstaan van munten en papiergeld. Volg de reis van papier naar plastic en ontrafel de evolutie van geld door de geschiedenis heen.

Ruilhandel spel:

Doe mee aan een praktische ruilhandelervaring om de uitdagingen van directe ruil te begrijpen en de behoefte aan een efficiënter systeem in te zien.

Hoofdstuk 4:

De oorsprong van fiatgeld

Ontdek de oorsprong van fiatgeld aan de hand van een kort historisch overzicht en begrijp hoe het de dominante vorm van geld werd.

Activiteit: fractioneel bankieren

Krijg inzicht te krijgen in de werking van dit systeem, waarbij de nadruk ligt op de afhankelijkheid van schulden en de gevolgen voor de bredere economie.

Het fiatsysteem:

Begrijp de fundamentele aspecten van het fiatsysteem: een per decreet vastgesteld monetair systeem, de rol van fractioneel bankieren en de hoofdrolspelers die dit systeem controleren.

Hoofdstuk 5:

Afname van de koopkracht:

Begrijp het concept van monetaire inflatie en de invloed ervan op de koopkracht. Ervaar de effecten van inflatie middels een veiling.

Activiteit: de gevolgen van het fiatsysteem

Zie de gevolgen van het fiatsysteem en de bredere impact van het huidige monetaire kader.

Digitaal centralebankgeld

Verken het evoluerende landschap van digitaal centralebankgeld en de potentiële impact op de toekomst van geld.

Wereldwijde schuldenlast en sociale ongelijkheid:

Verken de dubbele impact van de wereldwijde schuldenlast en sociale ongelijkheid. Herken de individuele en maatschappelijke gevolgen van schulden, met de nadruk op het verlies aan koopkracht en de groeiende welvaarts kloof.

De cypherpunks en decentralisatie:

Leer het verhaal van de cypherpunks en hun motivatie om op zoek te gaan naar een gedecentraliseerd geld. Maak onderscheid tussen gecentraliseerde en gedecentraliseerde systemen en leer meer over de geschiedenis van digitaal geld.

Hoofdstuk 6:

Satoshi Nakamoto en bitcoin's ontstaan:

Verken de mysterieuze figuur Satoshi Nakamoto en het ontstaan van bitcoin, en krijg zicht op beweegredenen achter de ontwikkeling ervan

Activiteit: tot consensus komen:

Oefen om tot consensus te komen in een peer-to-peer netwerk om praktische inzichten te krijgen over de manier waarop consensus tot stand komt op het Bitcoinnetwerk.

Persoonlijke verantwoordelijkheid:

Benadruk het belang van persoonlijke verantwoordelijkheid bij het gebruik van bitcoin en krijg inzicht in de individuele rollen en verantwoordelijkheid binnen het gedecentraliseerde bitcoinecosysteem.

Hoe bitcoin werkt:

Leer hoe het consensusmechanisme van Nakamoto werkt. Identificeer de belangrijkste spelers in het Bitcoinnetwerk, zoals miners, nodes, gebruikers, ontwikkelaars en projecten, en snap hoe de onderlinge samenwerkingsdynamiek werkt.

Bitcoin als eerlijk geld:

Onderzoek de rol van bitcoin als eerlijk digitaal geld, bespreek de evolutie, functies en eigenschappen ervan en neem deel aan een klassikale discussie over de vraag of bitcoin in aanmerking komt als eerlijk geld.

Lesdoelen

Hoofdstuk 7:

-  **Peer-to-peer transacties:**
Doe mee aan gedecentraliseerde transacties om de basisprincipes van bitcoin te ervaren.
-  **Een bitcoinwallet opzetten:**
Leer de essentiële stappen om een bitcoinwallet te downloaden, keys aan te maken en een backup te maken voor veilige transacties.
-  **Sparen en je eigen onderzoek doen:**
Begrijp hoe bitcoin fungeert als spaarmiddel en het belang van onafhankelijk onderzoek voordat je besluiten neemt.

-  **Type bitcoinwallets:**
Maak onderscheid tussen open- en closed source, custodial- en noncustodial wallets en begrijp de rol van sleutels in beveiliging.
-  **Bitcoin verkrijgen:**
Verken methoden zoals peer-to-peer transacties en bespreek privacykwesties met betrekking tot ken-je-klant (KYC) processen.

Hoofdstuk 8:

-  **Introductie tot het lightningnetwerk:**
Leer over de evolutie van bitcoin en hoe de mogelijkheden worden vergroot door middel van technologieën zoals het lightningnetwerk
-  **Een lightningwallet opzetten:**
Leer de essentiële stappen om een lightningwallet op te zetten, waarmee snellere en schaalbaardere transacties mogelijk worden.
-  **Hands-on activiteit:**
Doe mee aan een lightningwalletestafette om een beter begrip te krijgen van transacties via het lightning netwerk.

-  **Type lightningwallets:**
Maak onderscheid maken tussen open-source en closed-source, custodial en non-custodial lightningwallets voor verschillende type gebruikers.
-  **Lightningtransacties:**
Verken het proces van het verzenden en ontvangen van lightning transacties, met de nadruk op de snelheid en efficiëntie van het lightning netwerk.

Hoofdstuk 9:

-  **Het bitcoinkasboek:**
Begrijp het concept van een gedecentraliseerd kasboek dat wordt gefaciliteerd door nodes en miners en hoe het transparantie en veiligheid garandeert.
-  **Het UTXO-model:**
Begrijp de Unspent Transaction Output als een fundamenteel aspect van bitcoin.
-  **Publieke- en privésleutels:**
Ontdek het belang van cryptografische beveiliging bij bitcointransacties door middel van public en private keys, samen met een activiteit waarbij SHA-256 hashing wordt gedemonstreerd.

-  **Bitcoin, nodes en miners:**
Kijk naar de rol van nodes en miners in het onderhouden van het bitcoinnetwerk, waarbij aspecten als uitgifte, schaarste, halvering en moeilijkheid aan bod komen.
-  **Hoe bitcointransacties werken:**
Krijg inzicht in de hele levenscyclus van een bitcointransactie, waarbij de verzender, ontvanger, nodes, miners en de mempool betrokken zijn, met een speciale activiteit gericht op de mempool.

Hoofdstuk 10:

Filosofische onderbouwing van bitcoin:

Verken de basisfilosofie achter bitcoin en begrijp hoe het is ontstaan als antwoord op economische uitdagingen, met de nadruk op financiële vrijheid en hoe het verschilt van traditioneel geld.

De toekomst van bitcoin

Verdiep je in de toekomstige ontwikkelingen van bitcoin als revolutionair digitaal geld.

Reflectie op het bitcoindiploma:

-  Vat de belangrijkste punten van het bitcoindiploma samen en moedig studenten aan om na te denken over hun reis en de verworven inzichten.
-  Activiteiten zijn onder andere het bekijken van een video over "waarom bitcoin?" en het opnieuw bekijken van de vragen van hoofdstuk 1 om de persoonlijke groei en de nieuw verworven kennis te evalueren.

Woordenlijst

2-Factor Authenticatie (2FA): Een beveiligingsmaatregel die twee authenticatiemethoden vereist, meestal een wachtwoord en een aparte code of apparaat, om toegang te krijgen tot een account of een transactie te voltooien.

51%-Aanval: Een type aanval op een blockchain netwerk waarbij een enkele entiteit of groep de controle heeft over de rekenkracht van het netwerk, waardoor ze transacties kunnen manipuleren en mogelijk het netwerk kunnen verstoren.

Altcoinseizoen: Een periode waarin alternatieve cryptocurrencies een aanzienlijke prijsstijging doormaken, vaak als gevolg van een verhoogde interesse en adoptie van investeerders.

Altcoins: Digitale valuta met uitzondering van bitcoin.

Atomic swap: Een peer-to-peer uitwisseling van cryptocurrencies van verschillende blockchains zonder de noodzaak van een gecentraliseerde exchange of tussenpersoon.

Bevestiging: Het proces waarbij een transactie wordt verwerkt door het netwerk en het teruggedraaien ervan hoogst onwaarschijnlijk wordt. De miners verifiëren de authenticiteit van transacties met hun computer hardware en software. Het wordt aanbevolen om minstens zes bevestigingen af te wachten om 'double spend' te voorkomen.

Consensusmechanisme: Een methode die in blockchaintechnologie wordt gebruikt om transacties te valideren en de integriteit van de blockchain te waarborgen.

Bitcoin: Een vorm van digitaal geld of systeem waarmee mensen geld naar elkaar kunnen sturen zonder een derde partij zoals een bank nodig te hebben.

Block explorer: Een tool die gebruikt wordt om de blockchain te bekijken en te verkennen, waarbij gebruikers individuele blocks, transacties en walletadressen kunnen bekijken.

Block reward: Het aantal nieuwe bitcoins dat wordt toegekend aan miners voor het toevoegen van een nieuw block aan de blockchain.

Blockchain: Een openbaar verslag van alle bitcoin transacties die hebben plaatsgevonden.

BTC: De eenheid die wordt gebruikt voor Bitcoin, een digitale valuta waarmee aankopen kunnen worden gedaan en kan worden verhandeld.

Centralebank: Een overheidsinstelling die het monetaire beleid van een land beheert.

Centralisatie: De concentratie van macht of controle in een kleine groep of zelfs een enkele entiteit.

Cold storage: Een methode om bitcoins offline op te slaan, weg van het risico van hackers of andere online bedreigingen.

Cryptocurrency exchange: Een platform waar gebruikers cryptocurrencies kunnen kopen, verkopen en verhandelen voor andere activa zoals fiatvaluta of andere cryptocurrencies.

Cryptocurrency wallet: Een softwareprogramma waarin private keys worden opgeslagen en waarmee gebruikers hun cryptocurrencies kunnen verzenden, ontvangen en beheren.

Cryptografie: Een tak van de wiskunde die helpt bij het maken van veilige systemen.

Decentrale Autonome Organisatie (DAO): Een organisatie of netwerk bestuurd door smart contracts en gerund op een blockchain zonder centrale autoriteit of managementstructuur.

Decentralisatie: De verdeling van macht en controle over een grote groep mensen of een netwerk in plaats van een centrale autoriteit.

Decentralized Finance (DeFi): Een beweging binnen de cryptocurrency industrie om gedecentraliseerde financiële producten en diensten te creëren die werken op een blockchain.

Digitaal bezit: Een digitale weergave van waarde die kan worden verhandeld of gebruikt als een waardeopslag, zoals een hoeveelheid bitcoin.

Digitale handtekening: Een wiskundig mechanisme waarmee iemand eigendom kan bewijzen.

Double spend: Wanneer een persoon probeert zijn bitcoin naar twee verschillende ontvangers op hetzelfde moment te sturen.

Gecentraliseerd systeem: Een systeem waarin macht of controle geconcentreerd is in een kleine groep of een enkele entiteit.

Gedecentraliseerd systeem: Een systeem waarin macht of controle verdeeld is over een groot aantal entiteiten.

Gedistribueerd kasboek: Een kasboek dat verspreid is over een netwerk van computers in plaats van opgeslagen op een centrale locatie.

Geldhoeveelheid: De totale hoeveelheid geld in omloop in een economie.

Geldontwaarding: De waardevermindering van een valuta.

Goederengeld: Voorwerpen die door veel mensen als waardevol beschouwd worden en gebruikt worden als ruilmiddel, zoals goud of zilver.

Handelspaar: Een set van twee valuta of activa die tegen elkaar kunnen worden verhandeld op een beurs.

Woordenlijst

Herstelzin (seedphrase): Een reeks van 12, 18 of 24 woorden die gebruikt kunnen worden om meerdere paren van private en public keys te genereren. Deze kunnen gebruikt worden om een bitcoinwallet te herstellen.

Kasboek: Een gestructureerd openbaar overzicht van alle transacties die zijn gedaan op het Bitcoin-netwerk.

Kapitaalbeperkingen: Beperkingen op het grensoverschrijdend verkeer van geld.

Koopkracht: Het vermogen van geld om goederen en diensten te kopen.

Mand met goederen: Een verzameling goederen of diensten die wordt gebruikt om veranderingen in de kosten van levensonderhoud te meten.

Merkle trees: Een boomachtige datastructuur die in de blockchain wordt gebruikt om de integriteit van grote verzamelingen gegevens efficiënt te verifiëren.

Mining pool: Een groep miners die samenwerkt om de kans op het vinden van nieuwe blocks en het verdienen van bitcoin te vergroten.

Mining: Het proces waarbij computerhardware wordt gebruikt om wiskundige berekeningen uit te voeren om transacties te bevestigen en de veiligheid van het Bitcoinnetwerk te vergroten.

Monetair en fiscaal beleid: Het beleid van respectievelijk een centralebank en de overheid dat de geldhoeveelheid en rentetarieven in een economie beïnvloedt.

Multi-signature (multisig) Wallet: Een wallet die meerdere handtekeningen of goedkeuringen vereist voordat een transactie kan worden uitgevoerd, wat extra veiligheid en controle biedt.

Multi-signature: Een beveiligingsfunctie die meer dan één private key vereist om een bitcointransactie te autoriseren.

Netwerk: Een groep van onderling verbonden entiteiten.

Node: Een computer of apparaat dat is aangesloten op het Bitcoinnetwerk en deelneemt aan de verificatie en verzending van transacties.

Node netwerk: Een netwerk van verbonden computers of apparaten die het Bitcoinnetwerk ondersteunen en onderhouden.

Nonce: Een willekeurig getal dat aan een block header wordt toegevoegd om een hash te maken die voldoet aan de moeilijkheidsdoelstelling.

Non-Fungible Token (NFT): Een type digitaal bezit dat een uniek of one-of-a-kind item vertegenwoordigt, vaak gebruikt om kunst, verzamelobjecten of andere unieke objecten te vertegenwoordigen.

Orphan block: Een block dat niet is opgenomen in de hoofdketen van de blockchain omdat het ongeldig is gemaakt door een langere concurrerende keten.

Papieren wallet: Een stuk papier waarop de private en public keys van een gebruiker staat om cryptocurrency offline op te slaan en te beheren.

Peer-to-peer (P2P): Een gedecentraliseerd netwerk waarin deelnemers direct met elkaar communiceren in plaats van via een centrale autoriteit.

Peg: Een vaste wisselkoers tussen twee valuta's waarbij de ene is gekoppeld aan de waarde van een andere.

Private blockchain: Een blockchain die gecontroleerd wordt door één organisatie in plaats van gedecentraliseerd te zijn.

Private key: Een geheim stuk data dat iemand de mogelijkheid geeft om bitcoin van een specifieke wallet uit te geven door middel van een cryptografische handtekening.

Proof-of-Stake (PoS): Een consensusmechanisme dat wordt gebruikt in sommige blockchain-netwerken. Het vereist dat gebruikers een bepaalde hoeveelheid cryptocurrency vastzetten (stake) om deel te nemen aan de validatie van transacties.

Proof-of-Work (PoW): Een consensusmechanisme dat vereist dat gebruikers een bepaalde hoeveelheid rekenwerk uitvoeren om deel te nemen aan het netwerk.

Publieke blockchain: Een blockchain die voor iedereen toegankelijk is om aan deel te nemen en transacties te verifiëren, waardoor deze gedecentraliseerd is.

Public key/bitcoinadres: Een openbaar wachtwoord/nummer dat wordt gebruikt om bitcoin te ontvangen. Het is afgeleid van de private key van een gebruiker via een wiskundig proces.

Rekeneenheid: Een standaard meeteenheid die wordt gebruikt om de waarde van goederen en diensten uit te drukken.

Reserveratio: Het deel van de deposito's dat een bank moet aanhouden als reserves.

Restrictief bankieren: Beperkingen op bankdiensten of toegang tot bankdiensten.

Ruilhandel: De uitwisseling van goederen en diensten zonder het gebruik van geld.

Woordenlijst

Ruilmiddelen: Goederen, fysiek of digitaal die algemeen geaccepteerd worden in ruil voor goederen en diensten.

Satoshi Nakamoto: Het pseudoniem dat werd gebruikt door de anonieme maker(s) van Bitcoin.

Satoshi: De kleinste eenheid van Bitcoin, gelijk aan 1/100.000.000 van een bitcoin. Het is vernoemd naar de maker van Bitcoin, Satoshi Nakamoto.

Satoshis per byte (sat/b): Een eenheid die wordt gebruikt om het bedrag aan bitcointransactiekosten te meten dat wordt betaald per byte aan transactiegegevens.

Schuld: Geld dat aan iemand anders verschuldigd is.

SegWit (segregated witness): Een upgrade van het bitcoinprotocol die de manier verandert waarop gegevens worden opgeslagen op de blockchain, waardoor een grotere capaciteit en lagere transactiekosten mogelijk worden.

Sidechain: Een blockchain die verbonden is met een andere blockchain, waardoor de overdracht van activa of informatie tussen de twee ketens mogelijk is.

Smart contract: Een zelfuitvoerend contract met de voorwaarden van de overeenkomst in code geschreven.

Soft fork: Een wijziging in het bitcoinprotocol die compatibel is met oudere versies van de software.

Stablecoin: Een type cryptocurrency dat is ontworpen om een stabiele waarde te behouden, vaak door te worden gekoppeld aan een fiatvaluta of ander activum.

Tijdswaarde van geld: Het principe dat geld in het heden meer waard is dan in de toekomst.

Token: Een waarde-eenheid gecreëerd op een blockchain, vaak gebruikt om een specifieke asset of utility binnen een bepaald ecosysteem te vertegenwoordigen.

Tokenisering: Het proces van het creëren van een digitale representatie van een activum of activaklasse op een blockchain, wat fractioneel eigendom en overdraagbaarheid mogelijk maakt.

Transactie ID: Een reeks cijfers en letters die de details van een bitcoin overdracht weergeeft (zoals het verzonden bedrag, de adressen van de verzender en ontvanger, en de datum van de overdracht) op de blockchain.

Transactie: De overdracht van bitcoins van het ene adres naar het andere op het bitcoinnetwerk.

Transactievergoeding: Een klein bedrag aan bitcoins betaald door de verzender van een transactie, waardoor miners worden gestimuleerd om de transactie op te nemen in een block en toe te voegen aan de blockchain.

Toevallig samenvallen van behoeften: Het fenomeen waarbij twee partijen in een ruileconomie allebei hebben wat de andere partij wil en willen hebben wat de andere partij heeft.

Veiling: Een proces waarbij goederen of activa worden verkocht aan de hoogste bidder.

Vertrouwenloos: Een systeem of handeling die geen vertrouwen in een derde partij of tussenpersoon vereist, maar vertrouwt op de veiligheid en transparantie van de onderliggende technologie.

Volatiliteit: De mate van variatie in de prijs van een activum in een bepaalde tijd.

Vraag en aanbod: Het economische principe dat de prijs van goederen of diensten wordt bepaald door de wisselwerking tussen de hoeveelheid aangeboden goederen of diensten en de gevraagde hoeveelheid.

Walletadres: Een unieke identificatie die wordt gebruikt om bitcoins te verzenden en ontvangen op het bitcoinnetwerk, meestal weergegeven als een reeks letters en cijfers.

Walletbackup: Een kopie van de private keys en herstelzin/seed van een bitcoinwallet, die gebruikt kan worden om toegang tot de wallet te herstellen in het geval dat het origineel verloren of gestolen is.

Wallet: Een virtuele container voor bitcoins, vergelijkbaar met een fysieke wallet, die de private key(s) bevat waarmee bitcoins die eraan zijn toegewezen kunnen worden uitgegeven.

Whale: Een persoon of organisatie die een aanzienlijke hoeveelheid cryptocurrency bezit en in staat is om de marktprijzen te beïnvloeden door middel van grote transacties.

White-hat hacker: Een ethische hacker die zijn vaardigheden gebruikt om kwetsbaarheden in computersystemen en netwerken te identificeren en te verhelpen.

Whitepaper: Een document dat het probleem en de bijbehorende oplossing uiteenzet dat een blockchainproject of cryptocurrency tracht op te lossen.

XBT en BTC: Afkortingen voor bitcoin.

Vertaling Engels - Nederlands

acceptability - aanvaardbaarheid	durability - duurzaamheid
altcoins - altcoins	e-Gold - e-Gold
atomic swap - atomic swap	established history - gevestigde geschiedenis
Austrian school of economics - Oostenrijkse school van de economie	exchange rate - wisselkoers
barter - ruilhandel	exchange rate policies - wisselkoersbeleid
basket of goods - mand met goederen	expansionary fiscal policy - expansief begrotingsbeleid
bearer asset - bezitsactivum	fees - vergoedigen
bitcoin address - bitcoinadres	fiat currency - fiatvaluta
bitcoin blockchain - bitcoinblockchain	fiat money - fiatgeld
bitcoin ledger - bitcoinkasboek	fiat system - fiatsysteem
bitcoin network - bitcoinnetwerk	fractional reserve banking - fractioneel bankieren
bitcoin node - bitcoinnode	funding - geld storten
bitcoin protocol - bitcoinprotocol	fungibility - uitwisselbaarheid
bitcoin transactions - bitcointransacties	gatekeepers - poortwachters
bitcoin wallet - bitcoinwallet	genesis block - genesis block
block - block	halvening - halvening
block explorer - block explorer	halving - halving
block reward - block reward	halving event - halving moment
block subsidy - block subsidy	halvings - halvings
blockchain - blockchain	hard fork - hard fork
blockchains - blockchains	hash - hash
broadcast - broadcast	hash functions - hash functies
broadcasting - broadcasten	hashing - hashing
candidate block - template block	hot wallet - hot wallet
capital controls - kapitaalbeperkingen	hyperbitcoinization - hyperbitcoinization
copyright resistant - bestand tegen censuur	key concepts - begrippen
centralized exchanges - gecentraliseerde exchanges	ledger - kasboek
channel operator - beheerder van het kanaal	legal tender - wettig betaalmiddel
circular economies - circulaire economieën	lightning invoice - lightning invoice
circulating supply - hoeveelheid in omloop	lightning network - lightningnetwerk
class discussion - discussie in de klas	lightning transactions - lightningtransacties
class exercise - oefening in de klas	lightning wallet - lightningwallet
closed-source - closed-source	medium of exchange - ruilmiddel
cold storage - cold storage	memory pool - memory pool
commodities - goederen	mempool - mempool
commodity money - goederengeld	merkle trees - merkle trees
communities - gemeenschappen	mined - gemined
consensus mechanism - consensusmechanisme	miners - miners
contractionary fiscal policy - krimpend begrotingsbeleid	mining - mining
cryptocurrencies - cryptovaluta	mining reward - mining reward
custodial - custodial	monetary inflation - monetaire inflatie
cyberpunks - cypherpunks	monetary system - monetaire systeem
debasement - geldontwaarding	multi-signature - multi-handtekening
debt burden - schuldenlast	multisig - multisig
decentralized currency - gedecentraliseerd geld	node - node
decentralized finance - decentralized finance	nodes - nodes
decentralized ledger - gedecentraliseerd kasboek	non custodial - self-custodial
decentralized systems - gedecentraliseerde systemen	nonce - nonce
depositors - depositohouders	off-chain - off-chain
difficulty adjustment - difficulty adjustment	on-chain - on-chain
digital assets - digitale bezittingen	open source - open-source
digital currencies - digitale valuta	payment rails - betaalinfrastuctuur
digital money - digitaal geld	peer-to-peer - peer-to-peer
digital signature - digitale handtekening	physical money - fysiek geld
distributed Ledger - gedistribueerd kasboek	pigpen cipher - pigpen-code
divisibility - deelbaar(heid)	plugin - plug-in
double coincidence of wants - samenvallen van behoeften	plugins - plug-ins
double spend - dubbele uitgave	portability - draagbaarheid
	private keys - private keys

private-key cryptography - cryptografie met private keys
proof-of-stake - proof-of-stake (PoS)
proof-of-work - proof-of-work (PoW)
public keys - public keys
purchasing power - koopkracht
recovery phrase - seed phrase
relay race - estafette
representative money - goederengeld
reserve ratio - reservevereiste
satisfaction - voldoening
satoshis - satoshis
sats - sats
scarce - schaars
scarcity - schaarsheid
seed - seed
seed phrase - seed phrase
segregated witness - segregated witness
self custodial - self-custodial
self custody - self-custody
self-sovereign - zelf-soeverein
sending bitcoin - bitcoin versturen
sidechain - sidechain
signed transaction - ondertekende transactie
smart contract - smart contract
sound - eerlijk
sound digital money - eerlijk digitaal geld
sound money - eerlijk geld
stablecoin - stablecoin
store of value - spaarmiddel
supply schedule - leveringsschema
tab - rekening
teacher - docent
third party - derde partij
time preference - tijdsvoorkeur
time-stamping - time-stamping
time-stamps - time-stamps
to control money - geld beheren
to send - versturen
to send and receive - versturen en ontvangen
token - token
tokenization - tokenisering
trading pair - handelspaar
transaction fee - transactievergoeding
transactions - transacties
two-factor authentication - 2-factor authenticatie
unbanked - zonder bank
unit of account - rekeneenheid
unsound - oneerlijk
unsound digital money - oneerlijk digitaal geld
unsound money - oneerlijk geld
valid block - geldig block
verifiable - verifieerbaarheid
volatility - volatiliteit
vouchers - vouchers
wallet - wallet
whale - whale
white hat hacker - white hat hacker
whitepaper - whitepaper
who controls the money - wie beheert het geld



Nederlandse versie | 2024
ISBN: 9789916749180