Het Genesisboek

Het Genesisboek

Het verhaal van de mensen en projecten die aan de basis stonden van Bitcoin

Aaron van Wirdum

KONSENSUS NETWORK

The Genesis Book: The Story of the People and Projects That Inspired Bitcoin
Uitgegeven door Bitcoin Magazine Books

Het Genesisboek: Het verhaal van de mensen en projecten die aan de basis stonden van Bitcoin

Uitgever: *konsensus.network*

v1.1.0

ISBN 978-9916-749-40-1 Hardcover
978-9916-749-41-8 Paperback
978-9916-749-43-2 E-book

KONSENSUS NETWORK

Inhoudsopgave

III BITCOIN

Over dit boek

Bitcoin is niet zomaar uit het niets ontstaan. Al decennia vóór de uitvinding van Satoshi Nakamoto probeerden groepen computerwetenschappers, privacy-activisten en alternatieve economen een digitale vorm van geld te ontwikkelen die onafhankelijk van de overheid kon bestaan. Het Genesisboek vertelt het verhaal van de mensen en projecten die de weg vrijmaakten voor 's werelds eerste succesvolle peer-to-peer elektronisch betaalsysteem.

Reviews

'Ik had al enige tijd het vermoeden dat Van Wirdum de beste historicus van Bitcoin is, en dit boek bevestigt dat.

Het is een indrukwekkend werk. Het Genesisboek biedt een toegankelijk en essentieel overzicht van de geschiedenis, en onthult de vele verbanden tussen het Weense klassiek-liberalisme, de Anglo-Saksische Cypherpunkbeweging en de opkomst van Bitcoin.

Waar andere boeken in de branche vaak de nadruk leggen op veelgeprezen ondernemers, heeft Van Wirdum de technische kennis om belangrijke figuren te belichten die de fundamenten legden waarop het Bitcoin-gebouw later is opgericht.

In zestien informatieve hoofdstukken biedt Het Genesisboek een combinatie van diepgaand onderzoek en filosofische inzichten die je alleen verwacht van een veteraan in de sector (Van Wirdum was een van de eerste schrijvers die in de Bitcoin-industrie aan de slag ging), met de aantrekkelijke schrijfstijl die je zoekt in een gerespecteerd tijdschrift.

Je kunt Bitcoin niet begrijpen zonder kennis te maken met zijn bijzondere oorsprong, en ik ben blij dat dit boek bestaat om die kennis voor een breed publiek toegankelijk te maken.'

— Tuur Demeester

'Het Genesisboek neemt je mee op een eeuwenlange reis door minder bekende verhalen van visionairs, wiens inzichten en innovaties de basis vormden voor de revolutionaire creatie van Bitcoin. Van economen die de gevestigde orde uitdaagden tot Cypherpunks

die nieuwe wegen op het gebied van privacy verkenden, weeft Aaron van Wirdum zorgvuldig een verhaal over technologische overwinningen, tegenslagen en bijzondere doorbraken. De anekdotes over mensen die buiten de gebaande paden durfden te dromen en grenzen verlegden om de financiële wereld te veranderen, zullen je zeker fascineren.'

— Jameson Lopp

'Waarom verschilt Bitcoin zo van eerdere versies? Dit boek werpt licht op de problemen *die slimme en hardwerkende mensen in de tijd vóór Bitcoin bezig hielden. Dit is de juiste manier om het verhaal van een technologie te vertellen. Alle belangrijke kwesties worden behandeld en zijn in een logische volgorde gepresenteerd. Dit is het beste boek dat ooit over Bitcoin geschreven is.'*

— Paul Sztorc

'Tot nu toe waren er veel boeken over Bitcoin, maar geen enkel boek pakte de veelzijdige culturele achtergrond zo compleet, gestructureerd en elegant aan. Aaron van Wirdum, bekend om zijn talent om technische materie helder naar een breder publiek over te brengen, heeft dat nu gedaan. Dit is een must-read *als je wilt begrijpen waar Bitcoin vandaan komt.'*

— Giacomo Zucco

Openingscitaat

Ik geloof niet dat we ooit weer een goede munteenheid zullen hebben voordat we het uit de handen van de overheid nemen. Aangezien we ze niet gewelddadig uit de handen van de overheid kunnen nemen, kunnen we alleen maar op een sluwe, indirecte manier, iets introduceren wat ze niet kunnen stoppen. - Friedrich Hayek (1984)

Inleiding

E-gold was in volle bloei. Tegen het jaar 2005 had het innovatieve online betalingssysteem van Douglas Jackson meer dan een miljoen accounts, die samen verantwoordelijk waren voor bijna $ 2 miljard aan transacties per jaar. De volledig gedekte digitale tokens die e-goldklanten gebruikten om al deze transacties uit te voeren, vertegenwoordigden 3,8 ton goud, opgeborgen in kluizen over de hele wereld. Als een van de eerste werkende implementaties van elektronisch geld, was e-gold in minder dan tien jaar tijd uitgegroeid tot de populairste digitale valuta op het internet.

Maar Jackson stond een onaangename verrassing te wachten. In december 2005, net voor het einde van het jaar, voerde de Amerikaanse geheime dienst een inval uit bij zijn bedrijf en zijn woning in Melbourne, Florida. Ze namen boeken en administratieve gegevens mee, en federale agenten namen alles wat zelfs maar enigszins interessant leek in beslag: naast juridische documenten en zakelijke contracten, omvatte dit ook het adresboek van zijn vrouw, de paspoorten van hun kinderen en de creditcards van op het nachtkastje. Op datzelfde moment werden de servers van e-gold, in een AT&T-gebouw in Orlando, zo'n 110 kilometer verder naar het noordwesten, offline gehaald, en werden alle transactiegegevens in beslag genomen.

De Amerikaanse geheime dienst, bijgestaan door de IRS en de FBI, was van mening dat de betalingsverwerker een broedplaats was geworden voor criminelen, die met slechts een e-mailadres hun e-goldaccounts konden aanmaken — dus vrijwel anoniem. In een tijdperk waarin creditcardfraude op het internet hoogtij vierde, zou het betaalsysteem van Jackson als een magneet voor oplichters

functioneren. Erger nog, wetshandhavers vermoedden dat kinderpornografen en terroristen van de relatieve anonimiteit van e-gold misbruik maakten.

Jackson werd aangeklaagd en beschuldigd van het witwassen van geld en het runnen van een niet-gelicentieerde betaaldienst.[1]

Digitaal goud

Jackson had nooit beoogd dat e-gold voor illegale doeleinden misbruikt zou worden. Hij geloofde ook niet dat dit op een serieuze schaal gebeurde. Sterker nog, hij beweerde dat e-gold een beter fraudedetectiesysteem had dan elke andere bestaande betalingsverwerker. Daarnaast was hij altijd meer dan bereid om met politie samen te werken. E-gold was ook een van de oprichtende leden van het *National Center for Missing & Exploited Children's Financial Coalition Against Child Pornography*. De gegevens die deze coalitie verzamelde, zo stelde Jackson, gaven aan dat e-gold vrijwel niet voor dergelijke doeleinden werd gebruikt.

Jackson, als succesvol en onafhankelijk oncoloog en veteraan van het medisch korps van het Amerikaanse leger, was in de jaren negentig al geïnteresseerd geraakt in het monetaire beleid en de invloed daarvan op de economie. Hij ontdekte dat moderne valuta – dollars, ponden, yen – niet langer gedekt waren, waardoor ze in feite, uit het niets, met een druk op de knop gecreëerd konden worden. Toen hij zich verder in het onderwerp verdiepte, raakte hij ervan overtuigd dat dit de economie op zeer schadelijke manieren beïnvloedde.

Jackson was dus van plan om een alternatief aan te bieden.

Tijdens zijn onderzoek naar valuta, ontwikkelde Jackson een hernieuwde waardering voor het *klassieke geld* – goud. Hij ontdekte dat mensen ten minste sinds de pre-dynastieke Egyptische tijd waarde hechtten aan dit glanzende, gele metaal, en dat met goede reden: het natuurlijke element werd niet beïnvloed door de willekeur van mensen.

Het pre-dynastieke Egypte was echter allang verdwenen en zelfs Jackson moest toegeven dat het kostbare metaal voor dagelijkse transacties niet echt praktisch was. Nu het nieuwe millennium naderde, besefte Jackson dat mensen niet gingen

1 Lawrence H. White, *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and e-gold*, Cato Journal, 34, No. 2: 281–301.

terugkeren naar de tijd waarin ze betaalden met gouden munten. Sterker nog, zelfs koperen munten en papiergeld zouden waarschijnlijk binnenkort ouderwets lijken.

Nee, de toekomst van geld moest digitaal zijn.

Met dat toekomstbeeld zag Jackson (heel letterlijk) een gouden kans. Hij bundelde de krachten met advocaat Barry Downey en richtte in 1996, onder zijn leiderschap, *Gold & Silver Reserve Inc.* op. De start-up zou een betalingssysteem voor de eenentwintigste eeuw runnen, maar dan wel gebaseerd op dat klassieke geld. Ze zouden een elektronisch equivalent voor goud leveren: *e-gold*.

Het basisidee was simpel. *Gold & Silver Reserve Inc.* huurde kluizen die ze vulden met het fysieke, gouden metaal zelf. Voor elk stuk goud in deze kluizen gaf het bedrijf een digitale *token* uit — in feite een nummer in een database. De tokens vertegenwoordigden een claim op het goud. Als iemand tokens had die gelijk stonden aan tien gram goud, was tien gram goud in een van de kluizen wettelijk van hen.

De belangrijkste innovatie was dat *Gold & Silver Reserve Inc.* ook een server in stand hield die een openbaar toegankelijk boekhoudsysteem voor de tokens huisvestte. Mensen van over de hele wereld konden op de server inloggen en een persoonlijke rekening aanmaken, waardoor ze tokens naar en van elke andere rekening konden sturen en ontvangen. Bij elke transactie werkte *Gold & Silver Reserve Inc.* de rekeningsaldi dienovereenkomstig bij.

Dankzij de kracht van het internet, konden e-gold gebruikers elkaar dus in wezen over grote afstanden, direct, en tegen minimale kosten, betalen. Op de grenzeloze *informatiesnelweg* kon iedereen met een internetverbinding iemand anders betalen, zonder beperkingen door nationale grenzen of bankregels.

Jackson creëerde e-gold, zo zei hij vaak, als een instelling om het materiële welzijn van de mensheid te bevorderen door toegang te bieden tot wereldwijde markten:

'In tegenstelling tot andere, is e-gold een betalingssysteem dat mensen van elke regio of economische achtergrond wereldwijd laat opereren: een migrant kan gemakkelijk waarde naar huis sturen en een handelaar kan betalingen accepteren van iemand in een derdewereldland die misschien geen toegang heeft tot een creditcard of bankreke-

ning.'[2]

Bovendien beweerde Jackson dat e-gold de mogelijkheid bood om een soort geld te gebruiken dat bestand is tegen inflatie. Omdat het digitaal was, was e-gold eigenlijk voor veel mensen toegankelijker dan echt goud.

Op de lange termijn had e-gold zelfs het potentieel om de ruggengraat van een geheel nieuw financieel systeem te worden, suggereerde Jackson optimistisch.

'Hoe vinden we een bankensysteem uit dat geen catastrofale verstoringen veroorzaakt, dat zelf het minst waarschijnlijk is om schommelingen te introduceren en dat het meest waarschijnlijk de juiste aanpassingen zal maken… is het meest prangende, onopgeloste economische probleem van onze tijd', citeerde hij op een gegeven moment uit het boek *The Rationale of Central Banking and the Free Banking Alternative* van econome Vera Smith.

'Een systeem en munteenheid zoals e-gold, vooral na opkomst en integratie in de financiële mainstream als reserve-activum dat als betaalmiddel wordt gebruikt, kan dit probleem zeker en vast oplossen.'[3]

Juridische kwesties

Vroeg in de jaren 2000 groeide e-gold snel, en Jackson werkte onvermoeid om zijn dienst te verbeteren. Hij stelde meer soorten edelmetalen beschikbaar, en voegde tevens nieuwe betalingsfuncties toe, zoals geautomatiseerde, maandelijkse betalingen. Bovendien maakte hij toegang tot het systeem mogelijk via mobiele telefoons via het toen nieuwe WAP-protocol.[4]

Maar Jackson was iets vergeten: hij had zijn bedrijf niet als betaaldienst geregistreerd. Daardoor voerde hij ook niet alle vereiste types van *Know-Your-Customer* (KYC) en *Anti-Money Laundering* (AML) controles uit. Hij was zich er niet van bewust dat hij dat moest doen.

---

2 Huis van Afgevaardigden, *Deleting Commercial Pornography Sites From the Internet: The U.S. Financial Industry's Efforts to Combat This Problem*, Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, One Hundred Ninth Congress, Second Session, 21 september 2006, online

3 White, *Troubling Suppression*, 289.

4 e-gold, *e-gold News*, December 1999, geraadpleegd online

Het was niet zo dat hij nonchalant was. Het werd pas een federale misdaad om zonder licentie als betaaldienst te opereren na de invoering van de *Patriot Act*, die in het leven werd geroepen als reactie op de terroristische aanslagen van 11 september 2001, enkele jaren na de lancering van e-gold. Nog belangrijker: het was niet duidelijk dat Jacksons onderneming überhaupt als een betaaldienst beschouwd zou worden. Het e-goldsysteem verstuurde geen dollars of andere nationale valuta, waarvoor zulke regels doorgaans van toepassing waren.

Desondanks had Jackson geprobeerd meer duidelijkheid te krijgen over de kwestie. *Gold & Silver Reserve Inc.* had aan de relevante overheidsinstanties zelf voorgesteld dat e-gold voor reguleringsdoeleinden gecategoriseerd kon worden als valuta, waardoor het bedrijf zich ook als een valutawisseldienst kon registreren. Maar als reactie hierop had het Amerikaanse ministerie van Financiën opnieuw bevestigd dat de definities van valuta niet op e-gold van toepassingen waren.

Bovendien had Jackson bij een agentschap van het ministerie van Financiën vrijwillig een conformiteitsonderzoek op de Bankgeheimwet gestart, puur om erachter te komen hoe zij dachten dat zijn bedrijf gereguleerd moest worden.[5] Toen de invallen plaatsvonden, wachtte hij nog op een antwoord.

De daaropvolgende juridische procedures brachten ernstige schade toe aan de e-goldonderneming. Bankrekeningen werden bevroren en bedrijfsgelden in beslag genomen. De juridische strijd die zich tussen Jackson en de Amerikaanse regering ontvouwde, duurde twee jaar en putte zijn middelen uit: de juridische kosten zouden uiteindelijk oplopen tot in de miljoenen. En voor zover het bedrijf van Jackson nog kon functioneren, moest dat nu onder een zweem van verdenking gebeuren.

Intussen had de Amerikaanse overheid beslagleggingsbevelen uitgevaardigd om achtenvijftig grote e-goldaccounts te sluiten op verdenking van witwassen. De doelwitten van de actie waren onafhankelijke e-goldbeurzen, waarvan sommige in het buitenland gevestigd waren. Op basis van de *Racketeering Act* uit 1961 (oorspronkelijk opgesteld om georganiseerde misdaad te bestrijden) werd 1.000 kilogram goud (ongeveer een kwart van de totale voorraad van e-gold) in beslag genomen en geliquideerd.

5 e-gold, *e-gold Welcomes US Government Review of its Status as a Privately Issued Currency*, 20 januari 2006, geraadpleegd online

Toen er in 2008 eindelijk een voorlopig vonnis kwam, bepaalde de rechter dat e-gold inderdaad een betaaldienst was, en verwierp daarmee Jacksons verzoek om de zaak te seponeren. Aangezien hij nu geconfronteerd werd met de mogelijkheid op een aanzienlijke gevangenisstraf en enorme boetes, besloot Jackson een schikking te treffen.[6]

In een van de weinige positieve wendingen in het hele verhaal toonde de rechter in haar uiteindelijke vonnis enige mildheid. Ze stelde dat 'de intentie om illegale activiteiten te ondernemen er niet was'.[7] Toch werd Jackson veroordeeld tot zesendertig maanden voorwaardelijke vrijlating (huisarrest), waarvan zes werden afgedwongen door middel van een enkelband. Hij moest ook een werkstraf van 300 uur uitvoeren en een boete van $ 200 betalen. Zijn bedrijf kreeg ondertussen een boete van $ 600.000. Twee van zijn werknemers – medeoprichters Barry Downey en Douglas' broer Reid Jackson – werden veroordeeld tot zesendertig maanden voorwaardelijke vrijlating, 300 uur werkstraf en een boete van $ 2.500 plus een boete van $ 100.

En natuurlijk moest e-gold een licentie verkrijgen voor het opereren van een betaaldienst. Het enige probleem? Als veroordeelde misdadiger kwam Jackson niet langer in aanmerking voor zo'n licentie, iets wat hij niet onmiddellijk had beseft toen hij met de schikking instemde. Net toen hij dacht dat hij eindelijk de juridische strijd voor altijd kon achterlaten en zijn bedrijven op welke manier dan ook kon proberen te redden, ontdekte Jackson dat dit niet onder zijn leiding kon gebeuren.

Uiteindelijk heeft e-gold nooit opnieuw de deuren geopend.

Jackson had e-gold opgericht om het materiële welzijn van mensen te verbeteren door een alternatief te bieden voor conventionele, ongedekte valuta zoals de Amerikaanse dollar. Opgesloten in zijn eigen huis, met meer dan een miljoen dollar aan juridische kosten op zijn naam, en zijn bedrijf noodgedwongen gesloten, had hij de pijnlijke les geleerd dat het aanbieden van een dergelijk alternatief niet zonder slag of stoot ging.

---

6 US Department of Justice, *Digital Currency Business e-gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges*, 21 juli 2008, online

7 e-gold *Transcript of sentence before the honorable Rosemarie M. Collyer United States District Judge*, 114, 20 november 2008, online

Satoshi Nakamoto

Het lot van Douglas Jackson en e-gold diende als een niet te miskennen waarschuwing voor iedereen met ambities om een alternatieve vorm van geld aan te bieden. Overheden (en met name de Amerikaanse overheid) konden besluiten om hard op te treden, met ernstige persoonlijke en financiële schade tot gevolg. Voor de meesten was dit waarschijnlijk het risico niet waard.

Maar dit hield een onbekend persoon of groep, alleen bekend als 'Satoshi Nakamoto', niet tegen. Rond dezelfde tijd dat Jackson zijn dagen thuis doorbracht met een enkelband om, bereidde Nakamoto de lancering van een eigen elektronisch geldsysteem voor.

Het ontwerp van Nakamoto's digitale geldsysteem was echter zeer verschillend van e-gold. Hoewel er niet veel bekend is over de achtergrond of beweegredenen van Satoshi Nakamoto, is het duidelijk dat deze mysterieuze entiteit (de naam is vrijwel zeker een pseudoniem) zijn eigen systeem bewust zodanig ontwierp om een soortgelijk lot als e-gold te vermijden.

Dit ontwerp was waarschijnlijk ook niet het resultaat van een spontane ingeving. Al jaren, zelfs ruim voor Jackson e-gold lanceerde, probeerde een kleine maar toegewijde groep technici een digitale vorm van contant geld te creëren: ze wisselden ideeën uit, ontwikkelden technieken, en werkten diverse voorstellen uit, in de hoop dichter bij een werkende oplossing te komen. Maar het succes bleef uit. Totdat Nakamoto de puzzelstukjes eindelijk op hun plek wist te krijgen.

In dit boek gaan we terug naar de ideeën en technologieën die Satoshi Nakamoto (waarschijnlijk) hebben geïnspireerd in het ontwikkelen van dit elektronische geldsysteem.

In Deel I onderzoeken we de gevarieerde oorsprong van sommige van deze grondleggende ideeën en technologieën die de basis vormden voor elektronisch geld. Deze lopen uiteen van heterodoxe zienswijzen over monetaire economie tot een opstandige revolutie in de cryptografie, en van de opkomst van de hackercultuur in de jaren '60 en '70 tot techno-utopische visies op ruimtekolonisatie, moleculaire nanotechnologie en eeuwig leven.

Deel II vertelt het verhaal van de Cypherpunks: een verzameling cryptografen, hackers en privacyactivisten die gedurende de jaren 1990 privacyhulpmiddelen voor het internet ontwikkelden en verspreidden, en die probeerden een elektro-

nische versie van contant geld te creëren. We focusen ook op enkele specifieke pogingen om dergelijke elektronische betalingssystemen te ontwikkelen.

Tot slot beschrijft Deel III van het boek hoe Satoshi Nakamoto zijn elektronische geldsysteem ontwierp en ontwikkelde, wat de inspiratiebron was voor dit ontwerp, en hoe het zich verhoudt tot andere vormen van (digitaal) geld.

Samen vormen zij het verhaal van de monetaire hervormers, computerwetenschappers, privacyactivisten, futurologen, ondernemers en andere pioniers die, elk op hun eigen manier, bijdroegen aan de opkomst van het eerste succesvolle peer-to-peer, elektronische geldsysteem ter wereld: Bitcoin.

Deel I

Grondslagen

Hoofdstuk 1

Spontane orde

Net als zijn vader wilde Friedrich August von Hayek hoogleraar in de biologie worden, maar de Eerste Wereldoorlog veranderde zijn levenspad volledig.[8] Hij werd geboren in 1899 en groeide op tijdens de laatste jaren van het Oostenrijks-Hongaarse Rijk. Op zijn achtiende verjaardag werd hij opgeroepen om aan het Italiaanse front te vechten. Het laatste deel van de oorlog bracht hij in vliegtuigen door als waarnemer.

Toen hij in 1918 na het einde van de oorlog thuis kwam, vond Hayek (het aristocratische voorvoegsel *von* werd na de ineenstorting van de dubbele monarchie weggelaten) zijn woonplaats Wenen in totale verwoesting terug. De oorlog was verloren, de economie vernietigd en het rijk was niet meer. Het moreel in de stad was gebroken.

Erger nog, de nieuwe Oostenrijkse regering spendeerde zoveel om de naoorlogse kosten te dekken dat de waarde van hun nationale munteenheid enorm kelderde. Hoewel de Oostenrijkse munt, de kroon, tijdens de oorlog al meer dan 90 procent van zijn koopkracht had verloren, liep dit in de naoorlogse jaren pas echt uit de hand. Terwijl een Amerikaanse dollar voor ongeveer negen kronen verkocht werd in 1917, kon diezelfde dollar tegen 1923 meer dan 70.000 van de Oostenrijkse munteenheden opbrengen. Het nationale geld was in feite vernietigd.[9]

8 Deirdre N. McCloskey, *How to be Human – Though an Economist*, 33.

9 Lawrence H. Officer, *Exchange Rates Between the United States Dollar and Forty-one Currencies*, MeasuringWorth, 2023.

Nadat hij van dichtbij geconfronteerd was met de verschrikkingen van de Grote Oorlog, waarin bijna achttien miljoen mannen en vrouwen het leven lieten, besloot Hayek om zijn tijd en energie te besteden aan het proberen te voorkomen van een herhaling van dergelijke dramatische conflicten in de toekomst. Hij was vastberaden om betere manieren te vinden om de maatschappij te organiseren.

Als leergierig persoon uit een hoogopgeleid gezin – beide grootvaders van hem waren ook academici – schreef Hayek zich in aan de Universiteit van Wenen, de oudste universiteit in de Duitstalige wereld en een van de meest gerenommeerde academische instituten in heel Europa. Gemotiveerd door zijn nieuwe missie, koos Hayek ervoor om politieke wetenschappen en recht te studeren, terwijl hij naast zijn hoofdstudies ook lessen in filosofie, psychologie en economie volgde.

Hij schreef zich niet meteen in voor alle economielessen. Voor de socialistisch-geïnspireerde Hayek leek de economieprofessor aan de universiteit een beetje te hard te denken vanuit vrijemarktprincipes. Pas toen diezelfde economieprofessor Hayek in dienst nam om een tijdelijk overheidskantoor in de stad te bemannen, besloot hij eindelijk zijn lessen een kans te geven.[10]

De naam van de professor was Ludwig von Mises. Hayek ontdekte al snel dat Mises een vooraanstaand econoom was binnen een relatief nieuwe school van economisch denken.[11]

Oostenrijkse economie

De Eerste Wereldoorlog was het gewelddadige hoogtepunt van een tijdperk dat sterk doordrenkt was van nationalisme, de ideologie die stelt dat collectieven van mensen met een gemeenschappelijke herkomst, geschiedenis, cultuur of taal — *naties* — zichzelf als staten moesten organiseren en handelen in het belang van deze staten.

Het nationalisme had in de negentiende eeuw ook invloed op de economische wetenschap. Waar de *klassieke economie*, met haar sterke nadruk op vrije markten zoals voorgesteld door baanbrekende economen zoals David Hume, Adam Smith, en David Ricardo, dominant was in de late achttiende eeuw, begonnen Europese

10 Eamonn Butler, *Hayek: His Contribution to the Political and Economic Thought of Our Time*.

11 Bruce Caldwell and Hansjoerg Klausinger, *Hayek: A Life, 1899–1950, Chs. 6–9*.

universiteiten vanaf de jaren 1800 de methoden van de *historische school van economie* te omarmen. De meest invloedrijke experts pleitten voor staatsinterventies in de economie, zoals arbeidswetten, beschermde heffingen, en progressieve belastingen.[12]

De methodologie van de historische economische school – de verzameling methoden die gebruikt worden om de economie te bestuderen – sloot algemene economische theorieën uit en stelde dat de *regels* waaraan economieën voldoen verschillen per cultuur en tijd. In tegenstelling tot het opstellen van modellen of theorema's, verzamelden historische economen grote hoeveelheden historische data voor empirische analyse.

Maar professor Carl Menger van de Universiteit van Wenen had deze aanpak in de jaren 1870 al afgewezen. Hij geloofde dat mensen en menselijke interacties te complex waren om enkel op basis van empirische gegevens waardevolle wetenschappelijke inzichten te kunnen afleiden. Een ontelbare hoeveelheid factoren beïnvloedt de gedachten en acties van een typisch persoon, redeneerde hij — het is onbegonnen werk om het aantal factoren die een hele samenleving beïnvloeden te bestuderen. Geen enkele hoeveelheid empirische data zou groot genoeg zijn om al deze factoren te omvatten, geloofde Menger. Elke conclusie die uit zo'n dataset wordt getrokken, zou nooit overtuigend zijn.

In plaats daarvan betoogde Menger dat economen moesten proberen om economische verschijnselen te begrijpen en uit te leggen door deductieve redenering. Door te beginnen met basisprincipes, kon logisch redeneren leiden tot onweerlegbare inzichten die het wetenschappelijke begrip van economische processen *a priori* uitbreidden (de Latijnse term *a priori* verwijst naar kennis die onafhankelijk is van ervaring, zoals wiskunde, in tegenstelling tot *a posteriori* kennis die afhankelijk is van empirisch bewijs, zoals meer typisch is in de meeste andere wetenschappelijke vakgebieden).

Menger bracht deze aanpak in de praktijk in zijn boek uit 1871 getiteld *Grundsätze der Volkswirtschaftslehre*. Hierin schetste hij de theorie van het marginale nut, die stelt dat de prijs van goederen en diensten deels afhangt van hoeveel extra voldoening men krijgt door er meer van te hebben.[13]

12 Ludwig von Mises, *The Historical Setting of the Austrian School of Economics*, 12.

13 Mises, *Historical Setting*, 12–13, 19–20.

Het boek en de methode van Menger betekende een fundamentele verschuiving in denkwijze. Tot dan toe hadden economen, zowel uit de klassieke als uit de historische school, altijd aangenomen dat de waarde van een product werd afgeleid van zijn productiekosten. Zij stelden dat een paar schoenen waardevol is omdat de productie ervan kosten met zich meebrengt — met name de kosten van arbeid, leer en benodigdheden. De reden dat het leer en de benodigdheden kosten met zich meebrengen, is op hun beurt omdat het produceren van het leer en de benodigdheden eveneens arbeid vereist (en mogelijk ook andere kosten). Dit werd de arbeidswaardetheorie genoemd.

Volgens de theorie van het marginale nut, stelde Menger dat waarde subjectief is: individuen waarderen producten en diensten als deze een persoonlijke behoefte of verlangen vervullen. De waarde van een paar schoenen komt niet voort uit de productiekosten, maar uit het feit dat *mensen het dragen van schoenen waarderen*.

Dit betekent dat de waarde van een bepaald product kan variëren van persoon tot persoon. Iemand die helemaal geen schoenen heeft, zal een nieuw paar waarschijnlijk meer waarderen dan iemand die al meerdere paren bezit. Op dezelfde manier kan *dezelfde* persoon hetzelfde product op verschillende tijdstippen anders waarderen. Nadat de persoon zonder schoenen in het vorige voorbeeld een paar heeft verworven, waardeert hij waarschijnlijk een tweede, identiek paar schoenen niet even hoog als het eerste.[14]

Met deze *subjectieve waardetheorie*, plaatste Menger het individu opnieuw in het centrum van de economie. Hij stelde dat niet landen of andere collectieven de drijvende kracht waren achter economische beslissingen, maar mensen en hun subjectieve voorkeuren. In plaats van de staat als uitgangspunt te nemen voor analyse, geloofde Menger dus dat de studie van economie moest beginnen door te begrijpen wat de kleinste onderdelen van elk economisch systeem beïnvloedt. Precies, de individuen.

Met zijn benadering, wellicht het best beschreven als een herleving van de klassieke economie gericht op individuele subjectieve ervaring, won Carl Menger de steun van verschillende van zijn collega's aan de Universiteit van Wenen. Door

14 Ludwig von Mises, Human Action: A Treatise on Economics, The Scholar's Edition, 21, 38–54.

de publicatie in de jaren 1880 van zijn tweede boek,[15] had Menger een filosofisch debat aangewakkerd over de methodologie van de economische wetenschap binnen Duitstalige universiteiten.

Tijdens deze soms vijandige *Methodenstreit*, begonnen Duitse economen – die sterk neigden naar de historische school – ietwat minachtend naar Mengers aanpak te verwijzen als de 'Oostenrijkse school van economie'. Hoewel oorspronkelijk bedoeld als een sneer (in die tijd associeerden de Duitsers het predicaat *Oostenrijks* met het verlies van Oostenrijk in de Oostenrijks-Pruisische oorlog van 1866), bleef de naam in gebruik. Economen die Mengers methodologie aannamen, werden sindsdien aangeduid als Oostenrijkse economen, zelfs wanneer ze niet uit Oostenrijk afkomstig waren.[16]

De vijandige sfeer tijdens de methodenstrijd in de late negentiende eeuw bereikte zijn hoogtepunt met de *de facto* verbanning van de Oostenrijkse economie uit Duitse universiteiten. De boycott bleef decennia van kracht, en verhinderdde in grote mate dat Mengers ideeën zich door de nieuwe, verenigde natiestaat verspreidden. In plaats daarvan bleef het nationalisme domineren, terwijl een andere collectivistische ideologie zich zonder veel wezenlijk tegengas ook begon te verspreiden doorheen de Duitse universiteiten: het socialisme was in opkomst.

Economische berekening

Oorspronkelijk gepopulariseerd door de Duitse auteur en sociale commentator Karl Marx, geloofden socialisten dat de economische geschiedenis van de wereld het best begrepen wordt als een klassenstrijd tussen degenen die kapitaal bezitten (goederen die kunnen worden gebruikt als productiemiddel, zoals fabrieken en hun machines) en de arbeidersklasse, die alleen hun arbeid verkopen. Marx voorspelde dat deze strijd in het voordeel van de kapitaalbezittende klasse (de *kapitalisten*) zou uitdraaien, omdat ze steeds meer kapitaal en eindeloos groeiende winsten zouden verwerven, totdat de arbeidersklasse (het proletariaat) onvermijdelijk in opstand zou komen.

Volgens Marx was het socialisme de uiteindelijke oplossing voor economische

15 Carl Menger, *Untersuchungen über die Methode der Sozialwissenschaften und der Politischen Oekonomie insbesondere*.

16 Mises, *Historical Setting*, 3–19.

ongelijkheid: een economisch systeem waarin de productiemiddelen onder gemeenschappelijk eigendom gebracht worden en hun opbrengsten over de hele samenleving worden verdeeld. Dit moest in eerste instantie onder toezicht van de staat gebeuren, om geleidelijk aan vervangen te worden door een anarchistische vorm van zelfbestuur.

Hoewel de ideeën van Marx pas echt populair leken te worden na zijn dood in 1883, hadden ze ook een behoorlijk aantal critici. Een vaak gehoord bezwaar was dat mensen in een socialistisch systeem geen stimulans zouden hebben om te werken, aangezien ze toch een vast aandeel van alle geproduceerde goederen zouden ontvangen, terwijl de goederen die ze zelf zouden helpen te maken, verspreid zouden worden over de rest van de samenleving. Een tweede bezwaar was het risico dat socialistische leiders zich tegen hun eigen bevolking zouden keren en veel van de onder staatsbeheer geproduceerde goederen voor zichzelf zouden opeisen, in plaats van ze eerlijk te verdelen.

Desondanks heeft het de opkomst van de socialistische leer in het Russische Rijk niet gestopt. In 1917, midden in de Eerste Wereldoorlog, wierpen revolutionairen, georganiseerd via arbeidersraden bekend als 'Soviets', de zittende regering omver en richtten de Sovjet-Unie op als een communistische staat.

Ongeveer drie jaar na deze gebeurtenissen bracht Mises, de professor die Hayek zijn overheidsbaan had aangeboden, een baanbrekende nieuwe kritiek op het socialisme.[17] Belangrijk om te vermelden, is dat deze kritiek standhield *zelfs* als mensen gemotiveerd waren om te werken, en *zelfs* als socialistische leiders zich inzetten voor een eerlijke verdeling van de economische winsten. Mises beweerde echter dat het fundamentele probleem van het socialisme het ontbreken van een direct feedbackmechanisme was om producenten te informeren of ze überhaupt waarde toevoegden aan de samenleving.

Laten we een autofabriek nemen om dit argument te illustreren. In een vrije markt voegt een fabriek die auto's produceert en winst maakt duidelijk waarde toe aan de maatschappij: mensen zijn bereid meer te betalen voor auto's dan de fabriek moet betalen voor de benodigde hulpbronnen – staal, machines, arbeidskrachten – om ze te produceren. Winst wijst erop dat de productie van de fabriek meer wordt gewaardeerd dan de input.

17 Ludwig von Mises, *Economic Calculation in the Socialist Commonwealth*.

Een autofabriek die verlies draait daarentegen, voegt duidelijk geen waarde toe aan de maatschappij, aangezien mensen de gebruikte middelen meer waarderen dan het eindproduct. Uiteindelijk zal zo'n fabriek de deuren moeten sluiten. De middelen die de fabriek gebruikte, kunnen nu worden gekocht (of in het geval van arbeid, ingehuurd) door winstgevendere bedrijven om beter ingezet te worden (de Oostenrijkse econoom Joseph Schumpeter zou dit later *creatieve destructie* noemen).

In een socialistische samenleving zou een staatsgeleide autofabriek op bevel van een centrale planner auto's produceren. Wanneer de auto's op bevel geproduceerd worden, is er geen terugkoppeling van de maatschappij in de vorm van winst of verlies. De autofabriek kan mogelijk middelen verspillen aan het maken van auto's die mensen niet waarderen, of niet zo hoog waarderen, als andere producten die gemaakt hadden kunnen worden met dezelfde middelen.

Zonder vrije markt is er geen *economische berekening* mogelijk, wat de fundamentele taak van ieder economisch systeem onmogelijk maakt: de efficiënte verdeling van schaarse middelen over de samenleving.[18]

'Zonder economische berekening kan er geen economie zijn', concludeerde Mises. 'Daarom kan er in een socialistische staat, waarin het nastreven van economische berekening onmogelijk is, in onze betekenis van het woord, geen economie bestaan.'[19]

Prijzen

Mises, en met name zijn concept van economische berekening, zou op Hayek een grote invloed hebben. Aan de Universiteit van Wenen groeide hij uit tot een enthousiaste student van de Oostenrijkse school van economie. Hij bestudeerde de werken van Menger, evenals andere 'eerste generatie'-Oostenrijkers zoals Eugen von Böhm-Bawerk. Hij werd ook een vaste bezoeker van privé-seminaries die Mises tweemaal per maand organiseerde in zijn overheidskantoor. Daar kwam een kleine groep geleerden samen om economische theorie, filosofie en welke andere

18 Hoewel dit argument inderdaad is aangevoerd in de context van consumptiegoederen, is een meer precieze verwoording van dit argument, uitgewerkt in latere economische debatten, dat dit vooral van toepassing is op kapitaalgoederen.

19 Mises, *Economic Calculation*, 18.

onderwerpen Mises en zijn gasten die week ook interessant vonden, te bespreken.

Mises hielp Hayek persoonlijk bij het opstarten van zijn academische carrière in de economie. In 1927, nadat hij zijn studie aan de Universiteit van Wenen had afgerond, werd Hayek benoemd tot directeur van Mises' pas opgerichte Oostenrijks Instituut voor Conjunctuuronderzoek. Dit bood de jonge econoom een perfecte omgeving om de theorie van zijn voormalige professor over economische berekening verder te ontwikkelen.

Hayek concentreerde zich met name op de functie en het effect van *prijzen*. Zoals hij in de volgende jaren zou uitleggen, zijn prijzen volgens hem de gedecentraliseerde en maatschappelijk schaalbare communicatiemiddelen van de markt.[20] Hoewel men prijzen meestal ziet als een eenvoudige functie van vraag en aanbod van goederen en diensten binnen een economie, liet Hayek zien dat prijzen in feite een breed scala aan relevante informatie bevatten die mensen nodig hebben om economische beslissingen te nemen.

Laten we als (vereenvoudigd) voorbeeld opnieuw de autofabriek van Mises nemen. Zoals eerder genoemd, heeft deze fabriek hulpbronnen nodig zoals staal, machines en arbeid om auto's te produceren — maar we concentreren ons voor nu alleen op staal. Stel dat deze specifieke fabrieksoperator zijn staal koopt van een staalproducent in een nabijgelegen stad. Deze staalproducent haalt op zijn beurt ijzererts uit een mijn halverwege het land. Tegelijkertijd koopt een lokale autodealer de auto's van de fabriek, in de tegenovergestelde richting van de toeleveringsketen, om ze vervolgens aan klanten te verkopen.

Iedereen in deze leveringsketen heeft de informatie die ze nodig hebben om hun eigen bedrijf uit te baten, en ze communiceren dit met alle andere marktdeelnemers door middel van prijzen.

De autohandelaar heeft een goed beeld van hoe hij auto's moet verkopen; hij weet bijvoorbeeld hoeveel vraag er is naar nieuwe auto's, en hij weet wat hij nodig heeft om ze te verkopen — misschien een toonzaal op een gunstige locatie en wat was om de auto's er mooi en glanzend uit te laten zien. De prijzen die klanten bereid zijn te betalen voor auto's, en de prijs die hij moet betalen voor een toonzaal en was, zullen dus bepalen welke prijs hij zelf voor nieuwe auto's bereid is te betalen aan de autofabriek.

---

20 Friedrich A. Hayek, *Prices and Production*.

Intussen weet de staalproducent hoeveel hij moet betalen voor erts, wat zijn oven kost om het erts om te zetten in staal en wat hij aan salarissen moet uitgeven. Zolang zijn klanten, zoals de autofabriek, meer betalen voor zijn staal dan wat het hem kost om het te produceren, zal hij staal blijven produceren.

Hoewel iedereen in de toeleveringsketen van elkaar afhangt, hoeft niemand *exact* te weten hoe iemand anders zijn werk doet. De kosten van een toonzaal kunnen van invloed zijn op hoeveel de autodealer bereid is aan de fabriek te betalen voor een nieuwe auto. Maar de fabrieksmanager hoeft zich niet echt te verdiepen in de vastgoedmarkt voor toonzalen. Hij hoeft zich ook niet te buigen over de schaarste van erts. Deze informatie wordt weerspiegeld in de prijzen die de autodealer biedt voor nieuwe auto's, en de prijs die de staalproducent vraagt voor nieuw staal.

Als we dit concept verder uitwerken, blijken prijzen te kunnen helpen bij de herverdeling van hulpbronnen wanneer er iets verandert in de economie.

Als de ijzerertsmijn bijvoorbeeld gedeeltelijk moet sluiten vanwege een brand, wordt het aanbod van erts kleiner, en de algehele vraag naar het overgebleven erts zal de prijs van ijzer opdrijven. De staalproducent zal dan op zijn beurt de prijs van zijn staal moeten verhogen om winstgevend te blijven. Deze verhoogde prijs voor staal communiceert eigenlijk de relevante informatie aan de autofabriek die deze nodig heeft om economische beslissingen te nemen (de autofabriek zou bijvoorbeeld kunnen besluiten staal te kopen bij een andere producent die zijn erts van een andere mijn krijgt).

Op dezelfde manier zal de fabriek van keukenapparatuur als de consumentenvraag naar keukenapparatuur stijgt, meer staal willen kopen, waardoor de staalprijs stijgt wanneer het de autofabriek overbiedt. De staalproducent zal de staal leveren aan de fabriek van keukenapparatuur in plaats van de autofabriek, niet omdat hij iets weet over (de vraag naar) auto's of keukenapparatuur, maar simpelweg omdat het prijssysteem hem heeft geïnformeerd dat dit winstgevender zal zijn (op de lange termijn zal de staalproducent ook gestimuleerd worden om meer staal te produceren).

Hayek legde uit dat relevante informatie in de economie kenbaar wordt gemaakt door middel van het prijssysteem, wat ervoor zorgt dat markten efficiënt middelen kunnen toewijzen daar waar ze door de samenleving het meest gewaardeerd worden.

'In wezen, in een systeem waarin de kennis van de relevante feiten is verspreid over vele mensen, kunnen prijzen fungeren om de afzonderlijke acties van verschillende mensen te coördineren net zoals dat subjectieve waarderingen het individu helpen om de onderdelen van zijn plan te coördineren', schreef de Oostenrijker: 'een wonder.'[21]

En belangrijk is dat dit allemaal mogelijk is zonder centrale planning. De vrije markt, zo betoogde Hayek, valt het best te begrijpen als een vorm van zelforganisatie van onderaf: een *spontane orde*.

Rentetarieven

Terwijl Mises Hayeks begrip van spontane orde vormde *in ruimtelijke zin* — door te laten zien hoe middelen van het ene punt in de samenleving naar het andere worden toegewezen — hielpen de werken van von Böhm-Bawerk hem om het concept van spontane orde door de *tijd* heen te begrijpen.

Von Böhm-Bawerk kwam in de jaren 1890 op de proppen met een nieuw idee in het vakgebied economie, dat van groot belang werd voor de Oostenrijkse School: *tijdsvoorkeur*. Von Böhm-Bawerk stelde dat mensen doorgaans liever vroeger dan later goederen en diensten willen ontvangen. De mate van deze voorkeur verschilt echter van persoon tot persoon. Iedereen heeft zijn eigen subjectieve tijdsvoorkeur.

Deze tijdsvoorkeuren, bepleitte von Böhm-Bawerk, manifesteren zich op de markt bijvoorbeeld in de vorm van rentetarieven.

Stel je voor dat zowel Marie als Joris graag een nieuwe auto willen hebben. Ze hebben beiden liever vandaag dan volgend jaar een nieuwe auto. Maar Marie, wier auto net kapot is gegaan en die elke dag naar haar werk moet rijden, hechtte veel meer waarde aan een nieuwe auto vandaag dan aan een nieuwe auto volgend jaar. Joris daarentegen heeft nog steeds een redelijk goede auto en werkt van thuis uit, dus heeft hij niet zo'n haast om een nieuwe te krijgen. Marie heeft een hogere tijdsvoorkeur dan Joris.

Stel je voor dat een nieuwe auto $ 20.000 kost. Marie heeft helaas geen geld,

21 Friedrich A. Hayek, *The Use of Knowledge in Society*, American Economic Review. XXXV, No. 4: 526–27.

terwijl Joris $ 20.000 aan spaargeld heeft. Op het eerste zicht zou dit suggereren dat Joris eerst een nieuwe auto zal kopen: Joris kan het zich vandaag al veroorloven, terwijl Marie nog meer moet sparen.

Maar er is ook nog een andere optie. Joris zou Marie $ 20.000 kunnen lenen. Of dit een goede deal is voor hen beiden, kan eenvoudig worden ingeschat met behulp van rentetarieven. Laten we zeggen dat Marie, omdat ze een hoge tijdsvoorkeur heeft, vandaag in principe een auto 10 procent meer zou waarderen dan een auto volgend jaar. Dat wil zeggen dat ze bereid zou zijn om $ 22.000 voor een auto van $ 20.000 te betalen als ze deze vandaag kan hebben in plaats van een jaar vanaf nu. Ze is daarom bereid om 10 procent rente te betalen op een lening van $ 20.000. Joris, die een lage tijdsvoorkeur heeft, zou een nieuwe auto vandaag slechts 1 procent meer waarderen dan een auto volgend jaar, een verschil van slechts $ 200.

Joris zou dus kunnen besluiten om zijn aankoop uit te stellen en in plaats daarvan $ 20.000 te lenen aan Marie. Na een jaar zal hij het geleende bedrag plus een extra $ 2.000 aan rente terugkrijgen. Dit zorgt ervoor dat Marie de auto vandaag al kan kopen, terwijl de extra $ 2.000 voor Joris de *kosten* van het uitstellen van de aankoop van $ 200 ruimschoots goedmaakt. Beide partijen zullen er voordeel uit halen. Rentetarieven stellen hen in staat onderling hun middelen in de tijd te verdelen, zodat ze het beste overeenkomen met hun individuele tijdsvoorkeuren.

Hoewel dit natuurlijk een zeer vereenvoudigd voorbeeld is, doen kredietmarkten iets vergelijkbaars op grotere schaal. Geldverstrekkers en -ontleners komen een rentetarief overeen waar het aanbod en de vraag naar geld elkaar treffen, gebaseerd op de gezamenlijke tijdsvoorkeuren. Als zodanig zijn rentetarieven in feite ook prijzen. Ze weerspiegelen de prijs van geld.

En net zoals alle prijzen, communiceert de prijs van geld relevante informatie. Hayek was van mening dat de gemiddelde rente iets onthult over de hele economie. Als de rentetarieven hoog zijn, wijst dit erop dat veel mensen een hoge tijdsvoorkeur hebben en niet erg bereid zijn om geld uit te lenen. Ze geven er de voorkeur aan om goederen en diensten eerder dan later aan te schaffen. Omgekeerd, als de rentetarieven laag zijn, suggereert dit dat veel mensen een relatief lage tijdsvoorkeur hebben en bereid zijn hun aankopen uit te stellen als dat betekent dat ze ondertussen wat rente kunnen verdienen.

Hayek was dus van mening dat rentetarieven producenten informeerden over de productiefase waar ze hun middelen aan moesten besteden. Lage rentetarieven signaleerden aan producenten dat ze dit *goedkope geld* moesten benutten om productieprocessen op lange termijn te verbeteren door te investeren in goederen van een hogere orde, zoals een nieuwe oven om staal te produceren, die later kan worden gebruikt in de productie van auto's (of keukenapparatuur). Daarentegen maken hoge rentevoeten het lenen van geld duur, wat producenten aanmoedigt om reeds beschikbare middelen te gebruiken en zich te concentreren op het voltooien van de productie in een laat stadium (het laatste deel van het proces waar de uiteindelijke consumptiegoederen zoals auto's worden gemaakt en tentoongesteld in toonzalen voor mensen om te kopen).

Het mooie hiervan, zag Hayek in, is dat de tijdsvoorkeuren van mensen netjes overeenkomen met de productiecapaciteit van de economie. Als tijdsvoorkeuren laag zijn, investeren mensen hun geld (of in de meeste gevallen zouden ze het *sparen* op een bankrekening en de bank investeert het voor hen), en producenten worden gestimuleerd om te investeren in hun langetermijnproductieprocessen. Dus wanneer tijdsvoorkeuren in de toekomst toenemen, kunnen mensen hun geld en de rente die ze verdienen uitgeven aan de vruchten van al deze verhoogde productiviteit.

Rentevoeten, legde Hayek uit, bevorderen spontane orde door de tijd heen! Dat is natuurlijk zo, *als* rentetarieven in feite de tijdsvoorkeuren nauwkeurig weerspiegelen. Hayek merkte echter op dat het in de praktijk vaak niet toegelaten werd om zo te zijn.

De Federal Reserve

Een aantal jaren voordat zijn student afstudeerde aan de Universiteit van Wenen, hielp Mises Hayek opnieuw om een tijdelijke functie te verkrijgen als onderzoeksassistent bij de Universiteit van New York.

Toen de jonge Oostenrijker in 1923 in de Verenigde Staten aankwam, waren de *Roaring Twenties* in volle gang. De Amerikaanse economie floreerde, en mensen waren maar al te blij om geld te lenen om auto's van Ford te kopen, nieuwe technologische wonderen zoals wasmachines, of vastgoed te kopen in de voorsteden

van grote steden. Of ze gebruikten het geld om te investeren in aandelen: de Dow Jones-beursindex bereikte jaar na jaar nieuwe hoogtepunten.

Hayeks onderzoek zou zich richten op de economische rol van één instituut in het bijzonder: het relatief nieuwe centrale banksysteem van de Verenigde Staten, genaamd de Federal Reserve. De *Fed*, zoals dit centraal banksysteem vaak wordt genoemd, was in 1913 opgezet om vertrouwen en stabiliteit te brengen in het Amerikaanse bankensysteem.

Er werd gedacht dat een anker voor vertrouwen en stabiliteit noodzakelijk was, omdat commerciële banken werkten op basis van *fractionele reserves*: ze hadden minder echt geld in hun kluizen dan wat spaarders op hun bankrekeningen hadden toegeschreven. Het verschil werd uitgeleend aan kredietnemers en bracht rente op voor zowel banken als hun spaarders. Maar dit kon ook economische instabiliteit veroorzaken, want als te veel spaarders het vertrouwen in een bank verloren en ervoor kozen om tegelijkertijd hun geld op te nemen, zou de bank krap bij kas kunnen komen te zitten, waardoor ze niet alle opnameverzoeken konden honoreren.

In het scenario van zo'n *bankrun*, kon de Federal Reserve nu optreden als *kredietverstrekker in uiterste nood* door een lening te verstrekken aan de bank die in de problemen kwam. Zo'n lening zou de bank van voldoende liquiditeit (contant geld) voorzien om de storm te doorstaan, zodat er geen reden was voor spaarders om zich zorgen te maken.

Maar Hayek, die helemaal uit Oostenrijk was gekomen om de rol van de Fed als kredietverstrekker in uiterste nood, en haar invloed op de Amerikaanse economie te onderzoeken, was kritisch.

Hayek vond dat de garanties van de nieuwe instelling economische prikkels verstoorden. Hij vreesde dat gunstige economische vooruitzichten de commerciële banken konden aansporen om leningen ruimer te verstrekken dan voorheen, waardoor de geldhoeveelheid in wezen toenam. Meer bankleningen betekent

meer geld om in de economie uit te geven.[22] Dit *nieuwe geld* zou de algemene prijzen omhoog drijven – *inflatie* – waardoor bedrijfswinsten over de hele lijn hoger uitvallen en op hun beurt de gunstige economische vooruitzichten bevestigen. De mogelijkheid van commerciële banken om in wezen nieuw geld aan te maken door middel van leningen, zou een feedback-loop van buitensporige kredietcreatie kunnen veroorzaken.

Wanneer de kredietcreatie echter onvermijdelijk vertraagt, valt het doek. Als de hoeveelheid nieuw geld die in de economie wordt geïnjecteerd afneemt, zullen de prijzen dalen — deflatie. Bedrijven zullen geconfronteerd worden met hun te optimistische inschattingen van de economische vooruitzichten en kunnen hun producten niet voor de verwachte prijzen verkopen. Sommige bedrijven zullen moeten inkrimpen, wat leidt tot een stijging van de werkloosheid en verdere vertraging van de economie, omdat mensen minder te besteden hebben. Andere bedrijven zullen failliet gaan omdat ze hun leningen niet kunnen terugbetalen, wat commerciële banken in de problemen brengt om aan de depositovereisten te voldoen. Deze banken zullen nieuwe leningen moeten stopzetten, wat de economie nog verder vertraagt, resulterend in meer ontslagen en onbetaalde leningen, en zo verder.

Economen zouden later naar een dergelijke dynamiek verwijzen als een *deflatoire schuldenspiraal*. Deze lagen aan de basis van enkele bankencrises die de oprichting van de Federal Reserve in eerste instantie motiveerden.[23]

Volgens Hayek was er geen reden om aan te nemen dat het oprichten van een *kredietverstrekker in uiterste nood* deze kwalijke dynamiek zou beperken. Integendeel, het zou het zelfs kunnen versterken.

In het oude systeem, merkte hij op, hadden commerciële banken tenminste

---

22 Als persoon A 100 bij de bank stort en de bank hiervan 90 uitleent aan persoon B, zal persoon A nog steeds denken dat hij of zij 100 heeft, terwijl persoon B 90 zal hebben, voor een totaal van 190. Bovendien, als persoon B de 90 opnieuw bij de bank stort en de bank hiervan 81 uitleent aan persoon C, zullen drie mensen denken dat ze samen 271 bezitten. Dit kan zo doorgaan, wat lijkt alsof er steeds meer geld in omloop komt. Dit concept staat bekend als de *geldmultiplier*. In werkelijkheid kan de geldmultiplier zelfs nog agressiever zijn dan dit conventionele voorbeeld van fractioneel bankieren suggereert, omdat banken geen stortingen hoeven te ontvangen voordat ze leningen kunnen verstrekken; ze kunnen leningen uitgeven door eenvoudigweg krediet te creëren in de bankrekeningen van klanten.

23 Gary Richardson and Tim Sablik, *Banking Panics of the Gilded Age: 1863–1913*, Federal Reserve History, 4 december 2015, online

nog een goede reden om voorzichtig te zijn en niet te veel leningen te verstrekken:

> *'In afwezigheid van enige centrale bank, is de voornaamste beperking voor individuele banken tegen het uitgeven van buitensporig krediet in een stijgende economische activiteitsfase, de noodzaak om voldoende liquiditeit te behouden om de vraag in een periode van krap geld het hoofd te bieden met hun eigen middelen.'*[24]

Het oprichten van een *kredietverstrekker in uiterste nood* kan inderdaad een toeloop op de bank en paniek voorkomen. Maar Hayek stelde dat dit tegelijkertijd de prikkel voor banken wegneemt om in eerste instantie enige terughoudendheid te tonen bij het verstrekken van leningen.

'Het zal dus onvermijdelijk leiden tot een gestage toename in het gebruik van krediet en daardoor de herhaling van recessies nog onvermijdelijker maken', concludeerde Hayek.[25]

Dit soort verkeerde afstemming van economische prikkels, waar bepaalde economische spelers – in dit geval, banken – beloond worden voor het nemen van meer risico's, maar niet de volledige kosten van deze risico's dragen, wordt in de economie *moreel risico* genoemd. Hayek vond dat de Federal Reserve dit morele risico in de economie introduceerde.

En Hayek geloofde dat dit niet eens de belangrijkste manier was waarop de Federal Reserve onhoudbare, door krediet geïnduceerde, economische bubbels stimuleerde.

De Oostenrijkse conjunctuurcyclus

Het jaarverslag van de Federal Reserve uit 1923 bepaalde de richting van Hayeks carrière als econoom voor de komende decennia. In dit document legde de Amerikaanse centrale bank uit hoe zij haar beheer van de geldhoeveelheid gebruikte om de economische activiteit te stabiliseren. In het bijzonder verklaarde de monetaire autoriteit van de VS hoe zij rentetarieven als beleidsinstrument inzette — een

24 Friedrich A. Hayek, *Monetary Policy in the United States after the Recovery from the Crisis of 1920*, in The Collected Works of F.A. Hayek, Good Money: part I, ed. Stephen Kresge, 145.

25 Hayek, *Monetary Policy*, 146.

nieuw concept op dat moment, geïntroduceerd door een instelling die zelf nog maar net opgericht was.[26]

Het idee was vrij eenvoudig. Door valuta in het bankensysteem te injecteren (doorgaans door overheidsobligaties te kopen), kon de Fed commerciële banken voorzien van meer reserves en ze daardoor stimuleren (en in staat stellen) om leningen te verstrekken tegen steeds lagere rentetarieven. Dit zou bedrijven en mensen aanmoedigen om te lenen. Anderzijds, door reserves uit het bankensysteem te halen (door overheidsobligaties te verkopen), konden banken worden ontmoedigd om leningen te verstrekken, waardoor de rentetarieven stijgen en economische activiteit wordt afgeremd.

De Federal Reserve geloofde dat ze de conjunctuurcyclus konden afvlakken door de rentetarieven zorgvuldig te beheren. Als de Fed de rentetarieven tijdens recessies licht kon verlagen, en ze tijdens oplevingen een beetje kon verhogen, konden ze de markt een kleine stimulans bieden als die in een dip zat, en een beetje afremmen als hij op hol sloeg. Hayek was een grote criticus van dit beleid.

De Oostenrijker was van mening dat de Federal Reserve valse signalen naar de markt zond door de rentetarieven kunstmatig laag te houden. Iedereen maakte gebruik van goedkoop geld om te investeren in bedrijven, die dit kapitaal gebruikten om meer middelen toe te wijzen aan hun productieprocessen. Echter, waarschuwde Hayek, er was geen overeenkomstige uitgestelde consumptie om de toekomstige productiegroei op te vangen. De rentetarieven waren niet laag omdat veel mensen een lage tijdsvoorkeur hadden en hun geld spaarden voor toekomstige uitgaven, maar omdat de Fed ze zo laag hield.

Wanneer rentetarieven uiteindelijk zouden stijgen en de creatie van nieuw krediet zou vertragen, zouden bedrijven worden gedwongen om de productie te voltooien, maar zouden ze ontdekken dat er geen echte vraag was om dit te evenaren. Zonder klanten om hun goederen te kopen, of in ieder geval niet tegen de prijzen die ze hadden verwacht, zouden bedrijven gedwongen zijn om werknemers te ontslaan en mogelijk in gebreke blijven op hun leningen. Zo start een deflatoire schuldenspiraal.

Toen Hayek in de Verenigde Staten aankwam, floreerde de economie: zowel de consumptie als de hoeveelheid investeringen schoten omhoog. Maar hij kwam

26 Stephen Kresge, *The Collected Works of F.A. Hayek, Good Money: part I*, 13.

tot de conclusie dat dit niet stand kon houden. De manipulatie van rentetarieven verstoorde de opkomst van de spontane economische orde in de tijd. Hayek was bezorgd dat de Federal Reserve in plaats van het afvlakken van de hoogte- en dieptepunten van de economische cyclus, deze eigenlijk versterkte.

En inderdaad, toen de Fed aan het eind van het decennium eindelijk de rente verhoogde, droogden de investeringen op terwijl er geen toename in consumptie was om dit te compenseren. De Roaring Twenties eindigden in 1929 met een knal en de Amerikaanse aandelenmarkt stortte in. In de daaropvolgende jaren verloor de Dow Jones-aandelenindex bijna 90 procent van zijn waarde, gingen tienduizenden bedrijven failliet, steeg de werkloosheid sterk en (ondanks de verantwoordelijkheid van de Federal Reserve als kredietverstrekker in uiterste nood) gingen ook duizenden banken op de fles.

Alhoewel het pijnlijk was, geloofde Hayek dat de beste aanpak destijds was om de deflatoire schuldenspiraal zijn gang te laten gaan. Daar waar kunstmatig lage rentetarieven een valse economische bloei hadden ingeluid, zou de economische malaise de economie herkalibreren naar duurzamere niveaus. Terwijl niet-rendabele bedrijven onderuitgingen, konden rendabele bedrijven hun middelen (inclusief hun werknemers) overnemen en ze beter benutten. Dit proces zou waarschijnlijk een tijdje duren, maar zou uiteindelijk tot een gezondere economie leiden.

Midden in de scherpe economische crisis die later bekend zou worden als de Grote Depressie, was de voorgestelde oplossing van Hayek echter niet erg geliefd. De meeste mensen waren van mening dat er *iets moest gedaan worden*.

De rivaliteit

En er kon iets gedaan worden, zo stelde een academicus uit Cambridge genaamd John Maynard Keynes. De Britse econoom zou tijdens de Grote Depressie snel naam maken door een onconventionele, maar dringend gewenste oplossing aan te dragen om de economie weer op de been te krijgen. In schril contrast met de pijnlijke oplossing die Hayek voorstelde, verspreidde Keynes een boodschap waar

veel mensen reikhalzend naar uitkeken.[27]

Keynes negeerde Hayeks analyse van de oorzaken van de depressie en beweerde dat de economische malaise gewoon het ongelukkige resultaat was van een daling van de totale vraag. Hij redeneerde dat de economie stagneerde omdat mensen, voornamelijk om psychologische redenen, minder geld uitgaven dan eerder. Hij omschreef het fenomeen als *dierlijke instincten*. Om uit de depressie te geraken, moesten mensen weer meer geld uitgeven.

In wat de basis zou worden van nog een nieuwe school van economisch denken - het *Keynesianisme* - beargumenteerde de Britse econoom dat als het grote publiek geen geld zou uitgeven, de overheid het in hun plaats moest doen. De overheid kon bijvoorbeeld investeren in openbare infrastructuurwerken, zelfs als dat zou betekenen dat daarvoor geld geleend moest worden. Geld lenen zou volgens Keynes sowieso goedkoop moeten zijn, aangezien hij vond dat de centrale bank de rentetarieven moest verlagen.

Door geld te besteden aan openbare infrastructuurwerken, zou de overheid banen creëren. Dat zorgt ervoor dat mensen lonen hebben om uit te geven en geld weer in de economie kan gaan circuleren. Wanneer mensen weer op eigen houtje gaan uitgeven, zou de overheid vervolgens haar uitgaven moeten verminderen. Keynes stelde voor dat beleidsmakers een *anti-cyclische* aanpak van overheidsuitgaven zouden moeten uitvoeren.

Eén specifieke beleidsmaker was helemaal klaar voor deze uitdaging. Franklin D. Roosevelt (FDR), die in 1932 de eerste Amerikaanse presidentsverkiezingen na de beurscrash won, had campagne gevoerd met de belofte om via zijn presidentieel mandaat actief een einde te maken aan de depressie. Toen hij zijn ambt opnam, vormden Keynes' ideeën het economische kader om zijn beleid te ondersteunen (zij het pas *nadat* dit beleid werd aangekondigd[28]). Via een reeks overheidsprogramma's, die *de New Deal* werden genoemd, begon FDR al snel miljarden dollars uit te geven aan wegen, luchthavens, bruggen, dammen en nog veel meer.

Hayek was echter helemaal niet overtuigd van de ideeën van Keynes. Aan-

27 Het meest uitgebreid uiteengezet in John Maynard Keynes, *The General Theory of Employment, Interest and Money*.

28 George Selgin, *The New Deal and Recovery, Part 15: The Keynesian Myth*, Cato Institute, 16 maart 2022, online

gezien hij geloofde dat de economische malaise slechts een correctie was van de onhoudbare hoogconjunctuur die eraan voorafging, was hij van mening dat overheidsuitgaven de uiteindelijk onhoudbare situatie alleen maar langer lieten voortduren.

Daarbovenop was er een wellicht nog belangrijker bezwaar tegen de Keynesiaanse anti-cyclische benadering, die niet eens echt gerelateerd was aan economie. Dit bezwaar was van politieke aard: Hayek geloofde niet dat politici te vertrouwen waren om te beslissen wanneer een economie in een opwaartse of neerwaartse trend zit. In plaats daarvan zouden ze in de verleiding komen om geld te lenen en in de economie uit te geven wanneer daar vraag naar is… wat evengoed continu het geval kan zijn.

'Er zullen altijd delen van het land of bevolkingsgroepen zijn die van mening zijn dat ze het moeilijk genoeg hebben om hulp te mogen ontvangen', schreef Hayek. 'Kan onder deze omstandigheden een rationeel anti-cyclisch beleid ontwikkeld worden als het in handen van politieke organen wordt gegeven?'[29]

Voor Hayek was het antwoord een overduidelijke *nee*.

Dit leidde tot wat vaak beschouwd wordt als een van de grootste intellectuele confrontaties van de twintigste eeuw. Gedurende de jaren 1930 stonden Hayek, die op dat moment professor was aan de London School of Economics, en Keynes, nog steeds bij *King's College* in Cambridge, vaak tegenover elkaar in publieke debatten en ook in hun privécorrespondentie. Hun respectieve universiteiten in het zuidoosten van Engeland dienden als het strijdtoneel voor de opkomende titanen van de economie en hun twee tegenovergestelde economische visies.

En er was in belangrijke opzichten een scherp contrast. Terwijl Keynes geloofde dat de economie onder andere regels werkt wanneer deze op nationale schaal wordt geanalyseerd (het macro-niveau), hield Hayek vol dat alles uiteindelijk voortkomt uit individuen en hun subjectieve keuzes (het micro-niveau). Waar Keynes graag focuste op prijsgemiddelden en totalen, was Hayek meer geïnteresseerd in prijsverschillen. En terwijl Keynes betoogde dat overheden een actieve rol moesten spelen in het beheren van de economie, hield Hayek vol dat de vrije markt het beste aan zichzelf kon worden overgelaten.

---

29 Friedrich A. Hayek, *The Gold Problem*, in *The Collected Works of F.A. Hayek, Good Money: part I*, ed. Stephen Kresge, 184.

Als Hayek het boegbeeld was van spontane orde van onderaf, dan had hij in Keynes en zijn interventiebeleid van bovenaf, zijn hedendaagse, intellectuele rivaal gevonden.

Hoofdstuk 2

Vrije en open source software

Richard Stallman was in de vroege jaren 1960, al vanaf jonge leeftijd, gefascineerd door computers. Toen hij op zomerkamp was, leende hij programmeerhandleidingen van zijn begeleiders. Er was destijds geen computer te bekennen – ze kostten gemakkelijk meer dan $ 100.000 per stuk – maar dat kleine detail ging zijn plezier niet bederven. Tijdens zijn reis schreef hij computerprogramma's volledig uit op papier.

Het zou nog een paar jaar duren voordat de jonge New Yorker voor het eerst met het echte werk kennismaakte. In 1970, net klaar met de middelbare school, kreeg de toen zeventienjarige Stallman een zomerbaan bij het Wetenschappelijk Centrum van IBM in Manhattan, om een numeriek analyseprogramma te schrijven. Hij rondde het project binnen enkele weken af, wat hem de rest van de zomer de gelegenheid gaf om bij het onderzoekscentrum een teksteditor en een programmeertaalprocessor te ontwerpen, gewoon voor de lol.

Na die zomer schreef Stallman zich in om aan Harvard natuurkunde te studeren. In het nieuwe computercentrum van de universiteit kon hij verder programmeren. Na verloop van tijd begon hij ook naar andere computers aan verschillende universiteiten en computerfaciliteiten in Cambridge te kijken. Hij ontdekte dat een bijzonder krachtige machine in het AI-lab van MIT gevestigd was. Het onderzoekscentrum van MIT was opgericht door twee pioniers op het gebied van AI – John McCarthy en Marvin Minsky – en werd door het Amerikaanse ministerie van Defensie gefinancierd, zonder extra voorwaarden.

De student van Harvard besloot dat hij de documentatie van de MIT-computer wilde bestuderen om meer informatie over de machine te verzamelen en te begrijpen hoe deze verschilde van wat ze hadden op Harvard. Maar toen hij het AI Lab bezocht, ontdekte Stallman dat ze helemaal geen dergelijke documentatie hadden. In plaats daarvan gaven ze hem een baan.

Het weerspiegelde de tamelijk anarchistische cultuur in het AI Lab. De leiders van het onderzoekscentrum hadden niet veel interesse in ervaring of kwalificaties, maar waardeerden vaardigheid en potentieel. Het was duidelijk dat dit wonderkind van Harvard, die het lab bezocht om hun computerdocumentatie te bestuderen, goed bij hen zou passen.[30]

De hackercultuur

De anarchistische cultuur in het AI Lab was ongeveer een decennium eerder voor het eerst ontstaan.[31]

Het begon toen het Lincoln Lab, een militair onderzoeks- en ontwikkelingscentrum voor geavanceerde technologie verbonden aan het MIT, rond 1960 een kleine revolutie ontketende door de universiteit de TX-0 te schenken, een vroege, volledig getransistoriseerde computer. In tegenstelling tot eerdere computers op de universiteit die altijd een speciale operator nodig hadden, was deze machine voor het eerst toegankelijk voor studenten.

De machine, die een hele kamer in beslag nam en een ton woog, had al snel de fascinatie gewekt van een specifieke groep studenten: de knutselende techneuten uit de modeltreinclub van de universiteit. Ze hadden nooit echt veel interesse gehad in de modeltreinen zelf, maar vonden het vooral leuk om het elektrische systeem van draden, schakelaars en hergebruikte telecomapparatuur te ontwerpen die de snelheid en richting van hun treintjes beheersten. Ze beseften dat er een veel interessanter spel was gearriveerd.

Vanaf het eerste moment dat die op de campus arriveerde, waren de jonge mannen (het waren aanvankelijk allemaal mannen) vastbesloten om de machtige TX-0 te beheersen. En inderdaad, al snel ontdekten ze hoe ze toegang konden

30 Richard Stallman, *Richard Stallman: High School Misfit, Symbol of Free Software, MacArthur-Certified Genius*. Interview door Michael Gross, mgross.com, 1999, online

31 Dit deel is grotendeels gebaseerd op Steven Levy, *Hackers: Heroes of the Computer Revolution*.

krijgen tot en de broncode konden bewerken van de verschillende programma's die in de machine waren geprogrammeerd. Kort daarna wisten ze te achterhalen hoe ze zelf hele nieuwe programma's konden schrijven.

Het duurde niet lang voordat ze hele nachten rond de TX-0 doorbrachten, op momenten dat ze de machine volledig voor zichzelf hadden. Verenigd door hun gedeelde passie, daagden de jongens elkaar uit om de computer steeds ingewikkeldere taken te laten uitvoeren. Wie elegante manieren om code te schrijven bedacht, had het recht om op te scheppen. Bijzonder slimme oplossingen werden in hun interne jargon *hacks* genoemd; de jongens identificeerden zichzelf dan ook trots als *hackers*.

Naarmate de jongens hun programmeervaardigheden in een sfeer van kameraadschap verbeterden, gingen ze de computer meer en meer als een levensstijl zien. Niets was voor hen belangrijker dan hacken, en niets was leuker. Het potentieel van de krachtige machines benutten, gaf hen een geweldig gevoel van zelbeschikking. Daarmee groeide ook een gevoel van verantwoordelijkheid.

De hackers voelden instinctief aan dat computers een blijvende invloed op de wereld zouden hebben. Na verloop van tijd ontwikkelden ze een filosofisch en ethisch kader rond programmeren en technologie. Dit vormde de basis voor een unieke subcultuur, gericht op technologie en gekenmerkt door experimenten en innovatie. Zelfs toen de groep hackers veranderde – nieuwe studenten kwamen naar MIT, terwijl oudere studenten vertrokken – bleef de hackercultuur behouden.

De hackers waren erop gesteld om zaken zelf in handen te nemen. Het was een cruciaal onderdeel van deze cultuur: alles waarvan ze dachten dat het verbeterd kon worden, wilden ze aanpassen, en wat kapot was moest hersteld worden. Om toestemming vragen was tijdverspilling; een goed idee moest onmiddellijk worden uitgevoerd en mogelijke beperkingen moesten genegeerd worden. Bureaucratie was de natuurlijke vijand van de hacker.

Als beperkingen als een uitdaging gezien werden, dan genoten hackers ervan om deze te overwinnen — en dat het liefst met een vleugje elegantie en flair. Hackers geloofden dat computers konden worden gebruikt om schoonheid te creëren: code kon een esthetische waarde hebben, en ze bewonderden goed geschreven programma's en originele oplossingen. En misschien wel het allerbelangrijkste, ze deelden hun werk met anderen.

Hackers waren ervan overtuigd dat vrij toegankelijke code en bestanden

iedereen ten goede kwamen en ze waren trots wanneer mensen de programma's gebruikten die ze geschreven hadden. Ze geloofden dat ze de ethische plicht hadden om hun code te delen en om toegang tot informatie voor anderen te vergemakkelijken. Er waren geen wachtwoorden, geen beperkingen, en geen *persoonlijke* documenten.

De hackers zouden uiteindelijk een speciaal besturingssysteem ontwikkelen om dat doel te dienen, het *Incompatible Time-Sharing System* (ITS) (een woordspeling op het *Compatible Time-Sharing System* dat eraan voorafging), dat hen in staat stelde om samen te programmeren. Als iemand inlogde en ontdekte dat een van zijn kameraden een nieuwe teksteditor of strategisch spel had ontwikkeld, konden ze simpelweg het bestand openen en zelf onmiddellijk bijdragen aan het project. Of, als twee hackers tegelijkertijd de computer gebruikten, konden ze de code gelijktijdig debuggen en verbeteren. Dit was de vrije en coöperatieve cultuur die Stallman in het AI Lab van MIT ontdekte.

Anarchisme

De computer van het AI Lab was inderdaad, door iedereen, vrij en zonder beperkingen, te gebruiken. Niet alleen werknemers, maar ook bezoekers van het lab konden de machine op elk gewenst moment gebruiken, en toegang krijgen tot elk programma of bestand dat zich op de machine bevond. De machine fungeerde als een gedeelde voorziening, voor iedereen beschikbaar.

Het leidde wel tot moeilijkheden. Iedereen die een ITS-computer gebruikte, kon bijvoorbeeld elk bestand verwijderen, zelfs als ze deze niet zelf hadden gemaakt. Op dezelfde manier verstoorde het crashen van de machine elk actief gebruikersproces.

Maar in de praktijk waren dergelijke incidenten zeldzaam. Het vernietigen van iemand anders zijn werk paste niet in de hackercultuur en hoewel het crashen van de computer hinderlijk was voor andere gebruikers, gaf het hen ook de kans om samen te werken bij het debuggen van de code en het vinden van een oplossing voor wat de crash veroorzaakte.

Dit was heel anders dan de computeromgevingen bij het IBM Wetenschappelijk Centrum en Harvard waaraan Stallman gewend was geraakt. Die machines

waren ontworpen met beveiligingsfuncties die vereisten dat sommige mensen meer bevoegdheden hadden dan anderen: bepaalde programma's waren alleen toegankelijk voor bepaalde gebruikers, zoals systeembeheerders of sommige professoren. De *elite*, zij die bevoorrechte accounts hadden, kon eenzijdig beslissen wat anderen wel en niet konden doen op de machines, wat betekende dat reguliere gebruikers vaak om hulp of toestemming moesten vragen.

De nieuwe collega's van Stallman in het AI Lab walgden van dit soort beleidslijnen. Volgens hen hadden de beheerders in feite politiestaten opgezet in hun respectieve computeromgevingen, waarbij ze zichzelf de autoriteit toe-eigenden om andere gebruikers te besturen en controleren.

Nu hij hun vrije alternatief had ervaren, was Stallman het volledig met hen eens. Terwijl het AI Lab bewees dat hun vorm van anarchie een productieve werkomgeving kon bevorderen, raakte hij ervan overtuigd dat de beperkende en gecontroleerde systemen feitelijk een digitale vorm van fascisme vertegenwoordigden.[32]

'De gebruikers van ons systeem waren vrije mensen, aan wie gevraagd werd om zich verantwoordelijk te gedragen. In plaats van een elite van macht, hadden we een elite van kennis, bestaande uit iedereen die gemotiveerd was om te leren', schreef Stallman later. 'Omdat niemand anderen kon domineren op onze machine, functioneerde het lab als een anarchie. Het zichtbare succes hiervan bekeerde mij tot het anarchisme. Voor de meeste mensen betekent *anarchie verspillende, destructieve wanorde*, maar voor een anarchist als ik betekent het vrijwillige organisatie naar behoefte, met de nadruk op doelen, in tegenstelling tot regels en vereisten tot uniformiteit omwille van de uniformiteit.'[33]

Hoewel Stallman geen anarchist was in de meest complete betekenis van het woord – hij geloofde namelijk nog steeds dat de staat vele belangrijke functies uitvoerde, waaronder het financieren van het AI Lab – dacht hij dat het anarchistische model ook in andere computeromgevingen kon werken. En inderdaad, rond deze tijd begon de hackercultuur zich ook te verspreiden buiten MIT, met name naar Stanford University, die een eigen AI Lab kreeg. Tegen het begin van de jaren '70 had de hackergemeenschap een nieuwe basis gevestigd in

32 Richard Stallman, *Talking to the Mailman*, Interview door Rob Lucas, New Left Review, Sept–Oct 2018, online

33 Richard Stallman, *RMS Berättar*, Linköping University, online

de San Francisco Bay Area.

En Stallman geloofde dat de hackercultuur ook buiten het academische domein levensvatbaar zou zijn. Met het AI Lab als een geslaagd voorbeeld, zou het vrije en samenwerkende ethos wellicht een model kunnen worden voor de opkomende computerrevolutie.

Problemen in het paradijs

Later werd echter duidelijk dat de verspreiding van de hackercultuur niet zo eenvoudig was.

Bijna tien jaar later was Stallman nog steeds werkzaam in het lab. Hij merkte dat de hackercultuur daadwerkelijk verdreven begon te worden uit haar oorspronkelijke thuisbasis. Mensen in en rond het AI Lab gingen steeds meer wachtwoorden en, erger nog, auteursrechtelijke licenties omarmen. Tegelijkertijd wilden de beheerders van MIT dat computergebruikers formulieren invulden voordat ze de machines konden bedienen, een praktijk die Stallman actief probeerde tegen te houden.[34]

En toch, vergeleken met wat er ging komen, waren dit kleine problemen.

In 1979 wilden Richard Greenblatt, een van de meest gerespecteerde hackers van het lab, en Russell Noftsker, een voormalig labbeheerder, een van de meest prominente projecten van het AI Lab op de markt brengen. Hun plan was om een start-up op te richten om speciale computers te verkopen die ontworpen waren voor LISP, de programmeertaal voor AI die in het onderzoeksinstituut in ontwikkeling was.

Het werd echter al snel duidelijk dat Greenblatt en Noftsker zeer verschillende ideeën hadden over de start-up. Greenblatt wilde dicht bij de geest van het AI Lab en haar anarchistische cultuur blijven. Dit betekende dat hij uit de buurt wilde blijven van investeerders en zo dicht mogelijk wilde aanleunen bij de gekende hackercultuur. Noftsker vond de benadering van Greenblatt echter onrealistisch. Hij zag een meer traditioneel bedrijf voor zich, dat zijn producten zou beschermen met softwarelicenties en auteursrechten.

Greenblatt en Noftsker slaagden er niet in om een compromis te bereiken en

34 Stallman, *Talking to the Mailman*.

besloten uit elkaar te gaan. Ze startten ieder hun eigen onderneming: Greenblatts *LISP Machine Incorporated* (LMI) en Noftskers *Symbolics* werden rivalen.

Aanvankelijk deelden zowel LMI als Symbolics de code die ze bij het AI Lab produceerden, en daardoor ook met elkaar. Echter, begin 1982, verbrak Symbolics deze driehoeksrelatie. Noftsker besloot dat het AI Lab wel nog de door Symbolics aangepaste versie van de LISP-software kon gebruiken, maar LMI mocht dit niet meer. Het was een ultimatum. De beslissing van Noftsker betekende dat elke hacker in het lab een kant moest kiezen.

Hoewel Greenblatt, die veel werk had verricht om het LISP-project te realiseren, de kennis en de capaciteiten had, beschikte hij over te weinig middelen. Ondertussen had het bedrijfsplan van Symbolics Noftsker in staat gesteld om fondsen te werven van investeerders. Hij gebruikte het geld om enkele van de beste hackers van het AI Lab in te huren. Om er zeker van te zijn dat de nieuw aangeworven hackers exclusief voor zijn start-up zouden werken, verbood hij alle medewerkers van Symbolics om bij te dragen aan het AI Lab.

In één klap waren veel van de beste programmeurs van het computerlab verdwenen, en ze namen hun werk met hen mee.

Het AI Lab was effectief uitgekocht. MIT's toevluchtsoord voor vrije samenwerking was frontaal in botsing gekomen met meedogenloze zakelijke belangen. Omdat de kleinschalige utopie van de hackers geroofd was van haar meest waardevolle middelen, bleef slechts een uitgehold overblijfsel van het onderzoekscentrum achter. Het lab had tijdens een kortstondig gouden tijdperk gediend als een toonbeeld van effectief anarchisme, maar was dat na de beslissing van Noftsker niet langer.

Voor Stallman betekende dit het einde van het lab.

De ontgoochelde hacker vatte het kort daarna samen in een brief:

De personen die nog in het lab waren, waren de professoren, studenten en non-hackeronderzoekers, die niet wisten hoe ze het systeem of de hardware moesten onderhouden, of dit zelfs niet wilden weten. Machines begonnen te breken en werden nooit gefixt; soms werden ze gewoon weggegooid. Noodzakelijke veranderingen in software konden niet worden doorgevoerd. De niet-hackers reageerden hierop door over te schakelen naar commerciële systemen, wat fascisme en licentieovereenkomsten met zich meebracht. Ik slenterde door het lab, door de kamers die 's nachts leeg waar ze

vroeger vol waren en dacht: 'Oh mijn arme AI-lab! Je gaat dood en ik kan je niet redden.' Iedereen verwachtte dat als er meer hackers werden opgeleid, Symbolics ze zou wegkapen, dus het leek niet eens de moeite waard om het te proberen... de hele cultuur werd uitgewist...[35]

Stallman had ooit gedroomd van een toekomst geïnspireerd door de vrije en collaboratieve hackercultuur, maar hij geloofde nu dat hij in plaats daarvan de laatste ademtochten ervan aan het aanschouwen was.

'Ik ben de laatste overlevende van een dode cultuur', klaagde Stallman met een gevoel van drama. 'En ik hoor echt niet meer thuis in de wereld. En op sommige manieren voel ik dat ik eigenlijk dood zou moeten zijn.'[36]

Vrije software

Toch was Stallman nog niet helemaal bereid om op te geven.

Stallman wees voornamelijk Noftsker aan als schuldige voor de ondergang van het AI Lab. De hacker zette zich vervolgens in om alle software-upgrades van Symbolics opnieuw te implementeren. Hij hield hun documentatie van nieuwe functies bij en schreef vervolgens code die dezelfde functies bood. In feite deed hij in zijn eentje het werk van zes ontwikkelaars van de start-up. Hij deelde zijn code met LMI, waardoor het bedrijf van Greenblatt een kans had om tegen Symbolics te concurreren. Hij hield dit lang genoeg vol zodat Greenblatt nieuwe programmeurs kon aannemen en zijn bedrijf weer op de rails kon krijgen.[37]

Vervolgens besloot Stallman dat het tijd was voor een nieuwe start. Hij had zichzelf ervan overtuigd dat de hackercultuur de wereld nog steeds kon veranderen, maar concludeerde dat er een nieuw plan nodig was: 'een ambitieus project dat de fundamenten aanvalt van de manier waarop de commerciële, vijandige manier van leven wordt voortgezet.'[38]

Specifiek wilde Stallman de algemene trend naar *propriëtaire software* omkeren, software die door licenties en auteursrechten beperkt werd, en die in de jaren

35 Levy, *Hackers*, 448.
36 Levy, *Hackers*, 472.
37 Stallman, *High School Misfit*.
38 Stallman, *RMS Berättar*.

'80 steeds gebruikelijker werd. In lijn met de hackerethiek geloofde Stallman dat een computerprogramma maximaal nut biedt als mensen het kunnen verbeteren. En aangezien computers het quasi kosteloos maakten om informatie te kopiëren, stelde hij dat het verhinderen van het delen van software 'de gehele mensheid saboteert', zo betoogde de hacker.[39]

Erger nog, propriëtaire software kan doorgaans niet geïnspecteerd worden. Als mensen geen toegang hebben tot de in mensentaal leesbare broncode van de software die ze op hun computers draaien, kunnen ze niet zeker weten wat hun eigen machine eigenlijk doet. Een programma kan kwaadaardig zijn en bijvoorbeeld zijn gebruiker beperken, censureren, bespioneren of op een andere manier misbruiken.[40]

Stallman was van mening dat het gebruik van propriëtaire software in feite betekende dat je de controle overliet aan degene die het had ontwikkeld.[41]

'Als gebruikers het programma niet beheersen, beheerst het programma de gebruikers', redeneerde hij. 'Met eigendomsrechtelijk beschermde software is er altijd een entiteit – de *eigenaar* van het programma – die controle heeft over het programma en daarmee macht uitoefent over de gebruikers.'[42]

In plaats daarvan wilde Stallman dat computers instrumenten van zelfbeschikking en vrijheid waren. Hij geloofde dat gebruikers te allen tijde de controle over hun eigen apparaten moesten hebben.

Om dit te verwezenlijken, ontwikkelde hij een filosofie die vereiste dat elk computerprogramma vier essentiële vrijheden moest bieden:[43]

- De vrijheid om het programma te gebruiken zoals je wenst, voor welk doel dan ook (vrijheid 0)[44].

39 Steven Levy, *Hackers*, 441–42.

40 Angela Watercutter, *Why Free Software Is More Important Now Than Ever Before*, Wired, 20 september 2013, online

41 Voor de nauwkeurigheid dient opgemerkt te worden dat dit deel van het argument technisch gezien pas duidelijk naar voren kwam toen Stallman het GNU-project een jaar of zo later lanceerde: het was nog geen deel van zijn oorspronkelijke motivatie om het project überhaupt te starten. Dit kleine anachronisme is in de tekst gebleven ten behoeve van de leesbaarheid.

42 Richard Stallman, *Free Software Is Even More Important Now*, gnu.org, online

43 GNU Operating System, *What is Free Software?* online

44 Eigenlijk werd vrijheid 0 pas expliciet toegevoegd in de jaren 1990. Daarvoor dacht Stallman dat het een automatische juridische consequentie was van de oorspronkelijke drie vrijheden.

- De vrijheid om te bekijken hoe het programma werkt en het zo aan te passen dat het je computerwerk naar wens uitvoert (vrijheid 1). Toegang tot de broncode is een noodzakelijke voorwaarde om dit te realiseren.

- De vrijheid om kopieën te herverdelen zodat je anderen kunt helpen (vrijheid 2).

- De vrijheid om kopieën van je aangepaste versies met anderen te delen (vrijheid 3). Door dit te doen kun je de hele gemeenschap de kans geven om te profiteren van je veranderingen. Toegang tot de broncode is een noodzakelijke voorwaarde.

Of samengevat, gebruikers hadden over het algemeen 'de vrijheid om software te draaien, kopiëren, verspreiden, bestuderen, veranderen en te verbeteren.'[45] Dit vereist dat de menselijk-leesbare broncode van een programma gepubliceerd is, en dat deze niet onderhevig is aan beperkende auteursrechtenlicenties. Stallman zou software, die deze vier essentiële vrijheden bood, classificeren als vrije software (vrij in de betekenis van *vrijheid*, benadrukte de hacker graag, en niet zoals in *gratis bier*).

GNU

Om echt de belofte van vrije software waar te maken, begreep Stallman dat elk programma op een computer de vereiste vrijheden moest bieden. Dit omvatte – in de eerste plaats – het besturingssysteem. Een tekstverwerker die zich houdt aan de vier vrijheden kan zijn gebruiker niet stiekem bespioneren, maar als het besturingssysteem waarop de tekstverwerker draait ook niet-vrije software is, kan niet worden uitgesloten dat het besturingssysteem bespioneert.

Daarom kondigde Stallman in 1983 zijn ongelooflijk ambitieus project aan om een alternatief te bieden voor het populaire Unix besturingssysteem. Waar Unix propriëtaire software was, bestond Stallmans besturingssysteem volledig uit vrije software. Passend noemde hij het project GNU: GNU is Niet Unix! (inderdaad, een recursief acroniem).[46]

45 GNO Operating System, *What is Free Software?*

46 Richard Stallman, *Free Unix!* September 27, 1983, online

GNU belichaamde de hackerethiek en wees propriëtaire software volledig af.

'Ik heb veel andere programmeurs gevonden die enthousiast zijn over GNU en willen helpen', schreef Stallman in het GNU Manifesto dat hij uitgaf na de aankondiging, waarin hij het doel en de staat van het project beschreef. 'Veel programmeurs zijn ongelukkig over de commercialisering van systeemsoftware. Het stelt hen wellicht in staat om meer geld te verdienen, maar het zorgt ervoor dat ze zich in conflict voelen met andere programmeurs in plaats van als kameraden. […] GNU dient als voorbeeld om te inspireren en als een vaandel om anderen rond te verzamelen om ons te vergezellen in het delen.'[47]

Inderdaad, GNU was meer dan alleen een stukje software, maar vertegenwoordigde het onstaan van een nieuwe sociale beweging: de vrije softwarebeweging.

Om de beweging te ondersteunen, richtte Stallman in 1985 ook de non-profitorganisatie Free Software Foundation op. De stichting zou pleiten voor vrije software en geld inzamelen om vrije softwareprojecten te financieren. Daarnaast leidde de Free Software Foundation de introductie van speciale vrije softwarelicenties onder de nieuwe paraplu van *copyleft*, ontworpen om vrije software te stimuleren.

Dit omvatte vooral de GNU General Public License: een licentie die het recht verleent om broncode te verspreiden en te wijzigen, zolang dit gebeurt onder dezelfde vrije voorwaarden. Met andere woorden, ontwikkelaars van vrije software konden software die onder deze licentie werd uitgebracht op elke gewenste manier in hun eigen projecten integreren, maar ontwikkelaars van propriëtaire software konden dat niet. Met het GNU-project in volle gang en de nieuwe licenties geïmplementeerd, stond vrije software op het punt een krachtige invloed te worden waarmee rekening moest worden gehouden.

De kathedraal en de bazaar

Traditioneel werden vrije softwareprojecten uitgevoerd door kleine groepjes ontwikkelaars vanuit speciale technologiehubs, zoals het AI Lab van MIT. Maar toen hij aan GNU begon te werken, nodigde Stallman andere ontwikkelaars uit om ook aan zijn project mee te werken. Door gebruik te maken van het ontluikende

47 GNU Operating System, *The GNU Manifesto*, 1985, online

internet, konden hackers zelfs vanuit de hele wereld code bijdragen.

Hoewel Stallman aan bijdragers voor hun werk normaal geen financiële compensatie beloofde, waren veel ontwikkelaars desondanks bereid om te helpen GNU werkelijkheid te laten worden. Misschien hoopten sommigen van hen respect of status te verwerven onder hun programmeercollega's door bij te dragen, zoals dat altijd een factor was binnen de hackergemeenschap. Anderen droegen wellicht bij omdat ze zelf GNU wilden gebruiken. Weer anderen vonden misschien de uitdaging op zichzelf boeiend genoeg om eraan deel te nemen. En misschien wilden sommigen simpelweg de wereld een betere plek maken en zagen ze dit project als een middel om dat doel te bereiken.

Wat hun redenen ook waren, ze droegen bij. Bovendien waren hun bijdragen waardevol. Vrijwillige programmeurs leverden, enigszins opmerkelijk, hoogwaardige code. Het stelde Stallman in staat om vele afzonderlijke delen van het GNU-besturingssysteem een paar jaar later al te voltooien — een indrukwekkende prestatie.

Rond datzelfde moment maakte de Finse software-ingenieur Linus Torvalds graag gebruik van de vrijheid geboden door de GNU General Public License. Hij nam een groot deel van Stallmans GNU-code, maar voegde zijn eigen kernel toe (een programma dat zich in het hart van een besturingssysteem van een computer bevindt), en in 1992 bracht Torvalds Linux uit.[48] Het was het eerste werkende besturingssysteem dat volledig uit vrije software bestond.

Maar Torvalds' voornaamste vernieuwing was mogelijk niet het Linux-kernel zelf. Het was de manier waarop hij het maakte. De jaren ervoor ontwikkelde de software-ingenieur een proces dat expliciet is ontworpen voor samenwerking via het internet.

Zoals uitvoerig besproken door Linux-bijdrager Eric S. Raymond in zijn essay *The Cathedral & The Bazaar* uit 1997 en het (later) gelijknamige boek, was de grootste aanpassing die Torvalds maakte, de benadering van de veiligheid van het project.

Tot die tijd beschouwden vrije software-ontwikkelaars bugs en andere kwetsbaarheden als grote risico's die aangepakt moesten worden door toegewijde

48 Om de zware afhankelijkheid van het project van GNU te benadrukken, geven sommigen de voorkeur aan de naam *GNU/Linux*.

experts die hun software zorgvuldig beoordeelden. Dit gold ook voor de code die ze van externe bijdragers ontvingen. Ze zouden de code pas vrijgeven als ze er zeker van waren dat het veilig was om deze te gebruiken. Raymond bestempelde deze top-down benadering als het *kathedraal*model.

In plaats daarvan gebruikte Torvalds wat Raymond het *bazaar*model noemde. Dit model gebruikte een flexibelere methode om bijdragen te integreren, waardoor ontwikkelaars hun wijzigingen meer direct konden uploaden naar verschillende versies van de software. Andere bijdragers konden de software vervolgens downloaden, testen en wijzigingen in hun eigen versies overnemen.

Zo'n flexibel systeem zou kunnen leiden tot versies van de software met meer fouten dan de software van hun tegenhangers in het kathedraal-model. Maar omdat het ontwikkelproces openlijk plaatsvindt, zijn andere bijdragers meestal sneller in staat om fouten te ontdekken en ze te corrigeren. Indien nodig, wordt de oplossing direct opgenomen in een nieuwe versie; onder het bazaarmodel vinden software-updates sneller en vaker plaats.

'Met een groot genoeg aantal bèta-testers en mede-ontwikkelaars, wordt bijna elk probleem snel vastgesteld en is de oplossing voor iemand duidelijk', schreef Raymond in zijn essay, waarbij hij een van de belangrijkste lessen die hij over de jaren had geleerd, samenvatte. 'Of, minder formeel, "Met genoeg ogen, zijn alle bugs oppervlakkig." '[49]

Hij gaf de uitspraak de naam de *Wet van Linus*.

Opmerkelijk genoeg, geloofde Raymond dat dit ontwikkelingsmodel voordelen kon bieden zelfs aan bedrijven en mensen die Stallmans bezorgdheid over eigendomssoftware niet deelden, maar gewoon kwaliteitscode wilden tegen lage kosten. Hij vermoedde echter dat velen van hen (vooral bedrijven) terughoudend waren om gratis software te gebruiken, juist omdat ze afgeschrikt werden door de ideologische verhalen eromheen. Om minder nadruk te leggen op Stallmans originele motivaties en meer op de pragmatische voordelen, leidde Raymond daarom in de late jaren '90 de poging om vrije software te rebranden als *open source software*.

Stallman stond zelf echter niet achter de herbenoeming. Voor hem was vrijheid

49 Eric S. Raymond, *The Cathedral & The Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*.

het voornaamste, en de term *open source* deed afbreuk aan deze boodschap. Vandaag de dag verwijzen de termen *vrije software* en *open source software* in vrijwel alle gevallen naar hetzelfde concept, maar het verschil in terminologie blijft de filosofische kloof vertegenwoordigen. De term *vrije en open source software* (FOSS) wordt gebruikt om beide zijden van het schisma expliciet te omvatten.[50]

Gemeenschappelijk begrip

Het bazaarmodel kan hoogwaardige code opleveren. Maar die kwaliteit is geen vanzelfsprekendheid. Volgens de Wet van Linus, vereist hoogwaardige code voldoende *ogen*, oftewel bijdragers.

FOSS-projecten hebben meestal niet de middelen om financiële beloningen te geven aan potentiële bijdragers. Daarnaast worden bestaande machtsverhoudingen vaak genegeerd in het kader van vrije en open-source-ontwikkeling. Zoals Raymond ook al stelde in zijn essay, was dwang natuurlijk volledig buiten de orde in 'het anarchistische paradijs dat we het internet noemen.' [51] Het aantrekken van bijdragers is daarom een cruciale vaardigheid gebleken voor ontwikkelaars van vrije en open software.

Geïnspireerd door de negentiende-eeuwse Russische anarchist Pyotr Alexeyevich Kropotkin, legde Raymond uit dat projectleiders moeten leren hoe ze effectieve gemeenschappen van belanghebbenden kunnen werven en motiveren op basis van een gemeenschappelijk begrip. Om ontwikkelaars te overtuigen bij te dragen, moet de leiding van een project bedenken hoe het project voordelen biedt voor hen. De prikkels moeten worden afgestemd op een gezamenlijk doel, stelde Raymond voor: 'een serieuze inspanning van vele samenkomende wilskrachten.'[52]

Dit betekent in de praktijk dat niemand echt de leiding heeft over FOSS-projecten in de bazaarstijl. Een projectleider kan het project niet in een richting sturen die niet gedragen wordt door de rest, zonder de ontwikkelaars te verliezen

50 Richard Stallman is ook geen fan van deze terminologie. Als er een term moet worden gebruikt die beide kanten van de kloof omvat, geeft hij de voorkeur aan *Free/Libre and Open Source Software* omdat dit duidelijker overbrengt dat het *vrije* deel over *vrijheid* gaat.

51 Raymond, *The Cathedral & The Bazaar*, 52.

52 Raymond, *The Cathedral & The Bazaar*, 52.

die hij zo hard nodig heeft. In het bazaarmodel wordt software beheerd door zijn schare van bijdragers, elk met hun eigen persoonlijke reden om betrokken te zijn.

Wanneer deze prikkels wel in lijn liggen en er een groep bijdragers bereid is aan een gemeenschappelijk doel te werken, kunnen de resultaten geweldig zijn. Hoewel niemand ooit echt de leiding heeft, zijn deze grootschalige samenwerkingsverbanden tussen vreemden met sterk uiteenlopende niveaus van kennis en vaardigheden, erin geslaagd om zeer complexe programma's te produceren, waarvan de Linux-kernel slechts één voorbeeld is van vele.

De ontwikkeling van vrije en open source software lijkt op die manier sterk op die andere vorm van grootschalige, leiderloze samenwerking: vrije markten. Net zoals vrije markten bestaan FOSS-projecten alleen uit vrijwillige interacties, benutten ze de kennis die verspreid is onder de deelnemers en wat misschien wel het meest interessant is, kunnen ze beter presteren dan top-down organisatievormen.

Net zoals vrije markten, kunnen vrije en open softwareprojecten een spontane orde vormen.

> *'In veel opzichten gedraagt de Linux-wereld zich als een vrije markt of een ecologie, een verzameling van individuen die hun eigenbelang nastreven. Tijdens dit proces ontstaat een zichzelf corrigerende spontane orde die veel complexer en efficiënter is dan wat elke vorm van centrale planning ooit zou kunnen bereiken.'*[53]

53 Raymond, *The Cathedral & The Bazaar*, 52.

Hoofdstuk 3

Neutraal geld

Friedrich Hayek legde in de jaren dertig het idee van de vrije markt uit in termen van spontane orde. Hij betoogde dat individuen, door in hun eigen belang te handelen, in staat waren middelen op een efficiënte manier over de samenleving te verdelen met behulp van het prijssysteem: een verbazingwekkend concept.

Het was dus volkomen logisch dat Hayek bijzonder geïnteresseerd was in het goed waarin goederen en diensten worden uitgedrukt — geld.

Vreemd genoeg, lijkt geld een fundamenteel principe van de Oostenrijkse economie tegen te spreken. Deze stroming is opgebouwd op het idee dat waarde subjectief is: mensen kennen waarde toe aan producten en diensten als ze een persoonlijke behoefte vervullen. Schoenen worden gewaardeerd omdat je ze kunt dragen, appels worden gewaardeerd omdat je ze kunt eten en auto's worden gewaardeerd omdat je erin kunt rijden. Maar geld lijkt op het eerste gezicht geen directe behoefte te vervullen. Je draagt het niet, je eet het niet, je rijdt er niet in.

Geld lijkt dus vrij waardeloos. Desondanks wordt geld algemeen geaccepteerd als betalingsmiddel in handel.

Deze schijnbare tegenstrijdigheid was in het begin van de twintigste eeuw al aangepakt door Hayeks mentor aan de Universiteit van Wenen, Ludwig von Mises.[54] De uitleg van Mises, de regressietheorie genoemd, erkent dat mensen daadwerkelijk geen geld willen. Ze willen de goederen en diensten die gekocht kunnen worden met geld. Ze verlangen naar koopkracht.

54 Ludwig von Mises, *The Theory of Money and Credit*, vertaling. J.E. Batson.

Mises redeneerde dat de verwachte koopkracht van geld afgeleid is van eerdere prestaties. Als $ 10 je gisteren in een restaurant een lunch kon kopen, zullen mensen aannemen dat ze er morgen ook een lunch voor kunnen kopen. En de reden dat $ 10 hen gisteren een lunch kon bieden, is dat de restauranteigenaar wist dat hij daarmee de dag daarvoor tien broden kon kopen bij de bakkerij, en waarschijnlijk dus ook de dag erna. De bakker accepteerde op zijn beurt $ 10 in ruil voor zijn brood, want daarmee kon hij de dag ervoor een pond meel kopen bij de lokale molenaar… en zo verder.

Maar dit laat uiteraard nog steeds een belangrijk deel van de tegenstrijdigheid onopgelost: wanneer begonnen mensen *voor het eerst* geld te accepteren en, vooral, waarom? Als we ver genoeg terug in de tijd gaan – regressie – moet er ooit iemand de eerste zijn geweest die geld begon te accepteren, zonder enige vorige ervaring om op te vertrouwen bij het inschatten van toekomstige koopkrachtverwachtingen.

Mises loste dit vraagstuk op door de theorie van Carl Menger over te nemen, die stelde dat geld oorspronkelijk is ontstaan uit ruilhandel.

Van ruilhandel naar geld

In een ruileconomie – een economie zonder geld – ruilen mensen rechtstreeks goederen en diensten met elkaar. Als de schoenmaker een paar schoenen heeft, maar liever een brood wil, en de bakker een brood heeft maar liever een paar schoenen wil, dan ruilen ze hun producten met elkaar. Na deze transactie zijn ze beiden (subjectief gezien) beter af dan daarvoor.

Zo'n ruileconomie lijdt echter onder een probleem wat bekend staat als de *dubbele toevalligheid van behoeften*. Een ruil kan alleen plaatsvinden als twee personen precies het product willen dat de ander te bieden heeft. De schoenmaker kan alleen schoenen ruilen voor een brood als de bakker toevallig een nieuw paar nodig heeft… maar dit gebeurt waarschijnlijk niet heel vaak.

Meer gespecialiseerde vaklieden hebben het in een ruileconomie nog moeilijker om te bemachtigen wat ze willen, omdat minder mensen hun product nodig hebben. Een horlogemaker kan bijna nooit een horloge ruilen voor een brood of een paar schoenen, omdat bakkers en schoenmakers niet vaak een nieuw horloge

nodig hebben.

Maar het tegenovergestelde is ook waar: sommige producten zouden relatief gemakkelijk te verhandelen moeten zijn. Neem bijvoorbeeld zout, en laten we aannemen dat veel mensen in deze economie vrij regelmatig zout nodig hebben om een maaltijd op smaak te brengen, of om voedsel te conserveren. In de woordenschat van Menger en de Oostenrijkse school, is zout *verkoopbaarder* (of *verhandelbaarder*) dan een horloge.

En zout heeft ook andere voordelen. Het is behoorlijk duurzaam want zout bederft niet. Het is redelijk draagbaar; zout kan makkelijk in een tas worden meegenomen. Het is deelbaar; zout kan moeiteloos in kleinere porties worden verdeeld, en die kleinere porties kunnen net zo gemakkelijk weer worden samengevoegd tot een grotere hoeveelheid. Bovendien is zout ook gemakkelijk te herkennen, en het is redelijk fungibel, wat betekent dat verschillende porties onderling uitwisselbaar zijn; zout is zout. En tot slot, afhankelijk van waar (en wanneer) je bent, kan zout ook schaars zijn; het kan moeilijk zijn om er meer van te verkrijgen.

Menger bedacht daarom dat het voor de horlogemaker verstandig was om een lading zout te accepteren, wanneer dit hem in ruil voor een horloge wordt aangeboden. Zelfs als hij zelf geen behoefte aan zout heeft, dan zou de bakker dit zeker wel hebben. De horlogemaker kan vervolgens het zout met de bakker ruilen en zo eindelijk aan dat brood komen dat hij nodig heeft.

Daarnaast is het niet alleen voor de horlogemaker verstandig om zout in ruil aan te nemen, maar ook voor de schoenmaker. De bakker zou waarschijnlijk vaker zout dan een paar schoenen accepteren in ruilhandel. Dit geeft de horlogemaker dus nog meer mogelijkheden met het zout dat hij in ruil krijgt, omdat hij het kan uitgeven bij zowel de bakker als de schoenmaker.

Naarmate meer mensen in deze ruileconomie zout gaan accepteren in de verwachting dat anderen dat ook zullen doen, zet dit een zelfversterkende cyclus in gang. Voor elke extra persoon die zout accepteert in ruilhandel, wordt zout voor iedereen aantrekkelijker om als ruilmiddel te accepteren. Op deze manier kan zout zich als een gangbaar *ruilmiddel* ontwikkelen.

Hoewel sommige mensen in deze economie zelf geen zout nodig hebben, of een dringende noodzaak om het aan iets uit te geven, zullen ze erop beginnen te vertrouwen dat het uiteindelijk nuttig voor hen zal zijn. Daarom beginnen ze met het opslaan van zout voor toekomstig gebruik. Zo wordt zout ook een *opslag van*

waarde.

En uiteindelijk zullen mensen in deze economie de waarde van producten en diensten in zout beginnen te meten. Een horloge kost misschien een kilo zout, een paar schoenen een pond, en een brood een ons. Zout wordt gebruikt om prijzen vast te stellen, waardoor het een *rekeneenheid* wordt.

Zodra het deze drie eigenschappen verwerft – ruilmiddel, opslag van waarde en rekeneenheid – is zout geld geworden.

Dit vergroot op zijn beurt de vraag naar zout. In deze economie werd zout oorspronkelijk alleen gewaardeerd om zijn inherente eigenschappen — het vermogen om een maaltijd te kruiden of voedsel te conserveren.[55] Maar zodra het als geld wordt aangenomen, zijn veel mensen erop gebrand meer zout te vergaren, omdat dit hen in staat stelt elk ander product te kopen. Het proces van *monetarisatie* voegt een *monetaire* premie aan de waarde van zout toe.

Deze premie verklaart waarom mensen bereid zijn geld – in dit voorbeeld, zout – aan te nemen in ruil voor goederen en diensten die op zichzelf meer wensen of behoeften vervullen, waardoor de schijnbare tegenstrijdigheid wordt overwonnen die werd geïntroduceerd door de subjectieve waardetheorie.

In het verleden werd zout daadwerkelijk als betaalmiddel gebruikt. Enkele duizenden jaren geleden ontvingen soldaten in het Romeinse Rijk hun loon in zout; het hedendaagse woord *salaris* is afgeleid van het Latijnse woord *salarium*, dat *zoutgeld* betekent. Toen de Italiaanse ontdekkingsreiziger Marco Polo in de dertiende eeuw naar China reisde, ontdekte hij dat de plaatselijke bevolking elkaar betaalde met een soort pannenkoeken gemaakt van zout. En er waren zelfs bepaalde Ethiopische stammen die zout als geld gebruikten, zelfs zo recent als de twintigste eeuw.

Desalniettemin ontdekten diverse beschavingen wereldwijd over een periode van duizenden jaren dat er een beter ruilmiddel bestond dan zout. Tegen de tijd dat Mises zijn regressietheorema publiceerde, was het grootste deel van de wereld

55 Dit wordt soms beschouwd als *intrinsieke waarde*, een veelgebruikte uitdrukking in de economie om aan te geven dat een goed economische gebruikswaarde heeft los van zijn monetaire rol. Oostenrijkse economen verwerpen echter over het algemeen het idee dat producten überhaupt intrinsieke waarde hebben: waarde is volgens hen altijd subjectief.

overgegaan op het gebruik van goud.[56]

Goud

De eigenschappen van goud maken het bijzonder geschikt als geld. Goud is ongelooflijk duurzaam: het rot niet, roest niet en bederft ook niet. Het is ook redelijk draagbaar. Gouden munten kunnen makkelijk worden meegenomen. Het is deelbaar, want met de juiste gereedschappen kan goud worden gesmolten tot kleinere stukjes, en deze kleinere porties kunnen weer worden samengesmolten tot grotere baren. De eigenschappen van goud maken het ook relatief makkelijk te herkennen, terwijl het perfect inwisselbaar is. En wellicht het belangrijkste, het winnen van goud uit de aardkorst is een moeilijk en duur proces, en wordt steeds lastiger naarmate de makkelijkst toegankelijke goudmijnen uitgeput raken, wat enige mate van schaarste garandeert. En als bonus, het glanzende, gele metaal wordt door velen als mooi beschouwd.

In de laatste eeuwen werd goud echter vrijwel nooit echt als munteenheid in transacties gebruikt; mensen gebruikten over het algemeen namelijk bankbiljetten. Deze bankbiljetten konden worden ingewisseld voor goud, dat in eerste instantie veilig bewaard werd door de banken die de biljetten uitgaven. Klanten van banken vonden het handiger om de biljetten als ruilmiddel te gebruiken terwijl het goud veilig in de bankkluizen bleef liggen.

Dit zorgde ervoor dat het merendeel van al het goud dat in de reserves van banken werd gehouden, nooit werd opgevraagd. Het stimuleerde banken om meer bankbiljetten uit te geven – en uit te lenen – dan ze daadwerkelijk konden rechtvaardigen met het goud in hun kluizen. Het wijdverbreide gebruik van papiergeld leidde tot het tijdperk van de fractionele reservebank. Na verloop van tijd groeide dit uit tot een complex systeem van kredietverlening, corresponderende banken

56 Recenter archeologisch onderzoek, gepubliceerd in David Graebers *Debt: The First 5,000 Years*, suggereert dat er nooit een pure ruilhandel-economie is geweest zoals beschreven in de regressietheorie. In plaats daarvan gebruikten de oudste menselijke beschavingen schuld als hun eerste vorm van geld. Schuld werkt echter alleen als valuta in omgevingen met een hoge mate van vertrouwen en op reputatie gebaseerde systemen. In omgevingen met weinig vertrouwen was goud vaak de valuta bij uitstek, en het is heel goed mogelijk dat het edelmetaal deze status in de loop van de tijd verwierf via een proces dat lijkt op wat wordt beschreven in de regressietheorie.

en clearinginstellingen, nauw verweven met de aandelenmarkten en het bredere financiële systeem.

En uiteindelijk kwam dit allemaal onder toezicht te staan van centrale banken zoals de Federal Reserve. Deze centrale banken waren verantwoordelijk geworden voor het beheren van de goudreserves van hun landen, waartegen zij nationale valuta uitgaven — papieren bankbiljetten die konden worden ingewisseld voor een vastgestelde hoeveelheid goud. Het echte goud werd eigenlijk alleen maar gebruikt voor internationale handel. Aan het begin van de twintigste eeuw was de wereld gebonden aan de goudstandaard.

De Eerste Wereldoorlog bracht echter een einde aan *de klassieke goudstandaard*. De meeste regeringen schaften de inwisselbaarheid van hun valuta af, waardoor ze hun oorlogsinspanningen vrijer konden financieren.[57] In plaats van een vertegenwoordiging van goud, werden de ongedekte nationale valuta simpelweg door overheidsbesluit als geld beschouwd, een vorm van geld genaamd *fiatgeld* (het Latijnse woord 'fiat' betekent *laat het zo zijn*, en wordt meestal geassocieerd met overheidsdecreten.)

In de eerste jaren nadat de oorlog was beëindigd, fluctueerden de fiatvaluta vrij in waarde ten opzichte van elkaar. Dit betekende dat als iemand van bijvoorbeeld de Verenigde Staten een product uit Engeland wilde kopen (importeren), ze eerst een deel van hun dollars moesten inwisselen voor ponden. Als dit op een grote schaal gebeurde, zou de extra vraag naar ponden op zijn beurt de wisselkoers tegenover de dollar verhogen (het zou meer dollars kosten om dezelfde hoeveelheid ponden te kopen).

Een sterke pond maakt vervolgens het importeren van producten en diensten uit Engeland duurder voor Amerikanen, waardoor de export van Engeland geremd wordt. Tegelijkertijd maakt een zwakke dollar het importeren van producten en diensten uit de VS aantrekkelijker voor Britten, wat potentieel kan resulteren in een verhoogde vraag naar Amerikaanse goederen, en op zijn beurt weer kan zorgen voor een hogere vraag naar dollars. Schommelingen in de valutawaarde stabiliseren dus op een bepaalde manier de handelsbalans tussen de twee landen.

Er werd aangenomen dat dit een tijdelijke situatie zou zijn. De meeste landen

57 Nicholas Dimsdale, *British Monetary Policy and the Exchange Rate 1920-1938*, Oxford Economic Papers 33, New Series: 307–49.

hadden het voornemen naar een goudstandaard terug te keren. Maar invloedrijke economen uit die tijd betoogden dat deze nieuwe goudstandaard wat anders moest werken dan de klassieke goudstandaard. Aangezien het merendeel van het goud dat nationale munteenheden dekte nooit werd opgevraagd, konden centrale banken daadwerkelijk meer geld uitgeven dan ze in goud konden verantwoorden (in de VS mocht de Fed dit doen, zolang zij binnen de *gouddekkingsratio* bleven: de verhouding tussen goud in reserve en uitgegeven dollars moest ten minste 40 procent zijn).

Deze flexibiliteit bood de mogelijkheid voor een nieuw soort monetair beleid: centrale banken konden geld toevoegen aan, of onttrekken uit het bankensysteem om rentetarieven te manipuleren, met als doel de waarde van geld te stabiliseren.

Het was dit beleid waar Hayek zo fel kritiek op had.

De stabilisators

Irving Fisher, een toonaangevende econoom in het begin van de twintigste eeuw, was de eerste pleitbezorger voor dit nieuwe type van monetair beleid. Fisher was een van de eerste economen die zich zorgen maakten over deflatie, of specifieker, de deflatoire schuldenspiraal. Hij geloofde dat alleen stabiele prijzen 'de kwalen van monetaire instabiliteit' konden voorkomen.[58]

Fisher wist natuurlijk dat prijzen van specifieke goederen en diensten soms veranderen, omdat de vraag en het aanbod van verschillende producten en diensten om allerlei redenen door de tijd heen fluctueren. Maar hij geloofde dat het algemene, gemiddelde prijsniveau na verloop van tijd stabiel moest blijven. Om de stabiliteit van de koopkracht van een munteenheid te bepalen, had Fisher dus een manier nodig om gemiddelde prijzen vast te stellen. En hij wist precies waar hij moest zoeken.

In eerder onderzoek leverde de econoom empirisch bewijs voor de kwantiteitstheorie van geld. Deze theorie stelt dat het algemene prijsniveau van goederen en diensten proportioneel is met de hoeveelheid geld in omloop. Om dit te bewijzen, gebruikte Fisher indexen, waarbij elke index bestond uit een scala aan goederen en diensten en hun gemiddelde prijs op een specifiek moment in de tijd.

58 Irving Fisher, *The Purchasing Power of Money*.

Het vergelijken van deze indexen over verschillende tijdlijnen gaf inzicht in de ontwikkeling van het algemene prijsniveau.

Fisher bedacht dat vergelijkbare indices gebruikt konden worden om een stabiele vorm van geld te creëren, waarbij een dollar door de tijd heen hetzelfde aandeel van een index zou moeten kopen. Zo'n index zou een selectie van alle producten bevatten die de gemiddelde consument koopt: een *consumentenprijsindex* (CPI). Het ene jaar zou een dollar misschien meer aardappelen en minder wortelen kunnen kopen, en het volgende jaar meer wortelen en minder aardappelen, maar de gemiddelde koopkracht van een dollar, gemeten volgens de CPI, zou ongeveer hetzelfde moeten blijven.

Fisher beweerde dat de Federal Reserve de stabiliteit van de dollar kon nastreven door de rentetarieven te manipuleren. Hij had in 1920 de *Stable Money Association* opgericht om deze beleidswijziging te realiseren. Een collectief, bestaande uit economen, politici en ondernemers, pleitte voor een stabilisatiebeleid via parlementaire ondervragingen, bekend als de 'stabilisatiehoorzittingen', terwijl ze daarnaast ook hun zaak op internationale conferenties en andere bijeenkomsten bepleitten waar monetair beleid een gespreksonderwerp was. Dit hielp om de ideeën van Fisher tot in de hoogste rangen van het *Federal Reserve System* en daarbuiten te verspreiden .

De Stable Money Association vond al gauw een bondgenoot in Hayeks hedendaagse rivaal, John Maynard Keynes. Maar Keynes ging zelfs nog verder dan Fisher en de Stable Money Association. Hij stelde voor om de goudstandaard volledig los te laten. In zijn verhandeling uit 1923, *A Tract on Monetary Reform*, betoogde de econoom van *King's College* dat het edelmetaal niet geschikt was om stabiele prijzen te garanderen, omdat het zelf onderhevig was aan marktsentimenten.

Hoewel dit inderdaad gedeeltelijk verzacht kon worden als de centrale banken een flexibelere aanpak zouden hanteren om muntstabiliteit te bereiken, betoogde Keynes dat de gouddekkingratio uiteindelijk de speelruimte van de centrale banken fundamenteel beperkte. En in de praktijk zou deze genegeerd worden wanneer dat als noodzakelijk werd beschouwd.

'In werkelijkheid is de goudstandaard al een barbaars overblijfsel. […]. We zijn allemaal, van de gouverneur van de Bank van Engeland af, nu vooral geïnteresseerd in het behouden van de stabiliteit van bedrijven, prijzen en werkgelegenheid en het is

niet waarschijnlijk dat we, gedwongen om een keuze te maken, bewust deze dingen zullen opofferen voor het achterhaalde dogma.'[59]

Als geld daarentegen volledig van de beperkingen van goud bevrijd was, kon het monetaire beleid zo flexibel zijn als de monetaire autoriteiten nodig achtten.

De verwerping van stabiel geld

Hayek verwierp het gebruik van rentetarieven door centrale banken als middel, omdat hij geloofde dat dit enkel tot een volatielere conjunctuurcyclus leidde. Maar hij verwierp ook het doel om prijzen te stabiliseren. Hayek keurde deze stabilisatoren af.

Prijzen, legde Hayek uit, bevatten een breed scala aan informatie. Daardoor is het mogelijk dat de prijzen van identieke goederen op verschillende locaties van elkaar verschillen. Een krat bananen zou bijvoorbeeld goedkoper kunnen zijn in Colombia, waar bananen groeien, vergeleken met IJsland, waar de bananen eerst naartoe vervoerd moeten worden. De kosten van het transport (en daarmee de kosten van brandstof en meer) zouden verwerkt zijn in de prijs van bananen in IJsland.

Daarom redeneerde Hayek dat, technisch gezien, een krat bananen in Colombia en een krat bananen in IJsland in economische zin als twee verschillende producten moeten worden beschouwd. Het interspatiële prijssysteem — verschillende prijzen op verschillende locaties — maakte een efficiënte toewijzing van bronnen over de ruimte mogelijk.

Daarnaast betoogde de econoom dat iets vergelijkbaars gold voor anderszins identieke producten op verschillende tijdstippen. Zoals het interspatiële prijssysteem zorgt voor een efficiënte verdeling van middelen over ruimte, zorgt het intertemporele prijssysteem voor een efficiënte verdeling van middelen doorheen de tijd.

Hayek:

'Strikt genomen zouden goederen die technisch gelijk zijn maar alleen op verschillende tijdstippen beschikbaar zijn, in economische zin beschouwd moeten worden als

59 John Maynard Keynes, *A Tract on Monetary Reform*, 173.

verschillende goederen, net zoals goederen die technisch hetzelfde zijn maar zich op verschillende plaatsen bevinden.'[60]

Vrije markten bevorderen innovatie, en de meeste producten worden door deze innovatie goedkoper om te produceren. Het produceren van een krat bananen, wordt na verloop van tijd betaalbaarder doordat bananenkwekers verbeterde technologie voor het beheer van hun plantages hebben. Het is dan logisch dat een krat bananen over tien jaar goedkoper zal zijn dan een krat bananen nu: de verschillen in productiekosten zullen tot uiting komen in de respectievelijke prijzen.

Hayek geloofde dus niet dat het stabiliseren van prijzen op basis van indices überhaupt wenselijk was. Als prijzen kunstmatig stabiel worden gehouden, zou dit het intertemporele prijssysteem verstoren, en uiteindelijk ook de toewijzing van middelen doorheen de tijd verstoren.

Laten we zeggen dat een bananenboer verwacht dat de prijs van bananen (net zoals alle andere consumentenproducten, gemiddeld genomen) in de toekomst stabiel zal blijven, terwijl hij ook weet dat zijn productiekosten zullen dalen. Dit zet hem aan om te investeren in toekomstige productie ten koste van de productie vandaag: hij zal later dezelfde hoeveelheid bananen kunnen verbouwen voor minder totale kosten, terwijl hij elke krat bananen voor dezelfde prijs als vandaag zal kunnen verkopen, en zo zijn totale winst kan verhogen.

Als alle producenten in de economie op dezelfde manier denken, als ze allemaal dezelfde prikkels volgen, en investeren in productie voor de toekomst ten koste van productie vandaag, zou dit op korte termijn tot een tekort aan totale economische productie en op lange termijn tot een overschot leiden.

Hayek schreef:

'Als, tijdens een algemene uitbreiding van de productie, de verwachting met zekerheid is dat de prijzen van producten niet zullen dalen, maar stabiel zullen blijven of zelfs zullen stijgen, zodat op een later tijdstip dezelfde of zelfs een hogere prijs kan worden verkregen voor het product dat tegen een lagere prijs is geproduceerd, moet het resultaat zijn dat de productie voor de latere periode, waarin het aanbod al op een relatief

60 Friedrich A. Hayek, *Intertemporal Price Equilibrium and Movements in the Value of Money*, in 'The Collected Works of F.A. Hayek, Good Money: part I', ed. Stephen Kresge, 195.

adequaat niveau is, nog verder wordt uitgebreid ten koste van die voor de eerdere periode, waarin het aanbod relatief minder adequaat is.'[61]

Om een spontane orde doorheen de tijd te hebben, moeten prijzen de mogelijkheid krijgen om te dalen.

Hayek concludeerde daarom:

'De acceptatie van de noodzaak voor een intertemporeel prijssysteem is niet alleen onverenigbaar met, het staat lijnrecht tegenover de heersende opvatting dat constante prijzen doorheen de tijd een voorwaarde voor een ongestoorde economie zijn.'[62]

Natuurlijk erkende de Oostenrijker ook dat een daling van de prijzen in sommige gevallen een negatieve impact op de economie kan hebben: hij waarschuwde tegen de manipulatie van rentetarieven juist omdat het uiteindelijk tot deflatie zou leiden. Hayek stelde echter dat deflatie alleen een probleem is als de daling van de prijzen daadwerkelijk wordt veroorzaakt door een afname van de geldhoeveelheid. In dat geval zouden bedrijven inderdaad minder verdienen dan verwacht, wat, zoals ook Fisher had aangegeven, een deflatoire schuldenspiraal in gang zou kunnen zetten.

Hayek benadrukte dat als de daling van de prijzen niet veroorzaakt werd door een krimpende geldhoeveelheid, maar het resultaat was van goedkopere productieprocessen, dit probleem niet zou bestaan.

'Een daling van het prijspeil als gevolg van continue verbeteringen in alle productietakken heeft niet dezelfde problematische gevolgen als deflatie. Theorie is tot nu toe nauwelijks verder gekomen dan dit onderscheid tussen de effecten van prijswijzigingen die enerzijds afkomstig zijn van de goederenkant *en anderzijds van de* geldkant.'[63]

De goudwisselstandaard

De Stable Money Association had zich in de periode kort na de Eerste Wereldoorlog snel laten gelden. Slechts een jaar na de oprichting wist de groep hun

61 Hayek, *Intertemporal Price Equilibrium*, 207.

62 Hayek, *Intertemporal Price Equilibrium*, 190.

63 Hayek, *Intertemporal Price Equilibrium*, 214.

standpunt met succes te verdedigen op de Economische en Financiële Conferentie van Genua in 1922. Daar kwamen vertegenwoordigers van 34 grote geïndustrialiseerde landen bijeen om de grote economische en politieke problemen van het naoorlogse Europa op te lossen.

De vertegenwoordigers op de conferentie stemden in met het aannemen van een *goudwisselstandaard*. Nationale valuta zouden een vaste wisselkoers ten opzichte van goud aanhouden, maar centrale banken kregen relatieve flexibiliteit om een monetair beleid te voeren dat prijsstabiliteit nastreeft door middel van het manipuleren van rentetarieven.

Deze beleidslijnen voor prijsstabilisatie moesten per land worden gestuurd: de stabilisatoren stelden voor dat de koopkracht van een valuta binnen de eigen nationale economie stabiel zou moeten blijven. Maar dit betekende dat als het totale prijspeil in verschillende landen zou beginnen te variëren, de waarde van hun nationale valuta tegenover elkaar kon fluctueren, wat de internationale handel potentieel zou kunnen beïnvloeden.

De stabilisatoren erkenden dit, maar vonden dat die afweging het waard was.

'[…] Wanneer stabiliteit van het interne prijsniveau en stabiliteit van de externe wisselkoersen onverenigbaar zijn, is de eerste doorgaans te verkiezen', schreef Keynes, en 'wanneer het dilemma acuut is, is het behoud van het eerste ten koste van het laatste, gelukkig misschien, de weg van de minste weerstand.'[64]

De stabilisatoren geloofden ook dat internationale handel onder een goudwisselstandaard vrij soepel kon doorgaan, als de centrale banken zich zouden houden aan wat Keynes de 'regels van het spel' had genoemd. In een notendop, landen met een handelsoverschot (die dus meer exporteren dan importeren) en daardoor een instroom van goud hebben, zouden volgens deze regels de rentetarieven moeten verlagen. Dit zou meer leningen stimuleren, wat zou resulteren in meer valuta in omloop en uiteindelijk hogere prijzen in het algemeen. Landen met een handelstekort zouden naar verwachting de rentetarieven verhogen om het tegenovergestelde effect te bereiken.

Het verhoogde prijspeil in landen met een handelsoverschot zou de producten van dat land minder aantrekkelijk moeten maken voor export, wat zou moeten helpen om de omvang van het handelsoverschot te verminderen. Tegelijkertijd

64 Keynes, *A Tract on Monetary Reform*, 164.

zouden lagere prijzen in de landen met handelstekorten de producten van deze landen aantrekkelijker moeten maken voor export, wat zou moeten helpen om hun handelstekort te verminderen. Net als in een systeem met zwevende fiatvaluta zou de verandering in totale prijzen tussen landen moeten helpen om het handelsevenwicht tussen hen in balans te brengen.

Ook Hayek erkende dat een dergelijk handelsevenwicht onder de goudwisselstandaard behouden kon worden, net zoals onder de fiatgeldstandaard. Maar hij was het er niet mee eens dat dit een goede zaak was.

Monetair nationalisme

In 1937 nam Hayek zowel de goudwisselstandaard als het zwevende fiatgeldsysteem onder de loep in een reeks lezingen getiteld *Monetary Nationalism and International Stability*. De lezingen wezen de internationale valuta-afspraken door de stabilisatoren, die Hayek had bestempeld als monetair nationalisme, volledig af.

Hayek stelde dat, onder zowel de goudwisselstandaard als ook een zwevend valutasysteem, de bedrijven en individuen die profiteren van een exporttoename (of in tegendeel, die lijden onder een exportdaling) niet noodzakelijkerwijs dezelfde bedrijven of individuen zijn die verantwoordelijk zijn voor de toename (of afname) van handel met het buitenland.

'Als we kijken naar de methoden die voor banken beschikbaar zijn om de hoeveelheid krediet uit te breiden of te doen inkrimpen, is er geen reden om aan te nemen dat ze de exacte hoeveelheid geld dat vernietigd moet worden, kunnen halen bij die personen waar het tijdig vrijgegeven zou worden als er geen bankensysteem zou zijn, of dat ze het extra geld zullen overhandigen aan diegenen die het geld zouden ontvangen als het direct vanuit het buitenland naar het binnenland zou zijn gekomen', schreef Hayek.[65]

Specifiek zal de verandering in rentetarieven onder de goudwisselstandaard waarschijnlijk niet reflecteren wat het rentetarief in een vrije markt zou zijn. Dit zorgt voor winnaars en verliezers: schuldenaren profiteren van lagere rentetarie-

65 Friedrich A. Hayek, *Monetary Nationalism and International Stability*, in 'The Collected Works of F.A. Hayek, Good Money: part II', ed. Stephen Kresge: 55.

ven, terwijl schuldeisers eronder lijden. Er is echter geen reden om aan te nemen dat de handelaar die zijn export verhoogt een schuldenaar is. Hij zou net zo goed een schuldeiser kunnen zijn, in welk geval hij door zijn eigen toename in internationale verkopen indirect schade lijdt.

In plaats van alleen de twee handelspartijen te beïnvloeden die over grenzen heen zaken doen, zorgde internationale handel onder de goudwisselstandaard in wezen voor een herverdeling van middelen via de kredietmarkten, merkte Hayek op.

> *'Er zijn daarentegen sterke argumenten om aan te nemen dat de verandering in beide landen de investeringsactiviteit volledig, of tot een mate die totaal niet in verhouding staat tot de feitelijke veranderingen in de economische situatie, negatief zullen beïnvloeden.'*[66]

Op een soortgelijke manier worden hulpbronnen in een systeem van zwevende fiatvaluta ook verdeeld aan meer partijen dan enkel zij die direct betrokken zijn bij de stijging (of daling) van de export, legde Hayek uit.

Laten we even beredeneren waarom dit zo is. Stel dat er een verschuiving in de vraag plaatsvindt van de auto-industrie in de VS naar de auto-industrie in Engeland. Dit betekent dat Amerikanen dollars moeten wisselen voor ponden om een nieuwe auto te kopen, wat invloed heeft op de relatieve waardes van de dollar en de pond. Als gevolg hiervan worden *alle* producten uit de Verenigde Staten goedkoper vanuit het perspectief van Engeland, terwijl alle producten uit Engeland duurder worden vanuit het perspectief van de Verenigde Staten. Alle exporteurs in de Verenigde Staten zullen daarom profiteren van hogere verkoopcijfers ten koste van bedrijven in Engeland.

Hoewel in dit voorbeeld de initiële verschuiving in vraag enkel plaatsvond binnen de twee auto-industrieën, zullen Britten ook aangemoedigd worden om Amerikaans voedsel, kleding, of elektronica te kopen. Niet omdat deze producten daadwerkelijk beter of goedkoper te produceren zijn, maar puur door de werking van het systeem van zwevende fiatvaluta.

In beide vormen verstoorde het monetair nationalisme de spontane orde over grenzen heen, concludeerde Hayek.

---

66 Hayek, *Monetary Nationalism*, 55–56.

Neutraal geld

Hayek verwierp stabilisatiebeleid en ook monetair nationalisme. Hij pleitte daarom voor een homogeen, internationaal soort geld met een vaste hoeveelheid, wat hij *neutraal geld* noemde.

Hayek was resoluut tegen de aanname van stabilisatoren dat monetaire stabiliteit op nationaal niveau gemeten moest worden. Hij betoogde dat, indien geld net zo gemakkelijk van het ene naar het andere land kan bewegen als binnen regio's van hetzelfde land, een algehele prijsstijging binnen een land simpelweg een toename in vraag naar goederen en diensten uit dat land weerspiegelt. Dit zou juist aan de markt signaleren dat middelen het beste aan dat land kunnen worden toegewezen, zodat het meer goederen en diensten kan produceren.

Een homogeen geld zou eenvoudig functioneren in de internationale handel: de betaling zou effect hebben op de verzender en de ontvanger en niemand anders, ongeacht in welke landen zij wonen. Een grenzeloze valuta zou daarom het beste het interspatiële prijssysteem mogelijk maken, zo redeneerde de Oostenrijker, en mensen in staat stellen om prijzen over verschillende locaties te vergelijken.

Geld met een vaste geldhoeveelheid zou ook het intertemporele prijssysteem het beste faciliteren, omdat het mensen in staat stelt om prijzen op verschillende tijdstippen nauwkeurig te vergelijken:

'Alleen met een geldsysteem waarin elke verandering in de geldhoeveelheid uitgesloten is, zal het mogelijk zijn om een structuur van geldprijzen op opeenvolgende momenten in de tijd te bedenken die correspondeert met het systeem van intertemporeel evenwicht,' schreef Hayek.[67]

Misschien wel het allerbelangrijkste gevolg van een vaste geldhoeveelheid is dat veranderingen in de productiekosten door de tijd heen duidelijk weerspiegeld worden in overeenkomstige veranderingen in prijzen. Als alle andere factoren buiten beschouwing worden gelaten, zullen de prijzen dalen als de kosten voor de productie van goederen dalen. Een geleidelijke daling van de prijzen – deflatie – was volgens Hayek de natuurlijke uitkomst van elke gezonde economie.

Volgens hayek had zo'n homogeen geld met een vaste geldhoeveelheid maar één groot probleem: hij geloofde niet dat het kon worden gerealiseerd.

Ten eerste, zelfs als een dergelijke munt gecreëerd zou kunnen worden, zouden

67 Hayek, *Intertemporal Price Equilibrium*, 212.

mensen nog steeds kunnen kiezen om krediet en andere alternatieven te gebruiken in plaats van daadwerkelijk geld, wat neerkomt op een feitelijke vergroting van de geldhoeveelheid.

'Het is uiteraard onmogelijk om [de hoeveelheid ruilmiddelen voor altijd vast te stellen], gezien de altijd aanwezige mogelijkheid om een surrogaatgeld in plaats van echt geld te gebruiken', concludeerde de Oostenrijker droevig. 'De hoeveelheid van dat surrogaat kan niet nauw gekoppeld zijn aan dat van het echte geld, en het creëren ervan zal exact hetzelfde effect hebben als dat van elke andere uitbreiding van de geldhoeveelheid.'[68]

Maar nog belangrijker, Hayek was van mening dat een homogene valuta met een vaste geldhoeveelheid überhaupt niet kon worden aangenomen, omdat hij er niet van overtuigd was dat er ooit een enkele internationale autoriteit zal zijn die zal worden toevertrouwd om een dergelijke valuta uit te geven. Iets zo belangrijk als een wereldwijde monetaire standaard vereist de sterkste garantie dat het universeel aanvaardbaar en toegankelijk zal blijven, maar Hayek was ervan overtuigd dat er geen bekende instantie was die deze garantie zou kunnen bieden.

'[...] zolang er afzonderlijke soevereine staten zijn, zal er altijd de dreiging van oorlog opdoemen, of het risico van het instorten van de internationale monetaire regelingen om een andere reden.'[69]

Neutraal geld was onmogelijk omdat, op een zeer fundamenteel niveau, naties elkaar niet konden vertrouwen.

Valuta-oorlogen

Inderdaad, dit gebrek aan vertrouwen had tegen het einde van de jaren dertig ook bijgedragen aan de ineenstorting van de goudwisselstandaard.

Voor zijn eigen kritiek op de goudwisselstandaard, ging Hayek uit van een ideaal scenario, waarbij de deelnemende landen zich hielden aan de regels van het spel. Deze regels schreven voor wanneer en hoe de centrale banken hun rentetarieven dienden aan te passen. Echter, het was al duidelijk dat zelfs dit ideale

68 Hayek, *Intertemporal Price Equilibrium*, 217.

69 Hayek, *Monetary Nationalism*, 87.

scenario zich niet in de werkelijkheid had voltrokken, aangezien meerdere van de deelnemende landen in plaats daarvan betrokken waren bij opeenvolgende competitieve devaluaties, in wat soms omschreven wordt als een *valutaoorlog*.

Als een nationale munteenheid devalueert, worden goederen en diensten relatief goedkoop vanuit het perspectief van andere landen. Een daling van de munteenheid kan daardoor de export stimuleren en zo tenminste tijdelijk de nationale economie ten goede komen. Maar er is ook een keerzijde. Wanneer de internationale vraag verschuift naar het land dat zijn munteenheid heeft gedevalueerd, betekent dit ook dat de vraag verschuift, *weg* van andere landen. Hun economieën hebben hierdoor vaak te lijden.

De snelste manier voor deze andere landen om hun concurrentievermogen terug te krijgen, is door hun eigen valuta te devalueren. Dit zou de handelsbalansen moeten herstellen naar hun oorspronkelijke staat. Maar als gevolg hiervan zou al het geld, in al deze economieën, minder waard zijn dan voorheen. Dit treft vanzelfsprekend spaarders, schuldeisers en mensen met een vast inkomen. Als iedereen meedoet met een valutaoorlog, dan is er niemand die wint.

Dit weerhield landen er echter niet van om precies dat te doen. Nog voordat de goudwisselstandaard werd ingevoerd, was Duitsland deze reeks van devaluaties in 1921 al vrij spectaculair begonnen door zijn munteenheid te hyperinflateren, om hun herstelbetalingen voor de oorlog te kunnen betalen. Hayeks geboorteland Oostenrijk volgde al snel. Frankrijk was de volgende, hoewel (als een van de overwinnaars van de Eerste Wereldoorlog) niet in dezelfde extreme mate: het devalueerde de franc vlak voor de invoering van de nieuwe goudstandaard in 1925. Als reactie hierop schortte Engeland in 1931, slechts een paar jaar na invoering van de nieuwe internationale monetaire afspraken, de goudconvertibiliteit op om de pond te kunnen devalueren.

Als een van de weinige landen die tijdens de oorlog een beperkte vorm van goudconvertibiliteit had gehandhaafd, was de Verenigde Staten aanvankelijk terughoudend om een devaluatie van de munteenheid uit te voeren. Op dat moment was een *troy ounce* goud precies $ 20,67 waard, en de *Federal Reserve* was in de vroege jaren 1930 nog steeds verplicht om zich aan de gouddekkingsgraad van 40 procent te houden.

Maar deze dekkingsratio begon een belemmerende factor te vormen toen president Franklin Roosevelt de Keynesiaanse methoden toepaste in een poging om

de Amerikaanse economie uit de economische depressie te helpen. Uiteindelijk besloot hij die obstakels op een ongekende manier te verwijderen.

Via Executive Order 6102, goedgekeurd met warme steun van Keynes,[70] verbood FDR in 1933 resoluut 'het hamsteren van gouden munten, goudstaven en goudcertificaten binnen de continentale Verenigde Staten'.[71] Alle Amerikaanse burgers werden bevolen al het goud dat ze bezaten in te ruilen voor dollars bij hun lokale Federale Reserve lidbank tegen het vaste tarief van $ 20.67. Bij niet-naleving hing er een boete van $ 10.000 en een gevangenisstraf van maximaal tien jaar boven het hoofd.

Een paar maanden later devalueerde Roosevelt de dollar tot $ 35 per troy ounce, waardoor de gouddekkingsratio van de Federal Reserve in wezen met ongeveer 69 procent in één nacht toenam. Dit betekende een nieuwe klap voor de goudwisselstandaard.

Daarna was Europa weer aan de beurt, te beginnen met de Fransen die in 1936 hun munteenheid voor de tweede keer devalueerden. En toen in de volgende jaren meer landen het voorbeeld van Engeland volgden om goud volledig te laten vallen zodat ze hun munteenheden konden devalueren, werd de goudwisselstandaard volledig losgelaten, nauwelijks een decennium nadat deze was ingevoerd.[72]

De reeks van muntdevaluaties, gecombineerd met een diepe economische depressie, eiste haar tol, met name in de landen die de oorlog in 1918 hadden verloren. De vernietiging van spaargeld, wijdverspreide werkloosheid en een gebrek aan perspectief in grote delen van Europa resulteerde in veel onzekerheid, wanhoop en uiteindelijk, woede.

Het bood een vruchtbare voedingsbodem voor een nieuwe en bijzonder gewelddadige, nationalistische, racistische en autoritaire collectivistische ideologie. Het fascisme kreeg over het hele continent voet aan de grond.

---

70 Nicholas Wapshott, *Keynes & Hayek: The Clash That Defined Modern Economics*: 159.

71 Franklin D. Roosevelt, *Relating to the Hoarding, Export, and Earmarking of Gold Coin, Bullion, or Currency and to Transactions in Foreign Exchange*, 28 augustus 1993, beschikbaar via *The American Presidency Project*.

72 Joris Rickards, *Currency Wars: The Making of the Next Global Crisis*, 56–77.

Hoofdstuk 4

Cryptografie

Whitfield Diffie had altijd al een voorliefde voor codes. Al sinds zijn docent in het vijfde leerjaar hem substitutieversleuteling leerde (een basistechniek in de wiskundige tak van de cryptografie), was hij gefascineerd door deze methode van geheimhouding. Het feit dat tekstversleutelingsalgoritmen in die tijd – de jaren vijftig – de specialiteit van het leger, geheime agenten en spionnen waren, droeg alleen maar bij tot de mysterieuze aantrekkingskracht.[73]

De jonge Whitfield was al snel in de ban van elk cryptografieboek dat zijn vader, een universiteitsprofessor, in de bibliotheek van het *City College* in New York kon vinden. Hij stortte zich op werken zoals het boek *Cryptoanalysis* uit 1939 van Helen Forché Gaines, dat diverse methoden beschreef om berichten om te zetten in onleesbare versleutelde tekst, bij voorkeur zo dat alleen de beoogde ontvanger ze kon ontcijferen.

Met de zeer simpele *Caesar-cipher* (vermoedelijk gebruikt door Julius Caesar), kunnen berichten bijvoorbeeld in *ciphertext* worden omgezet door elke letter te vervangen door een andere letter. De coderingssleutel '+1' vervangt bijvoorbeeld elke letter door de volgende letter in het alfabet - 'a' wordt 'b', 'b' wordt 'c', enzovoort. Het woord 'Secret' verandert in 'Tfdsfu'. Om de versleutelde tekst te ontcijferen, wordt dezelfde coderingssleutel gebruikt, maar in omgekeerde volgorde: elke letter wordt vervangen door de vorige letter in het alfabet ('Tfdsfu'

73 Een groot deel van dit hoofdstuk is gebaseerd op Steven Levy's *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*.

wordt weer ‘Secret’).

Deze +1 coderingssleutel is natuurlijk niet erg sterk. Een tegenstander die vastbesloten is om de resulterende ciphertext te ontcijferen – een *cryptanalist* – zou het waarschijnlijk bij hun eerste poging raden. En zelfs al doen ze dat niet, zijn er toch een aantal patronen in een versleutelde tekst die gespecialiseerde codekrakers kunnen helpen te bepalen welke vervangende letters waarschijnlijk overeenkomen met welke originele letters. Vooral in langere teksten kunnen aanwijzingen worden gevonden in de frequentie van specifieke letters en de lengte van woorden, om maar een paar voorbeelden te noemen.

Moderne coderingssleutels gebruikten daarom veel geavanceerdere technieken, en gebruikten bijvoorbeeld enkele delen van een tekst om andere delen te versleutelen. Tegen het midden van de twintigste eeuw was encryptie, en het breken ervan, essentieel voor militaire operaties. Het werk werd uitgevoerd door toegewijde specialisten die het vakgebied verder hadden ontwikkeld tot het punt waarop ciphertext volledig willekeurig kon lijken. Zonder patronen om te analyseren, waren zelfs de beste cryptografen ter wereld niet in staat om de codes te breken.

Desalniettemin bleef het basisidee grotendeels onveranderd. Net als bij de Caesar-cipher waren de geheime sleutels altijd *symmetrisch*: de decoderingssleutel was dezelfde als de coderingssleutel, alleen in omgekeerde volgorde gebruikt. Om veilig te communiceren, moesten mensen eerst een sleutel met elkaar uitwisselen.

Een sleutel via een onbeveiligd communicatiekanaal delen, was echter geen optie. Als iemand meeluisterde en de sleutel kon onderscheppen, zouden ze alle daaropvolgende berichten die met die sleutel gecodeerd waren, kunnen ontcijferen. Hiermee zou dus het hele doel van het versleutelen van berichten teniet gedaan worden. De sleutels werden daarom meestal in persoon gedeeld. Beide partijen moesten eerst fysiek samenkomen voordat ze versleutelde berichten konden uitwisselen.

Dit was natuurlijk niet altijd gemakkelijk, of zelfs mogelijk. Grote afstanden of extreme situaties zoals oorlog konden het proces aanzienlijk bemoeilijken. Toch geloofden cryptografen, zoals Diffie in zijn beginjaren leerde, dat er geen andere manier was: men moest eerst sleutels persoonlijk uitwisselen.

MIT

Ongeveer tien jaar nadat hij voor het eerst met de methode van de substitutiecipher kennismaakte, begon Whitfield Diffie wiskunde te studeren aan de Massachusetts Institute of Technology. Dit viel ook samen met de komst van de allereerste computers op de universiteitscampus. Hoewel hij zichzelf toen, als jonge twintiger en als een naar eigen zeggen vredelievend persoon, meer als een pure wiskundige dan als een informaticus zag, besloot Diffie toch om te leren programmeren. Zo wilde hij zijn vaardigheden uitbreiden met meer praktische kennis.

Het zou goed uitpakken voor hem. In 1965 studeerde hij af aan de technische universtiteit, en accepteerde hij een baan bij Mitre, een defensiecontractant die slechts een paar jaren daarvoor van MIT's Lincoln Laboratory afgesplitst was. Zo kon hij tijdens de Vietnamoorlog aan de dienstplicht ontsnappen, terwijl het werk zelf ook niets met de oorlog te maken had. Diffie zou helpen bij de ontwikkeling van het computeralgebrasysteem Macsyma.

Diffie hoefde zelfs niet naar het kantoor van Mitre te komen. Hij kon werken vanuit het AI Lab van MIT, waar hij zich volledig verdiepte in de nieuwe hackercultuur en haar vrije en collaboratieve filosofie.

Toch week Diffie op sommige punten van de typische hackerethiek af. Hij was niet van mening dat onbeperkte vrijheid in alle computeromgevingen gewenst was en vond dat software in bepaalde contexten ook privacy moest bieden. Naarmate mensen, bedrijven en regeringen hun activiteiten naar het digitale domein gingen verplaatsen, zag hij in dat het belangrijk zou worden om gevoelige data, zoals persoonlijke gezondheidsgegevens, bedrijfsfinanciën of militaire geheimen, te beschermen.

Diffie nam het initiatief om een virtuele *kluis* te bouwen. Net zoals een fysieke kluis, moest de digitale variant eenvoudig te openen zijn door de legitieme eigenaar van de gegevens, maar de toegang voor alle anderen beperken. Hij geloofde dat sterke versleuteling dit type probleem kon oplossen.

Hoewel de hacker zijn jeugdpassie eigenlijk niet echt had behouden (hij geloofde dat alle relevante paden in het domein van cryptografie al waren verkend) hielp zijn baas bij het AI Lab, de wiskundige Roland Silver, hem weer op de been. En toen Diffie ontdekte dat er, sinds hij het als kind bestudeerde, significante

vooruitgang in het veld van cryptografie geboekt was, werd zijn interesse opnieuw aangewakkerd.

Maar Diffie leerde nu ook dat de werkelijke voorhoede van cryptografie waarschijnlijk achter gesloten deuren verborgen bleef. De *National Security Agency* (NSA), de Amerikaanse inlichtingendienst die destijds in het geheim werkte en officieel niet bestond, had al jaren de beste cryptografen van het land binnengehaald. Waarschijnlijk bleef elk echt baanbrekend onderzoek, en de superieure cryptografische technieken die daaruit voortkwamen, geclassificeerd.

Het idee dat de NSA belangrijke informatie voor het publiek kon achterhouden, zat helemaal niet lekker bij Diffie.

Stanford

Toen de hackercultuur zich voor het eerst buiten de campus van MIT begon te verspreiden, vond het al snel een thuis in de San Francisco Bay Area, op de Stanford University. En zo zou ook Diffie zijn weg daarheen vinden. Toen hij in 1969 vierentwintig werd en de leeftijdsgrens voor zijn dienstplicht naderde, ruilde de afgestudeerde van MIT Mitre in om voor het AI Lab van Stanford te werken. Hier vond hij nieuwe uitdagingen die bij zijn hernieuwde interesse in cryptografie pasten.

De eerste van deze uitdagingen werd geïnspireerd door John McCarthy. De mede-oprichter van het AI Lab van MIT en de originele ontwerper van de LISP-programmeertaal was verder gegaan met het oprichten van Stanfords AI Lab, en hij leidde het onderzoeksinstituut toen Diffie daar voor het eerst aankwam. Tegen die tijd had McCarthy een interesse ontwikkeld in de toekomst van digitale handel, wat op zijn beurt Diffie ertoe aanzette om te dromen van het geautomatiseerde kantoor, waar software wordt gebruikt om werkgerelateerde documenten digitaal te creëren, verzamelen, opslaan, bewerken en te verspreiden. Dit motiveerde hem om zich te richten op het vraagstuk rondom *authenticatie*.

In de fysieke wereld worden documenten doorgaans geverifieerd door middel van persoonlijke, geschreven handtekeningen. Mensen ondertekenen een brief om te bewijzen dat ze echt degenen zijn die hem geschreven hebben, of ze voegen hun handtekening toe aan een contract om het juridisch bindend te maken. Maar,

zo bedacht Diffie, naarmate documenten meer digitaal worden, zouden mensen een digitaal equivalent van een handtekening nodig hebben om te bewijzen dat zij echt degenen zijn die de inhoud van deze documenten goedkeurden.

Het creëren van een dergelijke vorm van digitale authenticatie was echter niet zo eenvoudig: Diffie en McCarthy brachten talloze uren door in het onderzoeksinstituut, peinzend over mogelijke oplossingen. Het hoofdprobleem was dat zelfs specifieke individuele gegevens, bijvoorbeeld een lang, persoonlijk nummer, makkelijk waren om te kopiëren. Iedereen kon zo'n digitale handtekening overnemen van één contract en toevoegen aan een ander contract. Dat zou ze nutteloos maken.

Een andere uitdaging ontstond in de schoot van het *Advanced Research Projects Agency* (ARPA) van het ministerie van Defensie, dat in 1972 was begonnen met het verbinden van grote onderzoeksinstellingen in het land door middel van een computernetwerk: ARPAnet. Als onderdeel van dit project, zocht Larry Roberts, de directeur van Information Processing Techniques bij ARPA, naar manieren om berichten over het netwerk privé te houden. Nadat de NSA hem elke hulp had geweigerd - het geheime overheidsagentschap weigerde aan een dergelijk openbaar project te werken - hoopte hij dat een van zijn belangrijkste onderzoekers misschien een idee had.

Toen McCarthy, een van de belangrijkste onderzoekers, het probleem besprak met de hackers in Stanfords AI Lab, erkende Diffie het belang van dit vraagstuk. Als in de toekomst de communicatie steeds meer elektronisch zou plaatsvinden (en dit was al meer en meer het geval) zou het persoonlijk delen van coderingssleutels waarschijnlijk onhaalbaar worden, waardoor privégesprekken onmogelijk zouden zijn. Tenzij mensen toegang zouden hebben tot hulpmiddelen om hun communicatie te beveiligen, vreesde Diffie dat iedereen op elk moment potentieel in de gaten kon worden gehouden. Een verontrustend toekomstbeeld.

Terwijl hij oplossingen probeerde te vinden voor deze uitdagingen, groeide Diffies hernieuwde interesse in cryptografie langzaam uit tot een obsessie. Zijn enthousiasme werd verder aangewakkerd door het lezen van *The Codebreakers*, een boek uit 1967 van David Kahn dat de gehele geschiedenis van cryptografie gedetailleerd beschrijft en deels gebaseerd is op informatie van twee NSA-overlopers die naar de Sovjet-Unie waren gevlucht. Hij was steeds meer vastberaden om de cryptografische technieken en inzichten te achterhalen die nog steeds door

inlichtingendiensten werden onderdrukt.

Dit was echter niet de enige reden waarom de hacker van het AI Lab uiteindelijk besloot om alles op alles te zetten.

Rondreis door Amerika

Toen Diffie in de zomer van 1973 een oude vriendin, de dierentrainster Marie Fischer uit Brooklyn, bezocht, had hij niet verwacht verliefd te worden. Maar toen dat gebeurde, veranderden zijn plannen drastisch. In plaats van terug te keren naar de Westkust, besloot hij om zijn baan in het AI Lab van Stanford op te zeggen en tijd met zijn nieuwe vriendin op de weg door te brengen. De twee begonnen aan een rondreis door het land in een oude Datsun 510.

Dit gaf Diffie toevallig ook de tijd en gelegenheid om zich echt te wijden aan het ontdekken van superieure cryptografische technieken. Levend van zijn spaargeld, nam hij Fischer mee op zijn zoektocht naar aanwijzingen. Ze bezochten David Kahn, de auteur van *The Codebreakers*, in Great Neck op Long Island, snuffelden in bibliotheken op zoek naar referentiewerken, en maakten afspraken met experts in de cryptografie uit zowel de academische wereld als het bedrijfsleven over heel de VS.

Diffie hoopte uiteindelijk een *formele logicatheorie* te ontwikkelen, een wiskundig systeem dat als basis zou dienen voor de cryptografie. Om dit te bereiken, geloofde hij dat hij bij de basis moest beginnen.

Het eenvoudigste cryptografische fenomeen dat hij kon vinden was de *eenrichtingsfunctie*: een vergelijking waarvan het eenvoudig is om de oplossing in één richting uit te rekenen, maar aanzienlijk moeilijker om in de omgekeerde richting te berekenen.

Een zeer simpele eenrichtingsfunctie — aangeduid als een *polynoom* — zou herkenbaar moeten zijn voor iedereen die algebra heeft gestudeerd op de middelbare school. Het zou er bijvoorbeeld uit kunnen zien als $x^2 - 5x + 8$. Als de invoer (x) in dit voorbeeld 16 is, is het vrij makkelijk te berekenen dat de vergelijking het resultaat 184 als uitkomst geeft. Echter, wanneer alleen de uitkomst van 184 bekend is, kan de vergelijking niet eenvoudig worden omgekeerd om te berekenen dat de oorspronkelijke invoer (x) 16 was. Een eenrichtingsfunctie is

het wiskundige equivalent van een eenrichtingsstraat.

Bovendien leerde Diffie het concept van een *valdeur* kennen, waarvan men aannam dat het een onderdeel kon zijn van sommige soorten eenrichtingsfuncties. Een valdeur was in feite een geheim stuk informatie, meestal een andere vergelijking, dat de omgekeerde berekening ook gemakkelijk zou maken. Als de vergelijking in het voorbeeld hierboven een valdeur bevatte, kon de uitkomst 184 worden gebruikt om de invoer 16 net zo gemakkelijk te berekenen als dat het oorspronkelijk was om 184 uit 16 te produceren. Als een eenrichtingsfunctie een eenrichtingsstraat is, dan is de valdeurfunctie een geheime tunnel in de tegenovergestelde richting.

Deze concepten fascineerden Diffie. Eenrichtingsfuncties en valdeuren leken intuïtief iets van grote waarde te zijn in het veld van de cryptografie, hoewel hij niet precies wist hoe ze gebruikt konden worden.

Via een gemeenschappelijke kennis leidde Diffies vermoeden hem uiteindelijk naar Martin Hellman, een dertigjarige assistent-professor aan Stanford. Hellman deelde zowel Diffies interesse in cryptografie als zijn ideologische overtuiging dat deze technologie veel breder beschikbaar moest zijn: hij had net een baan van de NSA afgewezen omdat hij wilde dat zijn werk de bevolking ten goede zou komen. En ook Hellman had nagedacht over hoe eenrichtingsfuncties breder toegepast konden worden in de cryptografie.

Toen Diffie en Hellman elkaar voor het eerst ontmoetten in 1974 en het idee bespraken in Hellmans kantoor aan Stanford, vonden ze niet meteen de oplossing waar ze naar op zoek waren. Maar in elkaar vonden ze iemand die geïnteresseerd was in hetzelfde probleem. Vanaf dat moment zouden ze hun denkvermogen bundelen door ideeën aan elkaar te toetsen en nieuwe inzichten te delen.

Toen Diffie na meer dan een jaar reizen besloot om zich te vestigen in de Bay Area, werden hij en Hellman goede vrienden en al snel collega's: Hellman nam Diffie aan als deeltijdse onderzoeker aan de universiteit.

Publieke-sleutelcryptografie

Op een doodgewone middag, toen Diffie op het huis van zijn voormalige werkgever John McCarthy pastte, viel het kwartje eindelijk.

Twee sleutels.

De oplossing was om *twee* sleutels te gebruiken.

Cryptografen hadden altijd als vanzelfsprekend beschouwd dat coderingssleutels geheim moesten blijven, omdat ze ook dienden als decoderingssleutels. Maar Diffie negeerde deze *vanzelfsprekende waarheid* en kwam met het idee van *sleutelparen*. In plaats van slechts één geheime sleutel, zou iedereen twee sleutels hebben, namelijk een geheime sleutel die daadwerkelijk geheim moest blijven, en een publieke sleutel die vrijuit gedeeld kon worden.

Diffie was van mening dat de sleutels wiskundig met elkaar verbonden moesten zijn, waarbij de publieke sleutel in essentie van de geheime sleutel afgeleid werd door middel van een soort eenrichtingsfunctie. Zijn visie was erop gericht dat een verzender – laten we haar 'Alice' noemen, zoals cryptografen graag doen – een bericht versleutelde met haar geheime sleutel, waarna de beoogde ontvanger, 'Bob', het zou kunnen ontcijferen met behulp van haar publieke sleutel.

Als Bob het bericht inderdaad kan ontcijferen met de publieke sleutel van Alice, bewijst dit dat het bericht specifiek met Alice's geheime sleutel werd versleuteld. Dit maakt in feite een vorm van authenticatie mogelijk, aangezien de versleutelde versie van een bericht als Alice's digitale handtekening zou dienen.

Deze digitale handtekeningen zouden zelfs krachtiger zijn dan geschreven handtekeningen, aangezien een cryptografische handtekening alleen geldig zou zijn in combinatie met het precieze stuk data dat werd ondertekend. Als een digitaal contract na ondertekening zou worden gewijzigd, zou de cryptografische handtekening niet meer overeenkomen. Op een bepaalde manier zouden zowel de handtekening als de data zelf onmogelijk na te maken zijn.

Bovendien zag Diffie in dat het omgekeerde ook kon werken. Alice zou een bericht naar Bob kunnen versleutelen met *Bobs* publieke sleutel, waarna Bob, en alleen Bob, het zou kunnen ontcijferen met zijn geheime sleutel. *Publieke-sleutelcryptografie* beloofde zowel digitale authenticatie als veilige communicatie te bieden!

Toen het concept die avond aan Hellman werd uitgelegd, was hij het ermee eens dat Diffie potentieel iets belangrijks had bedacht, ook al was het idee nog maar in de ontwerpfase en moest de exacte wiskunde nog worden uitgewerkt. In de weken die volgden, legde het duo de vroege wiskundige basis om het idee tastbaarder te maken.

Dit resulteerde in het eerste gezamenlijk geschreven artikel van Diffie en Hellman. *Multiuser Cryptographic Techniques*, dat in het voorjaar van 1976 werd gepubliceerd en kort daarna werd gepresenteerd op de National Computer Conference in New York. In het artikel gaven de twee onderzoekers toe dat er nog grote vragen onbeantwoord waren. Ze wisten nog niet precies hoe encryptie of decryptie zou werken, noch hoe een publieke sleutel zou worden afgeleid van een geheime sleutel.

'Op dit moment hebben we noch een bewijs dat er publieke sleutelsystemen bestaan, noch een demonstratiesysteem.', gaven Diffie en Hellman toe in hun paper[74]

Ze kondigden echter aan dat ze bezig waren met iets groots: ze presenteerden het idee van cryptografie met publieke sleutels.

Ralph Merkle

Het artikel was nauwelijks gepubliceerd toen Hellman een brief van een afgestudeerde student aan de Universiteit van Californië, Berkeley ontving.

De student had zelf ook een werkstuk geschreven, zo legde hij uit in zijn brief. 'De mensen met wie ik probeer te praten, begrijpen totaal niet wat er aan de hand is, of zien elke poging tot het vinden van een oplossing als onmogelijk', schreef hij. Zijn frustratie druipte van de pagina. Hij concludeerde: 'Ik zie een kans voor samenwerking en ben geïnteresseerd om die verder te verkennen.'[75]

Ondertekend: Ralph C. Merkle.

Hoewel Merkle zo'n zeven of acht jaar jonger was dan Diffie en Hellman, leek zijn verhaal niet zo verschillend van dat van hen. Hij was altijd goed geweest met cijfers, stond consequent aan de top van elke wiskunde klas, en had sinds de aanvang van zijn universiteitsloopbaan een bijzondere interesse ontwikkeld voor computers.

In zijn laatste semester als student maakte hij tijdens een cursus over computerbeveiliging kennis met het veld cryptografie. Maar toen de docent de cipher van Caeser en andere vormen van symmetrische versleuteling besprak,

74 Whitfield Diffie and Martin E. Hellman, *Multiuser Cryptographic Techniques*, AFIPS…: Proceedings of the June 7-10, 1976, national computer conference and exposition: 109–112.

75 Levy, Crypto, 76.

realiseerde hij zich meteen dat de noodzakelijke sleuteluitwisseling in persoon de toepasbaarheid ervan ernstig beperkte. Merkle geloofde dat in een wereld waarin steeds meer communicatie digitaal zou gaan verlopen, er dringend behoefte was aan een betere oplossing.

In plaats van het hele land door te reizen op zoek naar antwoorden, beperkte Merkle zijn zoektocht naar een oplossing tot zijn eigen creatieve geest. En uiteindelijk bedacht hij een plan dat, althans tot op zekere hoogte, het probleem zou kunnen oplossen.

Zo zou het werken:

Eerst maakt Alice een groot aantal cryptografische puzzels, misschien wel miljoenen of zelfs meer. De oplossing voor elke puzzel bestaat uit een uniek getal en een even unieke geheime sleutel. Alice zelf kent de oplossing voor elke puzzel al: ze weet welke getallen bij welke geheime sleutels horen. Maar elke individuele puzzel kan ook door iemand anders worden opgelost, mits een beetje rekenkracht.

Alice stuurt vervolgens alle puzzels naar Bob. Bob kiest op zijn beurt willekeurig een puzzel, en lost deze met een beetje rekenkracht op om het unieke nummer en de bijbehorende geheime sleutel te vinden. Daarna stuurt hij het nummer (maar niet de bijbehorende geheime sleutel) naar Alice terug.

Op basis van het unieke nummer dat Bob terugstuurt, weet Alice onmiddellijk welke geheime sleutel Bob daarbij heeft gevonden. Deze geheime sleutel is dan de coderingssleutel die ze met elkaar delen. Net als elke andere symmetrische coderingssleutel, wordt deze gebruikt om berichten tussen hen te coderen en te decoderen.

Een afluisteraar die alle puzzels van Alice naar Bob heeft gezien, en ook welk uniek nummer Bob naar Alice heeft teruggestuurd, zal nog steeds de bijbehorende geheime sleutel niet weten.

Om erachter te komen welke sleutel Alice en Bob hebben gekozen, moet een afluisteraar alle puzzels willekeurig oplossen (via *brute kracht*) om dat ene unieke nummer te vinden dat Bob terugstuurde, wat tevens de geheime sleutel zal onthullen. Dit is echter een intensief rekenkundig proces. Afhankelijk van de hoeveelheid puzzels die aanvankelijk gemaakt werden (en de moeilijkheidsgraad om elke puzzel op te lossen), zal het veel rekenkracht en tijd in beslag kunnen nemen.

Alice en Bob hebben daarom een asymmetrisch voordeel ten opzichte van

de afluisteraar. Ze hoefden nauwelijks berekeningen uit te voeren om het over een geheime sleutel eens te worden, terwijl de afluisteraar heel veel berekeningen moet uitvoeren om hun gesprek te decoderen.

Deze oplossing vereiste echter wel dat Alice en Bob veel data met elkaar deelden in de vorm van puzzels, en de veiligheid van de oplossing nam lineair toe met het totale aantal puzzels. Om het kraken van het systeem tien keer moeilijker te maken, moeten ze tien keer zoveel puzzels delen; om het systeem honderd keer moeilijker te kraken te maken, moeten ze honderd keer zoveel puzzels delen, enzovoort. In de praktijk impliceren de limieten in data en rekenkracht van normale gebruikers dat een goed gefinancierde aanvaller met een supercomputer berichten in veel gevallen binnen enkele dagen zou kunnen ontcijferen.

Desondanks had Merkle een oplossing bedacht die twee mensen de mogelijkheid bood om tamelijk privé te communiceren zonder dat ze elkaar vooraf persoonlijk hoefden te ontmoeten. Hoewel het niet perfect was, was hij van mening dat deze techniek voor sleuteluitwisseling zeker innovatief en potentieel nuttig was.

Merkle was echter niet in staat om iemand anders te overtuigen. Zijn idee ontving weinig lof aan de Universiteit van Berkeley, en zijn artikel werd afgewezen door *Communications of the ACM*, het prestigieuze blad van de *Association for Computing Machinery* (ACM). Het verzenden van geheime sleutels via een onveilig netwerk werd door de recensenten als onacceptabel beschouwd. Bovendien merkten zij op dat er geen eerdere literatuur bestond die sleuteluitwisseling had vastgesteld als een belangrijk probleem.

Omdat hij het potentieel ervan aan niemand om hem heen kon uitleggen, stond de teleurgestelde student op het punt om zijn idee helemaal los te laten, totdat hij een proefdruk van Diffie en Hellmans paper in handen kreeg. Merkle zag meteen dat het duo een soortgelijk probleem probeerde op te lossen. Het bood een vorm van bevestiging die hij wanhopig nodig had en hij besloot om contact op te nemen.

In tegenstelling tot Merkle's professor in Berkeley en de recensenten van het tijdschrift, bewonderden Diffie en Hellman de vindingrijkheid van het voorstel. Waar het idee van Diffie draaide om sleutelparen, zorgde Merkle's aanpak er op een slimme manier voor dat Alice en Bob overeen konden komen over een gedeelde sleutel op zo'n manier dat alleen zij (gemakkelijk) konden berekenen

wat deze sleutel is. Hoewel Diffie en Hellman uiteindelijk concludeerden dat het protocol niet robuust genoeg was voor wat ze probeerden te bereiken, daagde het puzzelprotocol hen uit om het probleem vanuit een nieuw oogpunt te bekijken.

Hellman besloot om Merkle een zomerstage aan te bieden, waarbij hij de student uit Berkeley bijstond in het herschrijven van zijn paper tot een versie die uiteindelijk geaccepteerd werd door het ACM-blad. En door te bewijzen dat hij een creatieve en scherpzinnige denker was, werd Merkle bovendien ook betrokken bij verdere discussies rondom publieke-sleutelcryptografie.

Toen waren er drie indviduen bezig met het probleem.

De doorbraak

Uiteindelijk was het Hellman die de puzzelstukjes op hun plek liet vallen.

Hoewel zijn oplossing niet aan alle vereisten voldeed waar hij en Diffie op mikten (want er was geen digitale authenticatie), bedacht Hellman wel een protocol dat twee partijen privé liet communiceren, zonder de noodzaak om persoonlijk op voorhand een coderingssleutel te delen. Vergelijkbaar met het puzzelprotocol van Merkle is het idee achter de Diffie-Hellman-sleuteluitwisseling (zoals deze oplossing bekend zou worden) dat Alice en Bob een gezamenlijk geheim kunnen afspreken: in essentie, een symmetrische coderingssleutel die alleen zij kennen.

Om dit gedeelde geheim te genereren, gebruiken Alice en Bob sleutelparen, zoals oorspronkelijk door Diffie werd geopperd. Hun geheime sleutels zijn in wezen gewoon zeer grote willekeurige getallen, die zelfs de snelste supercomputers binnen een miljoen jaar niet kunnen raden. Elke publieke sleutel kan vervolgens van een geheime sleutel afgeleid worden door middel van een eenrichtingsfunctie. Het berekenen van de publieke sleutel uit de geheime sleutel is gemakkelijk, terwijl het berekenen van de geheime sleutel uit de publieke sleutel in principe onmogelijk is.

Om het gedeelde geheim te produceren, vermenigvuldigen Alice en Bob elk hun eigen *geheime sleutel* met de *publieke* sleutel van de ander. Dit moet hen beiden hetzelfde resultaat geven: het gedeelde geheim.

Dit werkt omdat in beide gevallen het gedeelde geheim in essentie een

combinatie is van beide geheime sleutels die telkens *eenmaal* door een eenrichtingsfunctie zijn gehaald. Wanneer Alice haar geheime sleutel vermenigvuldigt met de publieke sleutel van Bob, is de eenrichtingsfunctie al *ingebed* in de publieke sleutel van Bob, en hetzelfde is waar als Bob zijn geheime sleutel vermenigvuldigt met de publieke sleutel van Alice. Hoewel Alice en Bob de wiskunde in een andere *volgorde* uitvoeren, moet de uitkomst hetzelfde zijn.

(Dit is, weliswaar enigzins vereenvoudigd, vergelijkbaar met hoe de uitkomst van 2 x (3 x 5) en 3 x (2 x 5) beide 30 zijn. In deze analogie is de 2 de geheime sleutel van Alice, de 3 is de geheime sleutel van Bob, x 5 is de eenrichtingsfunctie, en 30 is het gedeelde geheim.)

Tegelijk kan niemand anders het gedeelde geheim van Alice en Bob vinden. Immers, als de twee *publieke* sleutels worden vermenigvuldigd, is het resultaat in wezen een combinatie van beide geheime sleutels, maar dan *twee keer* door een eenrichtingsfunctie heen gegaan, en dus een keer te veel (als we de analogie voortzetten, is dit te vergelijken met (2 x 5) x (3 x 5), wat 150 is in plaats van 30).

Het genereren van het gedeelde geheim vereist dus toegang tot ofwel de geheime sleutel van Alice of van Bob. Zolang zij deze geheim houden, kunnen ze gebruik maken van door de wiskunde gegarandeerde privécommunicatie.

Het Diffie-Hellman-sleuteluitwisselingsprotocol doorbrak de status-quo in het veld van de cryptografie en was in staat om iets te realiseren dat lang onmogelijk werd geacht. Hun techniek had de potentie om het volledige onderzoeksgebied van de cryptografie dramatisch te transformeren. De twee onconventionele cryptografen waren zich hier maar al te goed van bewust toen ze hun tweede publicatie, *New Directions in Cryptography*, indienden bij *IEEE Transactions on Information Theory*, een prestigieus wetenschappelijk tijdschrift, uitgegeven door een professionele vereniging voor elektronische techniek.

'Vandaag staan we aan de vooravond van een revolutie in de cryptografie', kondigden Diffie en Hellmann aan in hun paper, gepubliceerd in de editie van november 1976 van het tijdschrift. In de overtuiging dat hun doorbraak het begin van een grote omwenteling zou markeren, vervolgden ze: 'theoretische ontwikkelingen in informatietheorie en informatica beloven aantoonbaar veilige cryptosystemen mogelijk te maken, waardoor deze eeuwenoude kunst verandert

in een wetenschap.'[76]

Het werd al snel duidelijk dat Diffie en Hellman een stroomversnelling hadden veroorzaakt. Een nieuwe generatie cryptografen stond op het punt om een waterval aan innovatie in de wereld van de cryptografie te introduceren.

RSA

Onder de eersten die geïnspireerd raakten door het paper van Diffie en Hellman waren drie jonge wiskundigen van het MIT. Niet alleen hielden ze allen van getallen, ze waren ook gedreven om lastige problemen op te lossen. Ron Rivest, een assistent-professor aan de universiteit, Adi Shamir, een gastprofessor, en Leonard Adleman, een computerspecialist aan hetzelfde instituut, begonnen samen aan het ontwerp van een eenrichtingsfunctie die specifiek voor publieke-sleutelcryptografie moest dienen.

Enkele maanden later, in 1977, was het ze gelukt.

RSA, zoals hun algoritme werd genoemd (elke letter vertegenwoordigt een van de uitvinders), benutte eeuwenoude wiskundige inzichten in priemfactoren (de vermenigvuldiging van priemgetallen) om een eenrichtingsfunctie met een ingebouwde valdeur te creëren. Door berekeningen te doen met een maximaal getal, zouden twee opeenvolgende, maar verschillende vermenigvuldigingen altijd het originele invoergetal teruggeven. In feite zou de eerste vermenigvuldiging de data versleutelen, terwijl de tweede het zou ontsleutelen.

Als een vereenvoudigde analogie, het is alsof je wiskunde toepast op een klok. Aangezien een klok maar tot twaalf telt, is het resultaat van tien plus vijf drie. Drie plus zeven, brengt ons vervolgens weer terug naar tien. In deze analogie is tien de oorspronkelijke data, het optellen van vijf staat voor het versleutelen, het aanvankelijke resultaat van drie is de versleutelde data, en wanneer er weer zeven wordt opgeteld vertegenwoordigt dit de functie van de valdeur, wat neerkomt op het ontcijferen (decrypten).

RSA maakte het versleutelen en ontsleutelen van berichten compatibel met het oorspronkelijke idee van Diffie. Als Alice naar Bob een versleuteld bericht wilde

76 Whitfield Diffie and Martin E. Hellman, *New Directions in Cryptography*, IEEE Transactions On Information Theory, vol. IT-22, no. 6: 644.

sturen, kon ze simpelweg het bericht versleutelen met Bobs publieke sleutel. Bob kon het bericht vervolgens ontcijferen met alleen zijn geheime sleutel. Bob had de publieke sleutel van Alice niet meer nodig, en beiden hadden geen gedeeld geheim meer nodig.

Misschien nog belangrijker: het algoritme werkte net zo goed in omgekeerde volgorde. Twee opeenvolgende vermenigvuldigingen leverden altijd het oorspronkelijke getal terug, ongeacht welke van de twee vermenigvuldigingen eerst werd uitgevoerd. Voortbordurend op de klok-analogie, waarbij tien plus vijf plus zeven ons terugbracht naar tien, brengt de omgekeerde volgorde (tien plus zeven plus vijf) ons ook terug naar tien.

In de praktijk betekende dit dat een geheime sleutel kon worden gebruikt om data te versleutelen, die vervolgens kon worden ontcijferd met de bijpassende publieke sleutel. Hierdoor maakte RSA een cryptografisch handtekeningenprotocol mogelijk: Alice kan een bericht versleutelen, dat Bob (of iemand anders) kan ontcijferen met haar publieke sleutel, wat bewijst dat het bericht daadwerkelijk is versleuteld met Alice's geheime sleutel.

Terwijl de Diffie-Hellman-sleuteluitwisseling privécommunicatie mogelijk maakte, faciliteerde RSA voor het eerst ook een vorm van digitale authenticatie.

En tot slot, RSA-encryptie schaalde (ongeveer) exponentieel. Gewoon een paar cijfers toevoegen aan de originele priemgetallen die in dit protocol werden gebruikt, zou het veel moeilijker maken om later te ontdekken welke priemgetallen werden gebruikt, en daarmee ook veel moeilijker om de encryptie te breken. Met publieke sleutels die zo klein zijn dat zelfs informele computergebruikers ze gemakkelijk konden delen, was beveiliging voor miljoenen jaren wiskundig gegarandeerd.

Met RSA was Diffies visie voor publieke-sleutelcryptografie echt werkelijkheid geworden.

David Chaum

Een andere jonge cryptograaf die geïnspireerd werd door de doorbraak van Diffie en Hellman was David Chaum.

Chaum groeide op in de buitenwijken van Los Angeles in de jaren 60 en

begin jaren 70, waar hij al op jonge leeftijd een natuurlijke interesse voor beveiligingstechnologie ontwikkelde. Aanvankelijk ging zijn belangstelling uit naar hardware, zoals deursloten, inbraakalarmen en fysieke kluizen. Aan het einde van zijn jeugdjaren resulteerde dit in het ontwerpen van een nieuw type slot. Chaum stond zelfs op het punt zijn ontwerp aan een grote fabrikant te verkopen.

Maar tegen die tijd begon tevens zijn interesse in het relatief nieuwe gebied van de informatietechnologie te groeien. Hij wisselde regelmatig van universiteit. Zijn studie begon aan de University of California, Los Angeles nog voordat hij de middelbare school had afgerond. Hij schakelde daarna over naar de University of Sonora in Mexico om dicht bij zijn vriendin van dat moment te zijn, en studeerde uiteindelijk af aan de University of California, San Diego. Chaum studeerde informatica en wiskunde, en tegen de late jaren '70 leerde hij over cryptografie en de recente doorbraken in dat onderzoeksgebied.

Chaum zag natuurlijk ook de potentie van de publieke-sleutelcryptografie omdat hij eveneens glimpsen van de toekomst had opgevangen. Hij voorzag dat computers steeds gebruikelijker zouden worden, totdat uiteindelijk elk huishouden er een in huis zou hebben. En terwijl ARPAnet langzaam begon te transformeren naar het (meer algemeen toegankelijke) vroege internet, verwachtte hij dat elektronische communicatie de wereld zou transformeren.

Net zoals Diffie dat voor hem deed, herkende Chaum ook dat deze transformatie naar een tamelijk dystopische toekomst kon leiden. Hij begreep dat als berichten, documenten of bestanden over het internet zouden worden verzonden, al deze data het risico liep om op een nooit eerder geziene schaal door tirannen te worden gemonitord, onderschept en geëxploiteerd. Chaum maakte zich zorgen dat mensen zich anders zouden gaan gedragen als ze geloven dat ze mogelijk bekeken zouden worden. Massasurveillance zou een gevangenis voor de geest creëren, conformiteit bevorderen, en uiteindelijk fundamentele vrijheden vernietigen, aldus Chaum.

'De cyberruimte kent niet dezelfde fysieke beperkingen', legde Chaum later uit aan een journalist van het technologiemagazine *Wired*. 'Er zijn geen muren… het is een andere, angstaanjagende, vreemde plek en met identificatie wordt het een nachtmerrie van panoptisch toezicht. Juist? Alles wat je doet kan door iedereen gekend zijn, kan voor altijd worden opgenomen. Het druist volledig in tegen het

basisprincipe waarop de mechanismen van de democratie zijn gebaseerd'[77]

Maar hij zag dat er nu een alternatief was: een andere mogelijke toekomst. Chaum besefte dat de gloednieuwe ontwikkelingen in de cryptografie konden worden ingezet ter verdediging. De maatschappij stond op een kruispunt, en innovaties zoals publieke-sleutelcryptografie boden hoop op een wereld waarin mensen de macht hebben over hun eigen data.

Gedeeltelijk omdat hij wist dat Ralph Merkle naar Berkeley was gegaan (maar niet op de hoogte was dat Merkle's initiële puzzelprotocol daar niet bepaald goed was ontvangen), koos Chaum voor de universiteit in de Bay Area om zijn doctoraat te behalen. Hier was hij van dichtbij getuige van hoe cryptografie tegen het einde van dat decennium evolueerde van een niche interesse, uitsluitend voor kleine universiteitsafdelingen en academische tijdschriften, naar een kleine revolutie in de informatica, aangedreven door een toegewijde en groeiende gemeenschap van gelijkgestemde wiskundigen.

Het resulteerde in de allereerste *Crypto*-conferentie in 1981, georganiseerd aan de Universiteit van Californië, Santa Barbara. De grootste vernieuwers in het gebied – Diffie, Hellman, Merkle, Rivest, Shamir, Adelman – en ongeveer vijftig andere cryptografen waren aanwezig, met velen die elkaar voor het eerst in persoon ontmoetten. Ze presenteerden hun nieuwste documenten, bespraken mogelijke verbeteringen aan bestaande protocollen, of leerden elkaar gewoon wat beter kennen terwijl ze een avond doorbrachten met een barbecue op het strand.

Echter, dit gebeurde allemaal tot grote ontsteltenis van de NSA. Net als de nieuwe lichting cryptografen die samengekomen waren bij Crypto 1981, herkende ook de overheidsorganisatie de potentie van publieke-sleutelcryptografie. Maar in tegenstelling tot het optimisme en de vreugde van op de conferentie, waren mensen binnen de inlichtingengemeenschap bezorgd dat sterke encryptie hun hele werkwijze in gevaar zou kunnen brengen. Ze wilden deze cryptografische revolutie stoppen voordat het te ver zou gaan, en in de nasleep van de conferentie begon de NSA waarschuwingen te geven aan wetenschappelijke organisaties om geen presentaties te faciliteren, zoals die tijdens Crypto 1981 zo openlijk tentoongesteld werden.

Toen hij hiervan hoorde, besloot Chaum terug te vechten. Hij ondernam actie

77 Steven Levy, *E-Money*, Wired, 1 december 1994, online

om ervoor te zorgen dat de conferentie geen eenmalig evenement zou blijven. Uitgerust met een lijst van namen en contactinformatie die door Adleman was verstrekt, begon de promovendus contact op te nemen met alle grote namen in de cryptografie. Om geen aandacht te trekken van de NSA, stuurde hij fysieke brieven of ontmoette hij de mensen persoonlijk, maar vermeed telefoongesprekken over het onderwerp. Uiteindelijk wist Chaum iedereen terug samen te brengen in Santa Barbara op Crypto 1982, terwijl hij ook een Europese conventie (*Eurocrypt*) in Duitsland organiseerde in datzelfde jaar.

Daarnaast richtte Chaum de *International Association for Cryptologic Research* op, een non-profit organisatie die belast werd met het bevorderen van onderzoek in de cryptografie. Hij kondigde de oprichting van deze organisatie aan tijdens de Crypto conferentie van 1982, wat opnieuw voor veel irritatie zorgde bij de NSA.

De grootste bijdragen van Chaum aan de cryptografie waren echter niet de evenementen die hij organiseerde of de organisatie die hij oprichtte, maar de technieken die hij ontwikkelde.

Remailers

Publieke-sleutelcryptografie maakte het mogelijk voor twee mensen die elkaar nog nooit hadden ontmoet om berichten uit te wisselen die alleen zij konden lezen. Dit bood privacy in communicatie — een baanbrekende ontwikkeling.

Maar het was geen wondermiddel, besefte Chaum. Zelfs met de publieke-sleutelcryptografie, bleef een aanzienlijk privacy-risico bestaan: verkeersanalyse kon onthullen wie met wie praatte, en wanneer.

Dergelijke *metadata* kan meer over iemand onthullen dan men zou willen. Een onderzoeksjournalist wil misschien niet dat zijn bronnen bekend worden, bijvoorbeeld. Of burgers uit landen met autoritaire regimes willen misschien niet dat iemand weet dat ze communiceren met een politieke dissident. Ook zal een werknemer die naar vacatures bij een concurrerend bedrijf informeert er waarschijnlijk de voorkeur aan geven dat zijn baas niet ontdekt dat hij contact heeft gehad met dat bedrijf.

In zijn paper uit 1981 getiteld *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, stelde Chaum een oplossing voor dit probleem voor, eveneens

gebaseerd op publieke-sleutelcryptografie.[78]

Dit is hoe het werkt.

Als Alice een bericht aan Bob wil sturen, moet ze eerst zijn publieke sleutel nemen en het bericht daarmee versleutelen. Op deze manier kan alleen Bob het bericht ontcijferen.

Maar ze stuurt het bericht niet rechtstreeks naar Bob: een afluisteraar die hun verbindingen monitort, zou dan kunnen zien dat de twee communiceren, wat Alice juist probeert te vermijden.

In plaats daarvan neemt Alice het versleutelde bericht en voegt daar het e-mailadres van Bob aan toe. Vervolgens versleutelt ze dit hele pakket (het versleutelde bericht voor Bob en zijn e-mailadres) nog een keer, maar nu met de publieke sleutel van een speciale mixserver. Het bericht heeft nu twee lagen van codering: één laag voor het originele bericht en een andere laag voor het hele pakket. Alice stuurt dit dubbel versleutelde pakket dan naar de mixer.

Om het originele gecodeerde bericht en Bobs e-mailadres te vinden, ontcijfert de mixserver op zijn beurt het pakket met zijn geheime sleutel. De mixer gebruikt dit om het gecodeerde bericht naar Bob te sturen, die het vervolgens ontcijfert om Alice's originele bericht te lezen. Als tussenpersoon brak de mixer de directe link tussen Alice en Bob, waardoor het voor de afluisteraar moeilijker werd om te achterhalen dat ze communiceerden. Tenzij het duidelijk is uit de inhoud van het bericht, weet Bob zelf ook niet dat het van Alice afkomstig was.

Deze basisopzet functioneert zolang je op de mixer kan rekenen en zolang deze niet aan de gluurder (of aan Bob) onthult dat hij het versleutelde pakket eerst van Alice heeft ontvangen. Maar Chaum maakte duidelijk dat het zelfs niet nodig is om de mixer te vertrouwen.

Om het risico van een onbetrouwbare mixer te verminderen, kan Alice meerdere mixers gebruiken. In dat geval zou Alice een gecodeerd pakket naar mixer 1 sturen, dat mixer 1 kan ontcijferen om het e-mailadres van mixer 2 en een ander gecodeerd bericht te vinden. Dit bericht kan mixer 2 vervolgens ontcijferen om het e-mailadres van mixer 3 te vinden en nog een ander gecodeerd bericht. Dit bericht kan mixer 3 dan ontcijferen om inderdaad het e-mailadres van Bob en nog

78 David Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, Communications of the ACM 24, 2: 84–90.

een gecodeerd bericht te vinden. Dit laatste bericht kan Bob ten slotte ontcijferen om het originele bericht te lezen. Door elk één laag van de encryptie te verwijderen en het pakket naar de volgende ontvanger door te sturen, zouden de mixers weten van wie ze het pakket hebben ontvangen en naar wie ze het hebben doorgestuurd, maar geen van hen zou weten waar het pakket oorspronkelijk vandaan kwam en wie de eindontvanger is.

Een afluisteraar die Bobs communicatie probeert te monitoren, zou mogelijk kunnen weten dat mixer 3 uiteindelijk het bericht naar Bob stuurde, maar zelfs als mixer 3 deze informatie met de indringer deelt op verzoek (of gerechtelijk bevel), helpt dit de indringer slechts één stap vooruit. Als er ook maar één van de mixers weigert mee te werken, stopt het spoor (en als de mixers in verschillende rechtsgebieden verblijven, kunnen zelfs handhavingsautoriteiten uit een bepaald land het moeilijk hebben om de oorsprong van een bericht na te gaan).

Zo had Chaum het cruciale conceptuele fundament gelegd voor wat later bekend zou worden als *remailers*.

En zijn bijdragen aan de cryptografie zouden daar niet ophouden…

Hoofdstuk 5

Denationalisatie van geld

Economische depressie en valutadevaluaties hadden geleid tot fascisme en, uiteindelijk naar de Tweede Wereldoorlog.

Maar Friedrich Hayek merkte met spijt op dat veel van zijn collega's in de academische wereld destijds niet opmerkten welke schade het monetair beleid had aangericht. In plaats daarvan schreven vele intellectuelen van die tijd de opkomst van het fascisme toe aan het falen van de vrije markten. Economen, politicologen en andere academici in het Westen overwogen alternatieve manieren om de samenleving te organiseren, en socialistische ideeën werden steeds populairder, een ontwikkeling die Hayek ronduit gevaarlijk vond.

Om deze trend tegen te gaan, nam de Oostenrijker het op zich om uit te leggen waarom socialisme niet het antwoord was, maar deel uitmaakte van het probleem. Het resulterende boek, *De Weg naar Slavernij*, nam een meer politieke benadering, hoewel het sterk werd ondersteund met economische inzichten zoals het economisch calculatieprobleem. Geschreven en gepubliceerd tijdens de oorlogsjaren, was de kernthese dat collectivistische ideologieën, inclusief zowel fascisme als socialisme, de neiging hebben om te leiden tot totalitarisme. Het zou het meest succesvolle boek van Hayeks carrière worden.

Het was wellicht een geschikt moment voor Hayek om zijn aandacht en energie te verschuiven van de economie naar de politieke sfeer. Na twee decennia van debatten en rivaliteit, werd het duidelijk dat niet zijn, maar de ideeën van Keynes over het monetaire beleid mensen en instituten binnen universiteiten, beleidsin-

stellingen en overheidsinstellingen voor zich wonnen. Als de vrijemarktideologie al zou overleven, zou het waarschijnlijk gebaseerd zijn op de Keynesiaanse doctrine.

Dit werd bevestigd toen vertegenwoordigers van de geallieerde landen, vol vertrouwen in hun overwinning in de oorlog, in 1944 bijeenkwamen in het Mount Washington Hotel in Bretton Woods, New Hampshire. De deelnemers waren er om een nieuw monetair systeem te ontwerpen voor de periode na de oorlog en Keynes was uitgenodigd om het Verenigd Koninkrijk te vertegenwoordigen. Hayek, die tegen die tijd ook de Britse nationaliteit had gekregen, werd helemaal niet uitgenodigd.

Het belangrijkste resultaat van de Bretton Woods-conferentie kan worden beschouwd als een herinvoering van de goudwisselstandaard, maar in tegenstelling tot de vooroorlogse klassieke goudstandaard was deze sterk gericht op de Amerikaanse dollar. Internationale handel zou in dollars worden uitgevoerd, terwijl deze dollars op hun beurt konden worden ingewisseld voor goud: één troy ounce per $ 35. Andere nationale valuta zouden vaste wisselkoersen vaststellen ten opzichte van de dollar, en centrale banken werden verwacht de rentetarieven te sturen om hun nationale valuta te stabiliseren.

Bretton Woods was ook de geboorteplaats van twee nieuwe internationale monetaire instellingen, met Keynes als drijvende kracht achter hun oprichting. De eerste hiervan, het Internationaal Monetair Fonds (IMF), kreeg de taak om toezicht te houden op internationale wisselkoersen en kon geld lenen aan landen in financiële problemen. Het tweede, de Wereldbank, zou ook leningen verstrekken, maar met een sterkere focus op het heropbouwen van het naoorlogse Europa (en later andere ontwikkelingslanden).

Het *Bretton Woods-systeem*, zoals het later genoemd werd, werd kort na de nederlaag van de Asmogendheden in 1945 uitgerold, maar dan alleen in het Westen. Hoewel de Sovjet-Unie vertegenwoordigers naar Bretton Woods had gestuurd, weigerde deze communistische staat uiteindelijk om de overeenkomst te ratificeren. Ze beschuldigden het IMF en de Wereldbank 'takken van Wall Street'[79] te zijn. In plaats daarvan nam het vele Oost-Europese landen over na de

79 Edward S. Mason and Robert E. Asher, *The World Bank Since Bretton Woods: The Origins, Policies, Operations and Impact of the International Bank for Reconstruction*, 29.

oorlog. Het markeerde het begin van de Koude Oorlog, waarin (een Keynesiaanse variant van) vrijemarktkapitalisme in de Verenigde Staten en West-Europa op vele manieren zou concurreren met de socialistische doctrine in het Oosten.

Keynes was er echter niet om de effecten van het Bretton Woods-systeem en de instellingen van deze nieuwe monetaire orde te bestuderen. De econoom overleed kort na de oorlog, in 1946.

Hoewel Hayek zijn rivaal had overleefd, erkende hij dat de ideeën van Keynes de voorkeur genoten boven de zijne. Hij had niet het gevoel dat de nieuwe generatie Keynesiaanse economen echt geïnteresseerd was in een eerlijk en zinvol debat. De Oostenrijker besloot de London School of Economics te verlaten en zich aan te sluiten bij de Universiteit van Chicago. Daar trok hij zich grotendeels terug uit het vakgebied economie en verschoof zijn focus naar de wereld van de politiek en de filosofie.

Het tijdperk van Keynes

Halverwege de twintigste eeuw was *het tijdperk van Keynes* onmiskenbaar aangebroken in het kapitalistische Westen. Overheden, centrale banken en andere instellingen bepaalden het economische beleid en economen trachtten het theoretische raamwerk achter fiscale planning, stabilisatiebeleid en monetaire stimuli verder uit te werken. Zo introduceerde bijvoorbeeld Professor William Phillips van de London School of Economics de Phillips-curve, die aangaf dat er een omgekeerd verband was tussen inflatie en werkloosheid. Dit was precies zoals de Keynesiaanse theorie suggereerde: meer overheidsuitgaven resulteerden in meer banen.

Politici kregen de theoretische rechtvaardiging om met overheidsuitgaven een economische neergang te bestrijden. Dit leek een tijdje de oplossing voor alles, aangezien Keynesiaanse beleidslijnen overal in de westerse wereld werden uitgerold. In het Verenigd Koninkrijk had premier Winston Churchill in 1944 volledige werkgelegenheid tot een nationaal beleidsdoel verheven. In de Verenigde Staten ondertekende Franklin D. Roosevelt's opvolger, president Harry S. Truman, in 1946 de Employment Act, waardoor de uitvoerende tak van de regering verantwoordelijk werd voor het beheer van de economie. En in Europa had het naoorlogse herstelprogramma, informeel bekend als het Marshallplan,

het hele westelijke deel van het continent omgevormd tot een soort Keynesiaans laboratorium.

Iets later in de Verenigde Staten was Truman's opvolger Dwight D. Eisenhower de eerste president die het Keynesiaanse economiebeleid echt ten volle toepaste. Toen de VS in het midden van de jaren '50 werd geconfronteerd met enkele korte recessies, bestreed de president de werkloosheid met grote investeringen in de snelwegeninfrastructuur. En nadat de Sovjet-Unie erin slaagde de Spoetnik-satelliet in een baan om de aarde te brengen, volgde Eisenhower dit op met aanzienlijke financiële injecties in het ruimtevaartprogramma van NASA. Het leek te werken zoals bedoeld: de Amerikaanse economie bloeide op.

Toen Eisenhower tegen het einde van zijn presidentstermijn echter de uitgaven moest beperken, resulteerde dit vrijwel onmiddellijk in een nieuwe depressie. Het Amerikaanse volk was hier niet blij mee. Ze waren van mening dat Eisenhower alle middelen voorhanden had om deze trend te keren, maar dat hij deze keer naliet om in te grijpen.

Tegen de tijd dat de verkiezingen voor de opvolger van Eisenhower er aankwamen, was de economische neergang een groot thema geworden in de presidentiële campagnes. Terwijl de jonge Democratische kandidaat John F. Kennedy zijn aanhangers mobiliseerde onder het motto 'Laten we dit land weer in beweging krijgen', worstelde de Republikeinse kandidaat en zittend vicepresident Richard Nixon om zich te distantiëren van Eisenhower's conservatieve fiscale benadering aan het einde van zijn tweede termijn. Toen Kennedy uiteindelijk met een ongelooflijk kleine marge de race won, bleef een verslagen Nixon ervan overtuigd dat hij de verkiezingen zou hebben gewonnen als de bezuinigingen van Eisenhower niet in de weg hadden gestaan.[80]

Gedurende zijn presidentschap bevestigde Kennedy dat hij royaal zou investeren in de economie op basis van Keynesiaanse principes. Hij blies Eisenhower's initiële uitgavendrift snel nieuw leven in, door geld te pompen in het Amerikaanse ruimtevaartprogramma, terwijl hij ook rijkelijk uitgaf aan het leger. Na de moord op de president slechts enkele jaren later, in 1963, zette zijn vicepresident en opvolger Lyndon B. Johnson dit beleid voort, met de Vietnamoorlog als grote,

80 Andrew F. Brimmer, *Remembering William McChesney Martin Jr.*, Federal Reserve Bank of Minneapolis, 1 september 1998, online

nieuwe geldverslindende factor.

In 1968, aan het eind van Johnson's presidentschap, was Nixon klaar voor een nieuwe gooi naar het ambt. En deze keer won hij. Toen hij het roer van Johnson overnam, leek Nixon, in zijn hart conservatief op fiscaal vlak, aanvankelijk bereid en gretig om een einde te maken aan deze Keynesiaanse vrijgevigheid. Hij wees er op dat de regering jarenlang tientallen miljarden dollars meer had uitgegeven dan het aan belastingen ontving.

Toen de bezuinigingen van Nixon echter onmiddellijk resulteerden in een milde economische recessie, besloot de president alsnog mee te spelen met het spel. Hij verklaarde zichzelf een Keynesiaan, kondigde een plan voor volledige werkgelegenheid aan en stelde een expansieve begroting voor om de economie te stimuleren. Nixon had een waardevolle les geleerd tijdens zijn mislukte poging om een decennium eerder president te worden, en was klaar om de nieuwe politieke werkelijkheid te accepteren.[81]

Zoals de president verklaarde in de State of the Union van 1970:

'Ik erken de politieke populariteit van uitgavenprogramma's, en zeker in een verkiezingsjaar.'[82]

De Keynesiaanse leer stelde eigenlijk zowel overheidsuitgaven als bezuinigingen als vereiste: uitgaven om de economie een impuls te geven, en bezuinigingen wanneer dit niet langer noodzakelijk was, om ongecontroleerde inflatie te voorkomen. Het probleem was echter dat het nu duidelijk werd dat hoewel verhoogde uitgaven verkiezingen konden winnen, bezuinigingen dat niet deden. Nixon had op de harde manier geleerd dat het beter was om vast te houden aan het populairdere stadium van de Keynesiaanse cyclus van uitgaven, en gemakshalve dat deel van de leer te negeren dat voorschreef wanneer bezuinigingen nodig waren.

Dit probleem was natuurlijk voorzien. Hayek heeft altijd beweerd dat de grootste nalatigheid van Keynes wellicht niet op economisch gebied lag, maar op politiek gebied: het was over het algemeen niet zo dat je van verkozen

81 Wapshott, *Keynes & Hayek*, 242.

82 Wapshott, *Keynes & Hayek*, 242.

vertegenwoordigers kon verwachten dat ze de discipline zouden volhouden die een *anti-cyclische* aanpak vereist.

De Nixon-schok

De overdadige uitgavendrift van Nixon en een aantal van zijn voorgangers kon in zekere zin worden verklaard als een uitvoering van de Keynesiaanse doctrine. Maar tegen de jaren '70 werden sommige van de grootste dollar-bezitters wantrouwend. Het werd steeds duidelijker dat de Verenigde Staten boven hun stand leefden en veel meer geld drukten en uitgaven dan ze in goud konden verantwoorden.

Sommige landen met grote dollarreserves besloten uiteindelijk om hun papieren geld geleidelijk aan af te bouwen. Ze wilden dollars omzetten in goud, wat makkelijker gezegd dan gedaan was, aangezien het verplaatsen en opslaan van grote hoeveelheden goud een ernstige logistieke uitdaging vormde. De Franse president Georges Pompidou stuurde uiteindelijk een compleet oorlogsschip naar New York om het goud van zijn land op te halen bij de plaatselijke Federal Reserve Bank. Er waren sterke aanwijzingen dat de Britten hetzelfde plan hadden.

Tot Nixon er op 15 augustus 1971 een einde aan maakte.

Tegenwoordig bekend als de *Nixon-schok*, kondigde de president in een televisietoespraak aan dat de *opschorting* van de omwisselbaarheid van dollars naar goud 'in het belang van monetaire stabiliteit, en in het beste belang van de Verenigde Staten' was.[83] Zonder voorafgaande waarschuwing zorgde Nixon met een Executive order er eigenhandig voor dat er een bom terechtkwam onder het Bretton Woods-systeem: landen die dollars hielden als onderdeel van hun reserves konden het papieren geld niet langer omzetten in edelmetaal.

Omdat de dollar de enige munteenheid was die onder het Bretton Woods-systeem omwisselbaar was naar goud, betekende dit onmiddellijk het einde van de goudstandaard. Wat overbleef waren nationale, ongedekte valuta, oftewel fiatvaluta. Toen kort daarna zes Europese landen ermee instemden om de waarde van hun munteenheden aan elkaar te koppelen en ze te laten fluctueren tegenover

83 Richard Nixon, *Address to the Nation Outlining a New Economic Policy: 'The Challenge of Peace'*, 15 augustus 1971.

de dollar, werd het Bretton Woods-systeem effectief volledig verlaten.[84]

Ondertussen had Nixon in de verkiezingsperiode van 1972 het voornemen om de economie te laten opbloeien. Volgens hem kon hij dit realiseren door de Federal Reserve ertoe aan te zetten de rente te verlagen. Goedkoop geld zou leiden tot inflatie en dat zou op zijn beurt weer leiden tot minder werkloosheid, zoals de Phillips-curve aangaf. Nixon wees zijn economische raadgever Arthur Burns aan als voorzitter van de Federal Reserve. Aangezien de eerdere beperkingen opgelegd door de gouddekkingsratio nu waren opgeheven, oefende hij onmiddellijk druk uit op de nieuwe voorzitter.

Nixon kreeg zijn zin. Hij won de herverkiezing. En tegen 1973 waren de officiële inflatiecijfers, gebaseerd op de consumentenprijsindex (CPI), gestegen naar 9,6 procent, om vervolgens in de daaropvolgende jaren te stijgen naar dubbele cijfers.[85]

Inflatie

Hayek beweerde dat kunstmatig lage rentes zouden leiden tot een economische groei die niet vol te houden was, gevolgd door een pijnlijke correctie, waarbij de markt het best met rust kon worden gelaten om een natuurlijker evenwicht te vinden. Keynesianen daarentegen adviseerden dat de overheid met extra uitgaven zou moeten ingrijpen om de economie weer op het juiste spoor te krijgen na zo'n recessie.

Hayek erkende altijd dat dergelijke Keynesiaanse overheidsuitgaven op de korte termijn inderdaad kunnen werken. Als de overheid nieuw geld in de economie pompt, zou het kunnen lijken alsof de economie redelijk stabiel blijft. Maar onder die façade van aanhoudende welvaart, waarschuwde Hayek, zou een donkerdere economische realiteit schuilgaan: het creëren van geld was slechts een verlenging van de verkeerde toewijzing van middelen die door de initiële verstoring werd veroorzaakt.

Dit was misschien wel Hayeks grootste bezwaar tegen deze vorm van inflatie:

84 Michael J. Graetz and Olivia Briffault, *A 'Barbarous Relic': The French, Gold, and the Demise of Bretton Woods*, in The Bretton Woods Agreements, eds. Naomi Lamoreaux and Ian Shapiro: 121–142.

85 Federal Reserve Economic Data, *Consumer Price Index for All Urban Consumers*, beschikbaar online

het zou na verloop van tijd erg moeilijk worden om het terug te draaien. Inflatie is verslavend, waarschuwde de econoom. Zodra de economie gewend raakt aan gemakkelijk geld, zal het alleen maar meer nodig hebben om het kunstmatig hoge werkgelegenheidsniveau te handhaven.

In een vroeg stadium lijkt inflatie de economie inderdaad te stimuleren. Als inflatie begint, drijft het de prijzen op naar een hoger niveau dan bedrijven hadden verwacht. Dit wordt door hen als een aangename verrassing gezien, omdat ze hun producten voor meer geld kunnen verkopen dan ze hadden ingecalculeerd, waardoor ze grotere winsten genieten. Bedrijven die in zwaar weer verkeerden en anders ten onder waren gegaan, kunnen hun hoofd boven water houden dankzij deze onverwachte economische opleving.

Maar als de inflatie langere tijd aanhoudt, legt Hayek uit, zullen bedrijven uiteindelijk de verwachting van hogere toekomstige prijzen moeten meewegen. Om concurrerend te blijven, zullen ze hun investeringen in het productieproces moeten verhogen, wat de prijs van kapitaal en arbeid omhoogdrijft, tot het punt waarop de algehele winstmarges weer terug zijn op het punt waar ze begonnen.

Dit betekent ook dat de bedrijven die al kampten met problemen vóórdat de inflatie toesloeg, weer het risico lopen om failliet te gaan.

Om te voorkomen dat deze bedrijven kopje onder gaan, en om het positieve effect van het nieuwe geld te verlengen, is nog hogere inflatie nodig. Deze hogere inflatie zal de prijzen nog meer opdrijven dan verwacht, wat opnieuw een welkome verrassing betekent voor de bedrijven.

Maar als deze hogere inflatie ook aanhoudt, moet het natuurlijk uiteindelijk opnieuw worden meegenomen in het productieproces, waardoor de bedrijven die al worstelden weer het risico lopen om ten onder te gaan.

Deze bedrijven zouden misschien gered kunnen worden door nog meer inflatie, maar uiteindelijk, waarschuwde Hayek, kan nieuw geld alleen op korte termijn stimuleren, terwijl er naarmate de tijd vordert steeds meer van nodig zou zijn. Het zou onvermijdelijk resulteren in een economie met zowel hoge inflatie als economische stagnatie.

Hayek:

'Als inflatie al enige tijd aan de gang is, zullen veel activiteiten afhankelijk zijn geworden van het voortduren ervan in een progressief tempo. Er zal een situatie

ontstaan waarin, ondanks de stijgende prijzen, veel bedrijven verlies zullen lijden, en waarin er aanzienlijke werkloosheid kan zijn. Zodra de economie zich heeft aangepast aan een bepaald inflatietempo is een depressie met stijgende prijzen een typisch gevolg van slechts het afremmen van de stijging van de inflatie.[86]

In economische termen wordt dit resultaat (een economie met zowel inflatie van de munteenheid als economische stagnatie) stagflatie genoemd.

Het Cantillon-effect

Hayek maakte zich om diverse redenen zeer veel zorgen over inflatie (en het uiteindelijke vooruitzicht van stagflatie).

Ten eerste kan inflatie het intertemporele prijssysteem verstoren. Misschien wel het belangrijkste is, dat het de kredietmarkten in de war kan brengen, aangezien schuldenaren en schuldeisers door inflatie op zeer verschillende manieren worden beïnvloed: schuldenaren profiteren als de reële waarde van hun schulden daalt, terwijl schuldeisers verlies lijden omdat het geld dat ze later terugkrijgen minder waard zal zijn dan het geld dat ze hebben uitgeleend.

Een tweede aspect van inflatie, en in de ogen van Hayek wellicht nog bedrieglijker, is dat het de boekhoudkundige praktijken vertekent. Inflatie kan namelijk winstcijfers oppompen, waardoor het lijkt alsof het rendement op investeringen hoger is dan in werkelijkheid. Slimme individuen kunnen misschien de devaluatie van de munteenheid meenemen in hun winst-en-verliesberekeningen, maar de econoom merkt op dat belastinginspecteurs nog steeds zullen aandringen op het belasten van de *schijnwinsten*. Inflatie leidt in wezen tot een impliciete stijging van de belastingen.

Maar Hayeks grootste bezorgdheid omtrent inflatie was een zorg die al in de achttiende eeuw beschreven was door de Iers-Franse econoom Richard Cantillon, en die bekend stond als het Cantillon-effect.[87]

Het probleem, kort gezegd, is dat nieuw geld als eerste in omloop wordt gebracht door het in de economie te spenderen. En wanneer dit nieuwe geld

86 Friedrich A. Hayek, *Can We Still Avoid Inflation?* in *The Austrian Theory of the Trade Cycle and Other Essays*, ed. Richard M. Ebeling: 101.

87 Mark Blaug, *Economic Theory in Retrospect*, 4th edition, 20–23.

voor het eerst wordt uitgegeven, wordt het uitgegeven in een economie die nog steeds de *oude* prijzen hanteert, die nog niet de extra bijgedrukte geldhoeveelheid weerspiegelen. Het spenderen van dit geld leidt vervolgens tot het opdrijven van de prijzen van de eerste goederen of diensten die ermee worden gekocht. De bedrijven die deze goederen of diensten verkopen, genieten van extra winst.

Deze bedrijven krijgen de kans om het nieuwe geld als eerste opnieuw uit te geven, terwijl de meeste prijzen in de economie nog niet zijn aangepast aan de toename van de geldhoeveelheid. De bedrijven die *deze* betalingen ontvangen mogen vervolgens het geld uitgeven in een economie waarin sommige prijzen zijn bijgesteld, maar nog niet allemaal; toch een voordeel. Dit gaat door totdat het nieuwe geld volledig door de economie is verspreid: prijsverhogingen vinden eerst plaats in een deel van de economie, waarna het zich als een rimpeling door de rest van de samenleving verspreidt.

Dit betekent dat degenen die *dichtbij* de bron van het geld zijn, hiervan kunnen genieten voordat de prijzen aangepast zijn: ze ervaren een toename in hun reële inkomen. Degenen die zich aan de *buitenkant* bevinden, zien alle prijzen stijgen voordat ze het nieuwe geld te pakken krijgen. Als ze uiteindelijk een beetje van het nieuwe geld ontvangen, biedt dit geen comparatief voordeel meer. Tot het moment dat het nieuwe geld hen bereikt, ervaarden ze een daling in hun reële inkomen.

Zoals Hayek de bevindingen van Cantillon samenvatte:

> *'Alleen die personen profiteren van de toename van geld waarvan de inkomens vroeg stijgen, terwijl voor personen waarvan de inkomens later stijgen, de toename van de geldhoeveelheid schadelijk is.'*[88]

Goudproducenten waren historisch gezien te vinden in het hart van het Cantillon-effect. Maar naarmate de rol van goud in het financiële systeem minder belangrijk werd en het Keynesianisme zijn intrede deed, begonnen overheden steeds vaker hun plaats te claimen in het centrum van het geldcreatieproces. Telkens wanneer overheden de geldhoeveelheid vergroten om de economie te stimuleren, komt dit in onevenredige mate de overheid zelf ten goede. Door het Cantillon-effect profiteren ook overheidsmedewerkers, aannemers van de

88 Hayek, *Prices and Production*, 203.

overheid en de bedrijven die het dichtst bij de overheid staan, zoals financiële instellingen.

Dit resulteert in hogere prijzen in de delen van de economie die dicht bij de overheid staan, wat op zijn beurt weer meer middelen zal aantrekken. Belangrijk echter is dat deze middelen niet naar die delen van de economie stromen omdat ze daar de meeste waarde bieden voor de individuen in de samenleving. In plaats daarvan zal het Cantillon-effect de verdeling van middelen scheef trekken richting de bron van het nieuwe geld, in de praktijk richting de overheid en de financiële sector.

Aangezien het verslavende effect van inflatie vereist dat er steeds meer van is, zal na verloop van tijd een overmatige hoeveelheid bedrijfsactiviteit zich gaan richten op de overheid, volledig afhankelijk van de creatie van nieuw geld, maar zonder dat het veel waarde aan de samenleving toevoegt. Hayek voorspelde een voortdurende misallocatie van middelen ten gunste van de staat en ten nadele van de rest van de economie.

En uiteindelijk, zo waarschuwde de econoom, kan voortdurende, overdadige geldcreatie leiden tot de vernietiging van wat er nog over is van het vrijemarktsysteem. Hoge inflatie kan de prijzen, en daarmee de verdeling van middelen, zo ernstig verstoren dat er uiteindelijk sterke maatschappelijke druk ontstaat voor de invoering van prijscontroles.

Een rampzalige uitkomst, volgens Hayek:

> *'Openlijke inflatie is al erg genoeg, maar inflatie die onderdrukt wordt door [prijs]controles is nog erger: het is het echte einde van de markteconomie.'*[89]

De overheid buitenspel zetten

Keynesianen, zo'n beetje alle mainstream economen van die tijd, deelden Hayeks zorg over inflatie en in het bijzonder stagflatie niet. Ze geloofden in feite dat stagflatie onmogelijk was. Zoals de Phillips-curve had aangetoond, waren inflatie en werkloosheid *omgekeerd* gecorreleerd: een hogere inflatie zou betekenen dat er minder werkloosheid was.

89 Hayek, *Can We Still Avoid Inflation?* 108.

Maar de beleidsmaatregelen van Nixon begonnen de aannames van deze Keynesianen te weerleggen. Een combinatie van lage rentetarieven en stijgende olieprijzen door aanhoudende internationale strubbelingen zorgde in het begin van de jaren '70 al snel voor een opkomende inflatie. Maar nu verslechterden de economische vooruitzichten wereldwijd tegelijkertijd. Het decennium zou in het teken komen te staan van stagflatie. Dit bracht een geloofscrisis in de Keynesiaanse denkwijze met zich mee.

Hayek had zich in de aanloop naar de jaren '70 voornamelijk op de politiek gericht: hij had bijvoorbeeld uitgelegd hoe spontane orde ook gold voor de ontwikkeling van het rechtssysteeem, waardoor hij gematigder werd vergeleken met enkele van de radicalere libertarische Oostenrijkse economen. Maar halverwege de jaren '70 besloot hij dat hij niet langer kon zwijgen. Na een lange academische loopbaan die hem van de Universiteit van Chicago naar de Universiteit van Freiburg en uiteindelijk de Universiteit van Salzburg bracht, wendde Hayek zich opnieuw tot het schrijven over monetair beleid.

Hayek, een Oostenrijker, was ervan overtuigd dat de Keynesiaanse leer en haar onjuiste ideeën over geld de wereldwijde economie aan het ruïneren waren. Hij vond dat mensen hiervan bewust moesten worden gemaakt: dit was opnieuw een prioriteit voor hem geworden. Hoewel Hayek al ver in de zeventig was, was hij nog net zo vastberaden en compromisloos als altijd. Hij beschreef inflatie nu niet alleen als schadelijk, maar ook als ronduit onethisch, en vergeleek het zelfs met diefstal. Het geld was volgens Hayek al heel lang defect, en hij vond dat het hoog tijd was dat het gerepareerd werd.

Hoewel decennia van onverantwoorde overheidsuitgaven hadden geleid tot stagflatie, vond Hayek het te makkelijk om simpelweg de verantwoordelijke politici de schuld te geven. Hij geloofde dat het probleem dieper lag. Overheidsuitgaven waren populair vanwege de kortetermijnvoordelen die ze konden bieden. Al die geldcreatie gebeurde in democratische samenlevingen, in feite op verzoek van de maatschappij. Zolang de overheid en haar instellingen de poortwachters van de munteenheid waren, zouden invloedrijke belangengroepen politici er uiteindelijk toe aanzetten om zo'n krachtig instrument in hun voordeel te gebruiken.

Hayek kwam dus tot de conclusie dat overheden helemaal geen poortwachters van geld zouden moeten zijn:

'Een goede munteenheid, net als een goede wet, moet functioneren zonder rekening te houden met de effecten die beslissingen van de uitgever zullen hebben op bekende groepen of individuen', schreef Hayek.[90] 'Zelfs met de beste bedoelingen ter wereld, kan geen enkele regering deze druk weerstaan [van zulke groepen of individuen], tenzij ze kunnen wijzen op een vaste barrière die ze niet kunnen overschrijden.'[91]

Goud zou in theorie een dergelijke sterke barrière kunnen bieden. Idealiter zou goud dan zelf als munteenheid worden gebruikt, in plaats van dat het in bankkluizen wordt opgeslagen, wat het fractioneel reservebankieren mogelijk maakt. Maar de onpraktische aard van het rechtstreekse gebruik van goud bij transacties en de uitdagingen van een veilige opslag betekenen waarschijnlijk dat dit ideaal onhaalbaar is.

Een valuta gedekt door goud — zoals bij de klassieke goudstandaard — was praktischer, maar dit vereist vertrouwen dat regeringen niet de valuta zullen devalueren ten opzichte van goud, de dekkingsratio eenzijdig zullen veranderen, of zelfs de omwisselbaarheid volledig zullen opheffen. Dit zijn inderdaad allemaal dingen die Hayek regeringen in zijn eigen leven heeft zien doen.

Hayek heeft daarom altijd moeite gehad met het vinden van de ideale oplossing voor het problematische geldstelsel.

Maar in de nadagen van zijn carrière, viel het kwartje eindelijk voor hem.

'Midden in mijn radeloosheid over de hopeloosheid van het vinden van een politiek haalbare oplossing voor wat technisch gezien het eenvoudigst mogelijke probleem is, namelijk het stoppen van inflatie, heb ik ongeveer een jaar geleden in een lezing een ietwat schokkende suggestie geopperd. Het verder uitdiepen hiervan heeft geheel onverwachte nieuwe horizonten geopend', schreef Hayek halverwege de jaren '70.

'Ik kon niet nalaten het idee verder uit te diepen, omdat de taak om inflatie te voorkomen mij altijd van het grootste belang heeft geleken. Niet alleen vanwege de schade en het leed dat grote inflaties veroorzaken, maar ook omdat ik er al lang van overtuigd ben dat zelfs milde inflaties uiteindelijk de steeds terugkerende depressies en werkloosheid veroorzaken. Deze vormen terecht argumenten tegen het systeem van

90 Friedrich A. Hayek, *Denationalisation of Money*, 89.

91 Friedrich A. Hayek, *Denationalisation of Money*, 91.

vrij ondernemerschap en moeten worden voorkomen als een vrije samenleving wil overleven.'[92]

Het idee was dat geld aan de vrije markt overgelaten moest worden.

Denationaliseren van geld

Hayek bepleitte zijn zaak voor het eerst in zijn toespraak tot de Gold and Monetary Conference in Genève in 1975.[93] In 1976 presenteerde Hayek dit onconventionele voorstel uitvoerig in zijn boek *Denationalisatie van Geld*. In essentie betoogde de econoom dat banken volledig gedereguleerd moesten worden, zodat ze elk geld dat ze geschikt achten konden uitgeven: gedekt of ongedekt, inflatoir of deflatoir, al dan niet gecreëerd door leningen, en tegen elk renteniveau dat ze wilden vragen.

Hayek stelde voor om het feitelijke staatsmonopolie op geld te beëindigen.

In dit systeem (een behoorlijk radicale vorm van *vrij bankieren*) concurreren banken om klanten hun geld te laten gebruiken. Hayek geloofde dat juist deze concurrentie nodig was om de beste vorm van geld te ontwikkelen: zoals in elke vrije markt, moeten banken hun klanten een product leveren – in dit geval, geld zelf – met betere eigenschappen dan de producten die hun concurrenten aanbieden. Hayek redeneerde dat deze concurrentie tot verbetering zou leiden, omdat de markt het beste beschikbare geld zou selecteren.

Een bijzonder belangrijke eigenschap van elke munteenheid is ongetwijfeld de hoeveelheid geldeenheden, of specifieker, de groeisnelheid van de geldvoorraad — de grootste oorzaak van inflatie. Gebruikers van een munteenheid zullen waarschijnlijk niet willen dat de voorraad te snel uitgebreid wordt, omdat dit de koopkracht van de eenheden die ze bezitten, zou schaden. Hayek geloofde dat concurrentie in dit domein de uitgevers van valuta eerlijk zou houden: als één bank te veel van zijn geld creëerde, zouden klanten snel naar een alternatief overstappen. In feite zou ongewenste inflatie in essentie onmogelijk zijn, omdat mensen gewoonweg kunnen kiezen om niet mee te doen.

92 Friedrich A. Hayek, *Denationalisation of Money: The Argument Refined*, 13.

93 Opnieuw gepubliceerd in Friedrich A. Hayek, *Choice in Currency: A Way to Stop Inflation*.

Terwijl het vrijwel onmogelijk was gebleken om overheden te stoppen met het opblazen van hun nationale munteenheden om hun uitgaven te financieren, redeneerde Hayek dat de discipline van de vrije markt dit probleem vanzelf zou oplossen.

Als een hypothese over hoe geld eruit zou zien in een wereld met vrij bankieren, stelde de econoom zich voor dat banken waarschijnlijk zouden streven naar een specifiek niveau van koopkracht, mogelijk gebaseerd op een bepaalde prijsindex. Ze kunnen dit doen door meer valuta uit te geven als de koopkracht van het geld boven dat doelniveau stijgt en door valuta uit de circulatie te halen als de koopkracht daaronder zakt. Een groot deel van het werk van de banken zou zijn om uit te zoeken wat mensen als een wenselijk niveau van koopkracht voor hun valuta beschouwen, zodat ze het soort geld kunnen selecteren dat het beste aan hun behoeften voldoet.

'Elke uitgever van een aparte valuta zou in staat moeten zijn om de hoeveelheid ervan te reguleren om het zo voor het publiek het meest acceptabel te maken, en concurrentie zou hem daartoe dwingen', schreef Hayek. 'Sterker nog, hij zou weten dat de straf voor het niet waarmaken van de opgewekte verwachtingen zou leiden tot het onmiddellijk verlies van klanten.'

Hij voegde eraan toe: '[…] de uitgevende banken, enkel geleid door hun streven naar winst, zouden zo het publieke belang beter dienen dan welke instelling dan ook die dat zogenaamd nastreeft.'[94]

In *The Argument Refined*, de herziene en uitgebreidere versie van het boek dat twee jaar later werd gepubliceerd, stelde Hayek voor dat het meest aannemelijke resultaat van een vrij bankensysteem niet een breed scala aan valuta met verschillende doelen voor koopkracht zou zijn. In plaats daarvan speculeerde de econoom dat de overgrote meerderheid van de mensen zich zou richten op één type geld dat een algemeen acceptabel stabiliteitsdoel heeft. Dit stabiliteitsdoel zou op zijn beurt ook door andere valuta worden aangenomen, verwachtte Hayek, in wezen het stabiliteitsdoel zelf veranderend in iets van een meta-valuta waarop andere valuta zouden worden gebaseerd.

Op het eerste gezicht zou dit als een toegeving aan het gebruik van een consumentenprijsindex om stabiliteit te bepalen kunnen worden beschouwd, en

94 Friedrich A. Hayek, *The Argument Refined*, 78.

tot op zekere hoogte was dat misschien ook zo. Maar het is belangrijk om te benadrukken dat Hayeks versie van dit idee niet verplicht of bindend was, noch dat het een door de overheid aangewezen centraal orgaan omvatte om te bepalen hoe zo'n index opgezet zou moeten worden. Hij geloofde dat dit aan de vrije markt overgelaten moet worden, zodat mensen vrij zijn om te kiezen voor welk doel zij het meest stabiel (of anderszins wenselijk) beschouwen.

Dit zou inderdaad een valuta met een vaste voorraad kunnen omvatten, of wat Hayek eerder in zijn carrière had omschreven als neutraal geld.

Ongedekt geld

Het voorstel van Hayek kreeg niet meteen de steun van al zijn collega's binnen de Oostenrijkse school van economie. Veel Oostenrijkers waren van mening dat de markt al een lange tijd geleden de beste vorm van geld had gekozen. In een strijd die duizenden jaren heeft geduurd, had goud gewonnen. Zij hielden vol dat goud nog steeds de beste vorm van geld was, en dat nieuwe valuta op z'n minst *gedekt* moesten worden door het kostbare metaal.

Hoewel het in een vrij bankensysteem uiteraard mogelijk was om een door goud gedekte valuta te bieden, verwachtte Hayek niet dat de meeste mensen hiervoor zouden kiezen. Hij erkende dat de markt oorspronkelijk goud had gekozen als de beste vorm van geld, maar Hayek geloofde dat regeringen sindsdien de verdere ontwikkeling van geld hadden verhinderd door monopolisatie en strikte regulatie. Hayek verwachtte dat geld drastisch zou verbeteren als het aan de markt werd overgelaten.

'Ik geloof dat we het veel beter kunnen doen dan goud ooit mogelijk heeft gemaakt. Overheden kunnen het niet beter doen. Vrij ondernemerschap, oftewel de instellingen die zouden voortkomen uit een proces van concurrentie om goed geld te bieden, zouden dat ongetwijfeld wel kunnen', schreef hij. 'De mogelijkheid tot omzetting [naar goud] is een noodzakelijke waarborg die men aan een monopolist moet opleggen, maar is onnodig bij concurrerende aanbieders die zich niet in de concurrentiestrijd kunnen handhaven tenzij ze geld bieden dat minstens zo voordelig is voor de gebruiker als elk ander.'[95]

95 Friedrich A. Hayek, *The Argument Refined*, 83.

Hayek overwoog echter wel dat nieuwe munten van de vrije markt mogelijk in eerste instantie door fiatgeld gedekt moesten worden. Dit zou vergelijkbaar zijn met hoe fiatgeld in eerste instantie door goud werd gedekt tot mensen het nieuwe geld leerden vertrouwen. Dit kon een tijd duren, gaf de econoom toe: 'Het bijgeloof sterft maar langzaam.'[96] Maar uiteindelijk zouden mensen gaan begrijpen dat inflatoir fiatgeld continu waarde verliest tegenover het privégeld. Ze zouden door economische prikkels tot het inzicht komen dat wat ze echt van geld verwachten, schaarste is.

In een vrij bankensysteem zou er wel geen regulering zijn die garandeert dat gedekte valuta inderdaad uitwisselbaar waren voor datgene waardoor ze gedekt werden. Hoewel specifieke afspraken onder regulier contractrecht bindend kunnen zijn, zouden er geen bijzondere wetten zijn over de dekkingsratio en zou er ook geen kredietverstrekker in uiterste nood zijn. Banken zouden de kosten van hun eigen risico's dragen, en dat geldt ook voor de klanten die ervoor kiezen om deze banken te vertrouwen met hun geld. Maar dit kan misschien worden gezien als een goede zaak: vrij bankieren zou het morele risico wegnemen.

En door vrije banken volledig onafhankelijk van het bestaande financiële systeem te laten functioneren, geloofde Hayek dat het plan ook daadwerkelijk haalbaar was.

'Niet het minste voordeel van het voorgestelde afschaffen van het overheidsmonopolie op de uitgifte van geld, is dat het ons de kans zou geven om ons te bevrijden uit de impasse waarin deze ontwikkeling [van het bankwezen] ons heeft geleid', schreef Hayek. 'Het zou voorwaarden creëren waarbij de verantwoordelijkheid voor het beheren van de hoeveelheid valuta wordt gelegd op agentschappen wiens eigenbelang hen ertoe zou aanzetten het op zo'n manier te beheren dat het voor de meeste gebruikers het meest acceptabel is.'[97]

In een wereld waar banken en andere financiële instellingen in de loop der tijd afhankelijk waren geworden van een sterk gereguleerd en nauw verweven financieel systeem, en waar het buitengewoon moeilijk was om zinvolle veranderingen aan te brengen, betekende Hayeks oplossing een nieuwe start. Hij stelde voor om een marktgebaseerd monetair systeem uit te rollen naast de gevestigde financiële

96 Friedrich A. Hayek, *The Argument Refined*, 109.

97 Friedrich A. Hayek, *The Argument Refined*, 77.

sector, om zo een volledig nieuw valutasysteem te laten ontstaan als mensen het vrijwillig zouden adopteren.

Hayek zag geld als een spontane orde.

Het realiseren van vrij bankieren

Hoewel de meeste landen technisch gezien alternatieve valuta toestaan (er zijn doorgaans geen wetten die ze expliciet illegaal maken) wordt dit vaak niet weerspiegeld in de praktijk. Bankregulaties, vergunningen voor geldtransfers, antiwitwasregels, wetten tegen vervalsing evenals belastingen (zoals vermogenswinstbelasting op alternatieve valuta) bieden wetshandhavingsinstanties meer dan voldoende middelen om bedrijven die valuta uitgeven compleet te sluiten, en hun operators veroordeeld te krijgen, of op zijn minst maken ze het opereren van dergelijke bedrijven praktisch onmogelijk.

Hayek wist dat het volledig elimineren van al deze wettelijke en fiscale obstakels – ware deregulatie – op enorme tegenstand zou stuiten.

Het merendeel van deze weerstand, verwachtte hij, zou afkomstig zijn van overheden: precies dezelfde partijen die deze deregulering uiteindelijk moesten doorvoeren en juridisch de ruimte voor valutaconcurrentie moesten faciliteren. Hayek was van mening dat overheden elke reden hadden om dit te voorkomen: zij waren de grootste begunstigden van het fiatgeldsysteem en hadden in feite het monopolie op geld. Hayek geloofde dat als overheidsvaluta moesten concurreren met vrijemarktvaluta, deze geen schijn van kans zouden hebben, en overheden dus waarschijnlijk niet tevreden zijn met vrije banken.

Om het nog moeilijker te maken, zou het merendeel van de economen waarschijnlijk ook tegen zijn, voorzag Hayek. Geld van de vrije markt zou immers waarschijnlijk elke kans op het manipuleren van rentetarieven om de koopkracht van de munteenheid te beïnvloeden en deflatie te voorkomen, elimineren. De meeste economen van de jaren ’70 waren van mening dat overheidsinstellingen zoals de Federal Reserve een belangrijke rol speelden bij het beheer van de geldvoorraad.

‘Ik vrees dat *Keynesiaanse* propaganda doorgedrongen is tot de massa, [en] inflatie respectabel heeft gemaakt en onruststokers heeft voorzien van argumenten die

de professionele politici niet kunnen weerleggen', schreef Hayek gefrustreerd.[98]

Hayek, de Oostenrijkse econoom, voegde nog toe dat hij verwachtte dat de meeste van de huidige banken ook tegen de verandering zouden zijn. De 'oude bankiers', zoals hij ze noemde, zouden niet in staat zijn om de nieuwe uitdagingen aan te kunnen die een vrije bankensector op hen zou zetten.

'Vooral in landen waar de concurrentie tussen banken al generaties lang wordt beperkt door kartelafspraken, die meestal worden getolereerd en zelfs aangemoedigd door overheden, zou de oudere generatie bankiers waarschijnlijk totaal niet in staat zijn om zich voor te stellen hoe het nieuwe systeem zou werken en daarom in de praktijk unaniem zijn in het afwijzen ervan', schreef Hayek.[99]

Met overheden, economen en bankiers als voorziene tegenstanders, verwachtte Hayek zeker dat het realiseren van vrij bankieren een moeilijke strijd ging zijn, maar toch geloofde hij sterk dat het desondanks gedaan moest worden.

Hayek schreef in de tweede, verfijnde versie van zijn boek: '[Denationalisatie van geld is] de enige manier waarop we nog kunnen hopen om de voortdurende vooruitgang van alle overheidssturing richting totalitarisme te stoppen, wat voor veel scherpzinnige waarnemers onvermijdelijk lijkt. Maar de tijd dringt. Wat nu dringend nodig is, is niet de bouw van een nieuw systeem, maar het snel verwijderen van alle wettelijke obstakels die al tweeduizend jaar de weg hebben geblokkeerd naar een evolutie die ongetwijfeld gunstige resultaten zal opleveren die we niet kunnen overzien.'[100]

En hij geloofde dat het mogelijk was. De sleutel lag bij het winnen van de steun van de algemene bevolking. Hayek maakte een vergelijking met de vrijhandelsbewegingen uit de negentiende eeuw en stelde dat een nieuwe burgerbeweging, een *vrij geld-beweging*, mensen zou kunnen informeren over de schade die inflatie en valutamanipulatie veroorzaken. Een bredere publieke bewustwording van deze kwesties zou een solide basis kunnen vormen voor de zaak. De daadwerkelijke politieke verandering (de deregulering van de bankensector) werd verondersteld in een later stadium te volgen.

Opgericht door onderzoekers George Selgin, Lawrence White, en Kevin Dowd een paar jaar later, in de jaren '80, kwam de moderne vrije-bankenschool waar-

98 Friedrich A. Hayek, *The Argument Refined*, 133.
99 Friedrich A. Hayek, *The Argument Refined*, 93.
100 Friedrich A. Hayek, *The Argument Refined*, 134.

schijnlijk het dichtst in de buurt van het opzetten van zo'n beweging. De door Hayek geïnspireerde lobbygroep deed onderzoek naar de geschiedenis en het potentieel van vrije banken en publiceerde hun bevindingen in verschillende boeken en artikelen.

Maar hoewel de moderne vrije-bankenschool een kleine aanhang kreeg van gelijkgestemde, meestal Oostenrijkse, economen, slaagde het er niet in om de harten en de geesten van het grote publiek te winnen. Hoewel Hayek nog lang genoeg leefde om een nieuwe generatie politici en economen zijn werk over vrije markten en het prijssysteem te zien herontdekken en revitaliseren, tot het hem zelfs de Nobelprijs voor economie opleverde in 1976, bleef Hayeks oproep voor monetaire hervorming onbeantwoord. fiatvaluta bleef oppermachtig tot, in 1992, Hayek op tweeënnegentig jarige leeftijd stierf.

Toch waren zijn ideeën niet volledig vergeten.

Het werk van Hayek op het gebied van geld diende kort na zijn overlijden als inspiratie voor een groep hackers en cryptografen uit Californië. Maar deze hackers en cryptografen waren niet van plan om politici, economen en bankiers te overtuigen om de wet te veranderen.

Ze gingen een toekomst bouwen zonder hen…

Hoofdstuk 6

eCash (en vertrouwensloze tijdstempels)

Sinds Whitfield Diffie en Martin Hellman de Diffie-Hellman-sleuteluitwisseling introduceerden in 1976, begrepen cryptografen hoe twee mensen die elkaar nooit eerder ontmoet hadden de inhoud van hun onderlinge berichten konden versleutelen voor iedereen behalve voor zichzelf. Ondertussen hadden de mixnetwerken van David Chaum al in de vroege jaren '80 de basis gelegd voor remailers: een digitale infrastructuur ontworpen om metadata te verbergen. Gecombineerd konden deze instrumenten een lange weg afleggen naar het bieden van privacy voor de meeste soorten van elektronische communicatie.

Maar het was ook Chaum die erkende dat het nog geen privacy kon bieden voor een zeer specifiek soort communicatie: communicatie van *waarde*.

Gedurende de jaren 70 en begin jaren 80 begon het bankwezen steeds meer geautomatiseerd te raken. Papieren bankbiljetten en metalen munten, die in die tijd niet langer door goud werden gedekt, begonnen steeds meer te worden verdrongen door betaalkaarten, terwijl banken onderling elektronisch schulden begonnen te vereffenen. Met de komst van de PC, en in zijn kielzog het internet, verwachtte Chaum dat de digitalisering van geld alleen maar zou versnellen. Dit zou financiële instellingen in staat stellen om kosten te besparen en hun beveiliging te verbeteren, terwijl het gemak voor de consument wordt verhoogd.

Maar Chaum realiseerde zich dat ook deze trend tot duistere situaties kon leiden. Als betalingsverkeer digitaal zou worden, zouden de banken die dit moge-

lijk maken door financiële regelgeving verplicht kunnen worden om gebruikers zichzelf te laten identificeren voordat ze toegang krijgen tot deze kanalen. Banken, en bij uitbreiding de overheidsinstellingen die op hen toezicht houden, zouden dan precies kunnen weten wie hoeveel geld naar wie stuurt, waar en wanneer.

Chaum zag de mogelijkheid van massasurveillance van betalingen als even zorgwekkend als de massasurveillance van elke andere vorm van communicatie. En niet zonder reden: iemands transactieverleden onthult mogelijk net zoveel persoonlijke informatie als hun tekstcommunicatie, zo niet meer.

'Er wordt een basis gelegd voor een dossiermaatschappij, waarin computers gebruikt kunnen worden om op basis van gegevens uit alledaagse consumententransacties de leefstijlen, gewoonten, locaties en relaties van individuen af te leiden', waarschuwde Chaum. 'Onzekerheid over of gegevens veilig blijven tegen misbruik door degenen die ze onderhouden of ervan gebruik maken kan een *afschrikwekkend effect* hebben, wat mensen ertoe kan brengen hun zichtbare activiteiten te veranderen. Naarmate de computerisering meer verspreid raakt, zal het potentieel voor deze problemen aanzienlijk toenemen.' [101]

Maar, zo stelde hij voor, er was een alternatieve toekomst mogelijk.

David Chaum legde uit: 'Elke keer dat een regering of bedrijf besluit om nog een set transacties te automatiseren, wordt de keuze gemaakt om informatie in handen van individuen of van organisaties te houden. Aan de ene kant ligt een ongekende controle en inspectie van mensenlevens, aan de andere kant een veilige gelijkwaardigheid tussen individuen en organisaties. De vorm van de samenleving in de volgende eeuw kan afhangen van welke aanpak de overhand heeft.'[102]

Volgens Chaum zou een maatschappij waarin anonieme transacties wel of niet mogelijk zijn uiteindelijk het verschil maken tussen democratie en dictatuur. Hij concludeerde daarom dat er een soort digitaal geld nodig was dat gebruikers een vergelijkbaar niveau van privacy bood als fysiek contant geld.

De wereld had behoefte aan *elektronisch geld*.

---

101 David Chaum, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, Communications of the ACM 28, no. 10: 1030–1044.

102 David Chaum, *Achieving Electronic Privacy*, Scientific American 267, 2: 96–101.

Het dubbele-uitgavenprobleem

Toen Chaum begon na te denken over ontwerpen voor een elektronisch geldsysteem, kwam hij al snel de eerste uitdaging tegen die iedereen die een digitale vorm van geld wil creëren, tegenkomt: *het probleem van dubbele uitgaven*.[103]

Eenvoudig gezegd, als valuta uitsluitend bestaat uit digitale informatie, enen en nullen, is het een fluitje van een cent om te kopiëren. Een enkele *digitale dollar* kan gerepliceerd worden en naar twee verschillende ontvangers worden gestuurd… of zelfs naar een miljoen verschillende ontvangers, tot het punt dat het geld last heeft van hyperinflatie. Het spreekt voor zich dat dit soort vervalsing de integriteit van de valuta fundamenteel zou schaden en het waardeloos zou maken.

Traditionele digitale geldsystemen lossen dit probleem van dubbele uitgaven op door middel van een vertrouwde partij, zoals een bank of betalingsverwerker.

De meest eenvoudige oplossing is dan ook het gebruik van een rekeningensysteem. In zo'n systeem hebben alle klanten van de bank een elektronische rekening bij de bank. Wanneer één van hen een andere wil betalen, sturen ze simpelweg een bericht naar de bank met de betalingsdetails. Ervan uitgaande dat de betaler voldoende saldo heeft, trekt de bank het bedrag af van zijn of haar rekeningsaldo en voegt het toe aan de rekening van de begunstigde.

Als de betaler niet genoeg geld heeft om de betaling uit te voeren, wordt de transactie geweigerd. Dus als iemand probeert zijn saldo dubbel te besteden door twee tegenstrijdige betalingsverzoeken naar de bank te sturen (terwijl hij niet genoeg geld heeft om beide betalingen te doen), zal de bank simpelweg kiezen welke transactie doorgaat (waarschijnlijk het eerste verzoek dat het ontving).

Dit lost het probleem van dubbele uitgaven op… maar het illustreert ook het privacyprobleem waar Chaum zich zorgen over maakte: de bank weet precies wie aan wie betaalt, hoeveel en wanneer. Bovendien heeft de bank totale controle over ieders saldi, en zou het mogelijk betalingen kunnen blokkeren of terugdraaien, en zelfs geld kunnen confisceren of verwijderen.

Daarom begon Chaum aan een zoektocht naar een manier waarop zo'n derde partij (de bank) dubbele uitgaven kon detecteren, zonder de mogelijkheid om te traceren hoe elke digitale dollar zich door de economie beweegt.

---

103 David Chaum, *Blind Signatures for Untraceable Payments*, Advances in Cryptology: Proceedings of Crypto 82: 199–203.

Blinde handtekeningen

De bekwaamde cryptoloog loste het probleem op in 1983. Nauwelijks nadat hij zijn doctoraat in informatica aan de Berkeley-universiteit had verdiend, werd Chaum aangesteld als professor aan diezelfde universiteit. Hij publiceerde zijn ontwerp voor een elektronisch geldsysteem in zijn paper getiteld *Blind Signatures for Untraceable Payments*.

Zoals de titel van het artikel al aangeeft, was zijn uitvinding van *blinde handtekeningen* de sleutel tot zijn ontwerp voor een privacy-respecterend betaalsysteem.

Chaums blinde handtekeningen waren een uitbreiding van de publieke-sleutelcryptografie en meer specifiek van het RSA cryptografische handtekening algoritme. Om even te herhalen, een cryptografische handtekening is in feite een stukje data (zoals een bericht) dat versleuteld is met een *geheime sleutel* en ontsleuteld kan worden met een *publieke sleutel*. Wanneer Alice een bericht en een bijbehorende cryptografische handtekening naar Bob stuurt, moet Bob in staat zijn het bericht te ontcijferen met Alice's publieke sleutel. Hierdoor wordt het omgezet in hetzelfde bericht, waardoor wiskundig wordt bewezen dat de handtekening inderdaad is gemaakt met haar geheime sleutel.

Een blinde handtekening voegt dus één laag van encryptie toe aan de mix.

Om Alice een blinde handtekening te laten maken, maakt Bob eerst een speciaal soort coderingssleutel aan, de zogenaamde *verblindende sleutel*, waarmee hij een bericht versleutelt. Bob geeft het versleutelde bericht vervolgens aan Alice, die het met haar geheime sleutel cryptografisch ondertekent. Wanneer ze het gecodeerde bericht ondertekent, weet ze niet wat het originele bericht eigenlijk is: ze *ondertekent blind*.

De resulterende handtekening is wiskundig aan Alice's publieke sleutel verbonden, zoals elke handtekening. Dat wil zeggen, haar publieke sleutel kan gebruikt worden om het exacte versleutelde bericht dat zij ondertekende te reproduceren (het bericht zelf zou nog steeds versleuteld zijn; het zou hetzelfde versleutelde *blob* reproduceren dat zij van Bob ontving).

Maar Bob kan ook *als eerste* de verblindende sleutel gebruiken om de laag encryptie die hiermee gecreëerd is, te verwijderen. In principe resulteert dit in een nieuwe, geldige handtekening van Alice, die dit keer overeenkomt met het originele bericht. Deze handtekening wordt de blinde handtekening genoemd. Met

de eerste laag encryptie verwijderd door Bob, kan nu iedereen de publieke sleutel van Alice gebruiken om het originele bericht vanuit de blinde handtekening te reproduceren.

Met andere woorden, iedereen die het originele bericht heeft, kan op dat moment Alice's publieke sleutel gebruiken om te verifiëren dat de blinde handtekening overeenkomt met het bericht. Dit geldt uiteraard ook voor Alice zelf. Als Bob haar het originele bericht en de blinde handtekening geeft, kan zij haar eigen publieke sleutel gebruiken om te verifiëren dat zij inderdaad een versleutelde versie van dat originele bericht blind ondertekende.

Als een realistische analogie die Chaum in zijn paper gebruikte, is het alsof Bob een brief in een envelop met carbonpapier stopt en deze envelop aan Alice overhandigt, die de buitenkant van de envelop ondertekent en deze teruggeeft aan Bob. Als Bob dan de envelop verwijdert en Alice de brief toont met een carbonkopie van haar handtekening, weet ze dat de brief inderdaad in de envelop zat die ze had ondertekend.

Anonieme betalingen

Om het blinde-handtekeningenschema te gebruiken voor een elektronisch geldsysteem, zou Alice uit het bovenstaande voorbeeld eigenlijk een bank zijn: laten we deze bank Alice Bank noemen. Alice Bank is een reguliere bank, waar klanten bankrekeningen hebben met dollardeposito's. En laten we zeggen dat Alice Bank vier klanten heeft: Bob, Carol, Dan en Erin.

Nu wil Bob iets kopen van Carol met elektronisch geld.

Ten eerste heeft Bob elektronisch geld nodig. Om dit te verkrijgen, vraagt hij een *opname* aan bij Alice Bank (idealiter had hij deze opname al gedaan voordat hij Carol wilde betalen, maar dat is een detail). Vreemd genoeg creëert Bob de digitale dollars zelf in de vorm van unieke serienummers. Vervolgens versleutelt hij deze nummers met een verblindende sleutel en stuurt ze naar Alice Bank.

Alice Bank ondertekent elke versleutelde dollar blindelings en stuurt de ondertekende versies terug naar Bob. Voor elke ondertekende dollar trekt Alice Bank een reguliere dollar van Bobs bankrekening af.

Daarna verwijdert Bob een laag van de encryptie met behulp van zijn ver-

blindende sleutel, waardoor Alice's ondertekeningen worden omgezet in blinde handtekeningen. Om Carol te betalen, stuurt hij de digitale dollars en bijbehorende blinde handtekeningen naar haar. Carol gebruikt de publieke sleutel van Alice Bank om de handtekeningen te verifiëren. Als deze correct zijn, stuurt ze de digitale dollars en de blinde handtekeningen door naar Alice Bank.

Alice Bank heeft deze digitale dollars nog nooit eerder gezien, omdat ze de eerste keer versleuteld waren. Het belangrijkste is dat ze kan bevestigen dat ze met haar eigen geheime sleutel zijn ondertekend. Vervolgens controleert Alice Bank de serienummers in haar lokale database om er zeker van te zijn dat dezelfde digitale dollars niet al door iemand anders zijn gedeponeerd, wat dubbele uitgaven voorkomt.[104]

Als de digitale dollars een geldige handtekening hebben en niet eerder zijn gebruikt, slagen ze voor beide controles. Alice Bank noteert dan deze digitale dollars in haar database om toekomstige dubbele uitgaven te voorkomen. Vervolgens wordt het equivalent van de digitale dollars als reguliere valuta op Carols bankrekening gestort, en krijgt ze hiervan een bevestiging. Carol weet nu dat ze een geldige betaling van Bob heeft ontvangen en levert hem het product of de dienst waarvoor hij betaalde.[105]

Omdat Alice Bank de ondertekende bankbiljetten pas voor het eerst ziet wanneer Carol ze stort, heeft de bank geen manier om te achterhalen dat ze oorspronkelijk van Bob kwamen. Ze hadden ook van iemand anders, zoals Dan of Erin, kunnen komen. Bovendien kan Alice Bank, nadat ze de digitale dollars aan Bob heeft uitgegeven, hem niet verhinderen ze te besteden, omdat ze niet kan

104 Chaum zou later ook een oplossing voorstellen waarbij dubbel uitgeven de anonimiteit van de dader zou kunnen opheffen, waardoor de noodzaak om elke binnenkomende betaling direct te controleren aan de hand van de bankgegevens enigszins wordt beperkt, aangezien de dader van een dubbele-uitgavenaanval kan worden geïdentificeerd.

105 Als een handig extra detail bevat het systeem ook een soort fraudepreventiecontrole, zij het een die ten koste gaat van privacy als en wanneer gebruikers ervoor zouden kiezen deze te gebruiken. Als Carol ten onrechte zou beweren dat ze nooit betaald is, zou Bob kunnen kiezen om de nonce aan Alice Bank te onthullen. Hiermee kan hij bewijzen dat hij de digitale dollars heeft gemaakt die Carol heeft gestort en dat hij ze aan haar heeft betaald.

bepalen welke digitale dollars ongeldig zouden moeten worden verklaard.[106]

Inderdaad, Chaum had een vorm van elektronisch geld ontworpen.[107]

In de jaren na de publicatie van zijn eerste werk over ontraceerbare betalingen, breidde Chaum de mogelijkheden van elektronisch geld verder uit in presentaties tijdens de Crypto-conferenties en in verschillende andere papers. Deze vervolgartikelen werkten precies uit hoe een elektronische geldregeling te implementeren, waarbij het beste gedetailleerde voorbeeld hiervan zijn paper uit 1985 was met de beschrijvende titel *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*.[108]

'De grootschalige geautomatiseerde transactiesystemen van de nabije toekomst kunnen zo worden ontworpen dat de privacy en de veiligheid van zowel individuen als organisaties beschermd blijven', zo verklaarde de introductie van één zin triomfantelijk.

DigiCash

Een paar jaar later, tegen 1989, had Chaum zijn intrek genomen in Amsterdam. Tijdens een van zijn eerdere bezoeken aan Nederland hadden lokale academici hem een baan aangeboden als hoofdcryptograaf bij het Centrum voor Wiskunde en Informatica (CWI), welke hij dankbaar had geaccepteerd. Het stelde hem in staat dicht bij zijn Nederlandse vriendin te wonen.

Ongeveer in deze periode overwoog de regering van Nederland een nieuw toltarievenproject. Het concept was dat auto's zouden betalen voor het privilege

106 Dat gezegd zijnde, zijn er nog enkele andere, mogelijk meer drastische maatregelen die Alice Bank had kunnen nemen. Naast het weigeren om digitale dollars aan Bob uit te geven, had ze ook alle elektronische contante betalingen kunnen blokkeren. Evenzo zou ze bepaalde gebruikers kunnen blokkeren van het accepteren van betalingen; zelfs als betalingen niet kunnen worden getraceerd, kunnen sommige gebruikers nog steeds worden uitgesloten van deelname aan het systeem.

107 Er kan worden gesteld dat Chaum een tamelijk losse definitie van *contant geld* gebruikte, aangezien contant geld meestal meer onderscheidende eigenschappen heeft. Chaums vorm van digitaal contant geld bood bijvoorbeeld beperkte overdraagbaarheid van persoon tot persoon — een kenmerk dat fysiek contant geld wel heeft, omdat het vrij kan worden doorgegeven. Niettemin heeft Chaum een vorm van digitaal geld uitgevonden die ten minste een vergelijkbaar niveau van privacy bood als fysiek contant geld, wat zijn hoofddoel was.

108 David Chaum, *Security Without Identification*.

om op bepaalde hoofdwegen te rijden door middel van een smartcard aan hun voorruit, die gescand zou worden door snelle kaartlezers op verschillende plekken langs de wegen. Maar het idee was controversieel: de Nederlanders waren niet enthousiast over het idee dat hun auto's gevolgd zouden worden.

Toen de overheid naar het CWI-onderzoekscentrum kwam om te vragen of ze wisten van enige privacybeschermende oplossingen om dit soort tolsysteem te realiseren, zag Chaum de kans waar hij op had gewacht. Hij had zijn technologie van blinde handtekeningen gepatenteerd, maar tot zijn eigen verbazing was de interesse in het ontwikkelen van digitale geldschema's sinds de publicatie van zijn papers beperkt geweest. Hij zag nu in dat er een unieke kans was om zelf te helpen de technologie in gebruik te nemen.

Chaum wist een groep studenten van de nabijgelegen Technische Universiteit Eindhoven te mobiliseren. Hij beloofde hen een reis naar de *International Collegiate Programming Contest* (ICPC) in Washington DC, op zijn kosten, en zelfs een vakantie naar Disney World in Florida, mits ze hielpen bij het omzetten van zijn blinde handtekening-technologie naar een werkbaar concept. Tijd was cruciaal, aangezien de Nederlandse overheid al een ontwikkelteam in gedachten had voor het project en niet echt zin had om het proces uit te stellen. Chaum en de studenten werkten dag en nacht, vanuit een van hun woonkamers.

Ze slaagden binnen tien dagen en hun *proof-of-concept* leverde Chaum het contract op.

Met deze initiële klus op zak, besloot de cryptograaf om DigiCash op te richten, een start-up gevestigd in Amsterdam die zich zou specialiseren in digitaal geld en betalingssystemen. Deze betalingssystemen omvatten uiteraard het overheidsproject voor tolheffing,[109] maar Chaum, die nu een eigen bedrijf leidde, wilde ook zijn grotere visie realiseren.

Het was begin jaren 90 steeds duidelijker geworden dat het internet mainstream zou worden, en Chaum was ervan overtuigd dat elektronische betalingen uiteindelijk een essentieel onderdeel van deze opkomende digitale wereld zouden zijn. Net als veel internetexperts in die tijd, verwachtte hij dat micro-betalingen

109 Uiteindelijk werd het tolproject niet aangenomen: het idee bleek te controversieel in Nederland. De technologie zou echter later worden gelicentieerd onder de naam *DyniCash* aan een onderneming in Dallas, Texas die gespecialiseerd was in communicatie op microgolf-frequenties voor treinen.

alomtegenwoordig zouden worden: webdiensten moesten op de een of andere manier geld verdienen, en de voor de hand liggende oplossing was inderdaad om mensen kleine bedragen te laten betalen om ze te gebruiken.

'Naarmate betalingen op het netwerk volwassen worden, ga je voor allerlei kleine dingen betalen, meer betalingen dan je vandaag de dag doet', voorspelde Chaum. 'Elk artikel dat je leest, elke vraag die je hebt, je zult ervoor moeten betalen.'[110]

Het prestigeproject van DigiCash was een digitaal betalingssysteem dat mensen in staat zou stellen om dergelijke betalingen privé te maken, met behulp van elektronisch geld — *eCash*.

CyberBucks

DigiCash begon snel internationaal onder de aandacht te komen. In een tijd waarin bedrijven als Netscape en Yahoo! bevestigden dat het grote geld zich verplaatste naar beginnende internetstart-ups, werd Chaums start-up door veel techondernemers in de vroege jaren 90 gezien als een rijzende ster in deze snelgroeiende industrie.

Het zou Chaum en zijn team, dat enkele van de studenten omvatte waarmee hij het project begon, meerdere jaren kosten om hun eerste proof-of-concept om te zetten in een volwaardig betalingssysteem. Met als uiteindelijk doel hun eCash-technologie te verkopen aan banken, was een niveau van beveiliging nodig vereist door banken.

In de tussentijd hebben ze wel een vroege versie van hun technologie uitgebracht. De eerste implementatie van Chaums elektronische geldontwerp door DigiCash werd uitgerold vanuit het eigen bedrijfskantoor, maar in plaats van Amerikaanse dollars, Nederlandse guldens of een andere fiatvaluta, gebruikte dit vroege elektronische geldsysteem *CyberBucks*.

CyberBucks was een verzinsel, niet gedekt door echte waarde, denk aan speelgeld, als je wilt. Maar het bedrijf beloofde wel nooit meer dan een miljoen eenheden in omloop te brengen. De virtuele munten werden meestal gratis

110 Peter H. Lewis, *Attention Internet Shoppers: E-Cash Is Here*, The New York Times, 19 oktober 1994, online

weggegeven, en iedereen kon het digitale geld op zijn computer opslaan, of het laden op een smartcard om een frisdrank of wat beltegoed te kopen in het DigiCash-gebouw zelf. Deze smartcards waren in feite onkraakbare, creditcard-achtige computers die speciaal waren ontworpen om dit soort betalingen te doen, en ze werden een belangrijke focus voor DigiCash: Chaum geloofde dat de smartcards essentieel waren voor de privacy van betalingen, omdat betalingen in persoon met een creditcard zelfs nog grotere privacyproblemen met zich meebrachten dan online betalingen.

Het idee achter CyberBucks was dat DigiCash-medewerkers konden experimenteren met de eCash-technologie, terwijl bezoekers konden proeven van de toekomst. Toen Chaum en zijn collega's besloten om 100 CyberBucks te schenken aan elke handelaar die bereid was om de internetmunteenheid als betaalmiddel te accepteren, begon een kleine groep enthousiastelingen CyberBucks ook buiten de kantoren van DigiCash te gebruiken. Hoewel het doorgaans alleen kon worden uitgegeven aan gadgetachtige producten zoals digitale afbeeldingen of kleine puzzelspellen voor Apple's Macintosh-computer, genoot de bedrijfsmunteenheid toch enige bredere acceptatie.

Daarnaast zijn de CyberBucks uiteindelijk op een niet-officiële CyberBucks-beurs verhandeld. Gebruikers konden de digitale geld-eenheden omzetten in daadwerkelijke fiatvaluta en vice versa. Na enige tijd kregen de CyberBucks een echte marktprijs, terwijl sommige gebruikers zelfs een klein beetje van de digitale valuta begonnen te verzamelen als een vorm van sparen of speculeren.

Dit vereiste wel veel vertrouwen in DigiCash. Hoewel het bedrijf beloofde de CyberBucks-voorraad te beperken tot één miljoen, was er geen ingebouwde methode om dit plafond af te dwingen. Theoretisch gezien konden Chaum en zijn collega's veel meer dan een miljoen CyberBucks uitgeven als ze dat wilden, en door de sterke privacyfuncties van het systeem zou er voor buitenstaanders geen manier zijn om te controleren of dit al dan niet was gebeurd.

Bovendien was het valutasysteem volledig afhankelijk van de voortdurende steun van DigiCash: de bedrijfsserver voorkwam dubbele uitgaven. Hoewel CyberBucks een leuk en interessant experiment was, was de uiteindelijke topprioriteit van DigiCash om hun belangrijkste elektronische geldproduct klaar te stomen voor het grote publiek…

eCash

Na vier jaar ontwikkeling bereikte eCash een standaard van beveiliging gelijk aan die van banken. In 1994 begonnen de proeven met echt geld, waarna financiële instellingen een licentie konden aanvragen bij de start-up van Chaum om de nieuwe technologie te gebruiken.

De eerste bank die deze kans greep, was de Mark Twain Bank in St. Louis, niet bepaald een internationale grootmacht, maar het was een begin. Klanten en bedrijven met een rekening bij Mark Twain konden genieten van privacy in hun elektronische transacties door betalingen te doen en te ontvangen in eCash.

Kort na de Mark Twain Bank volgden andere banken. Banken in verschillende landen, waaronder de Norske Bank en Bank Austria[111], destijds de grootste banken in respectievelijk Noorwegen en Oostenrijk, alsook de Australian Advance Bank, [112] begonnen kort daarna met eCash-proefprojecten. En begin 1996 stapte ook een van de grootste financiële instellingen ter wereld aan boord: Deutsche Bank begon de technologie van DigiCash te gebruiken.[113] Credit Suisse, nog een grote internationale speler, sloot zich ook aan bij de proeven.[114]

Echter, misschien nog opmerkelijker dan de samenwerkingsverbanden die Chaum tot stand bracht, waren de zakendeals die hij niet wist af te ronden. En hier begint het verhaal over wat er precies gebeurde bij DigiCash te variëren, afhankelijk van wie je het vraagt.

Volgens diverse medewerkers van DigiCash hadden grote spelers in de tech- en financiële industrie grote interesse getoond.[115] Twee van de drie meest prominente Nederlandse banken, ING en ABN Amro, zouden naar verluidt aanbiedingen voor samenwerkingen gemaakt hebben aan DigiCash ter waarde van tientallen miljoenen dollars. Ook betalingsreus Visa zou Chaum een deal van in de miljoenen hebben voorgelegd. Er wordt verder gezegd dat ook Netscape geïnteresseerd was: eCash had een mogelijke toevoeging kunnen zijn aan de

111 DigiCash, *Bank Austria and Den norske Bank to Issue ecash: the Electronic Cash for the Internet*, DigiCash, 14 april 1997, geraadpleegd online

112 DigiCash, *Advance Bank First to Provide DigiCash's ecash System in Australia*, DigiCash, October, 1996, geraadpleegd online

113 DigiCash, *DigiCash's Ecash to be Issued by Deutsche Bank*, DigiCash, 7 mei 1996, geraadpleegd online

114 Jeffrey Kutler, *Credit Suisse, Digicash in E-Commerce Test*, American Banker, 16 juni 1998, online

115 Next! Magazine *Hoe DigiCash alles verknalde*, Next!, January 1999, geraadpleegd online

populairste webbrowser van die tijd, maar deze samenwerking kwam niet tot stand.

Het grootste aanbod van allemaal zou echter zijn gekomen van niemand minder dan Microsoft. Zo luidt het verhaal, Bill Gates wilde eCash integreren in het Windows 95-besturingssysteem en bood DigiCash ongeveer 100 miljoen dollar om dit mogelijk te maken. In plaats daarvan zou Chaum twee dollar hebben gevraagd voor elke verkochte versie van Windows 95. Dit was te hoog gegrepen voor de Amerikaanse softwaregigant en daarmee was de deal van de baan.

Medewerkers van DigiCash stonden in eerste instantie achter de aanpak van Chaum, maar elke keer dat ze hoorden over het uiteenvallen van weer een miljoenendeal, groeide hun twijfel over zijn zakelijk inzicht. Een medewerker suggereerde later tegenover een Nederlandse reporter dat dezelfde eigenschap van wantrouwen, die Chaum tot een uitstekend cryptograaf maakte, hem in de weg stond als zakenman. Zijn 'paranoïde' karakter zou hem ongeschikt maken om zakenrelaties op te bouwen, wat ertoe leidde dat hij op het laatste moment uit zakenovereenkomsten stapte.

Bij de DigiCash kantoren nam de irritatie steeds verder toe. Naast het besef dat hun eigen baan op het spel stond als het bedrijf niet snel winstgevend zou worden, frustreerde het hen ook op ideologisch gebied dat Chaum er niet in slaagde om eCash bij meer mensen te introduceren. DigiCash wist ontwikkelaars aan te trekken die zich inzetten voor digitale privacy, en in een tijd waarin e-commerce populair begon te worden bij het grote publiek, waren ze bezorgd dat DigiCash niet mee ging doen.

Chaum zelf verwerpt deze beweringen echter krachtig als kwaadwillige laster. Hij beweert dat de verschillende aanbiedingen van meerdere miljoenen dollars niet zo concreet waren als deze werknemers leken te denken. In plaats van zijn persoonlijke tekortkomingen als zakenman, stelt hij dat er simpelweg geen grote markt was voor digitaal geld, een interpretatie die sommige van de meer commercieel ingestelde DigiCash-medewerkers ook hebben bevestigd.

Het maakt niet uit welke versie van het verhaal de waarheid dichter benadert, het is duidelijk dat eind 1996 het geduld in het DigiCash kantoor op was. De medewerkers van Chaum eisten een verandering in het bedrijfsbeleid.

Faillissement

Uiteindelijk kwam de verandering vanuit Chaums thuisland.

Op zoek naar nieuwe fondsen richtte zijn bedrijf zich tot Amerikaanse durfkapitalisten, aangezien de investeringscultuur in de VS immers beter bekend was, en een grotere honger naar dit soort high-tech-start-ups met een hoog risico. DigiCash kreeg een financiële injectie, terwijl MIT-hoogleraar Nicholas Negroponte tot voorzitter van de raad van bestuur werd benoemd en Chaum als CEO vervangen werd door Michael Nash, een veteraan van Visa.[116] Illustratief voor de nieuwe koers van het bedrijf verhuisde het hoofdkantoor van Amsterdam naar Palo Alto, Californië, in het hart van Silicon Valley, waar de waarderingen van technologie-start-ups door het dak gingen. Chaum bleef wel deel uitmaken van DigiCash, maar dan nu als CTO.

Dit was echter niet precies de soort verandering waarop de meeste Nederlandse werknemers van DigiCash hadden gehoopt. Verschillende van hen besloten op dit moment om het bedrijf te verlaten.

En misschien nog belangrijker, het bleek uiteindelijk niet veel verschil te maken.

eCash sloeg gewoonweg niet aan bij het publiek. De banken die de technologie uitprobeerden, promootten het niet echt bij hun klanten, en het hielp waarschijnlijk ook niet dat eCash relatief duur in gebruik was, waarbij het meestal enkele procenten van de transactiewaarde aan kosten in rekening bracht. Mark Twain bank had in een paar jaar tijd slechts 300 handelaren en 5.000 gebruikers ingeschreven, terwijl andere banken het niet veel beter deden.

En, wellicht Chaums lezing van DigiCash's geschiedenis kracht bijzettend, was het nieuwe leiderschap van het bedrijf ook niet in staat om grote deals te sluiten. Hoewel een samenwerking met CitiBank bijna rond was, wat DigiCash wellicht het broodnodige momentum had kunnen geven, liep het uiteindelijk spaak en de grote Amerikaanse financiële instelling trok zich terug.

Tegen eind 1997 had DigiCash het merendeel van zijn fondsen opgebrand. Na een laatste herschikking van de organisatie en leiderschap van het bedrijf, vroeg de start-up van Chaum in 1998 het faillissement aan.

---

116 American Banker, *Digicash Sends Signal by Hiring Visa Veteran*, American Banker, 6 mei 1997, online

Na acht jaar van bedrijvigheid, had DigiCash het niet kunnen waarmaken om aan de hype te voldoen die het had gegenereerd onder de eerste generatie van internetondernemers. Misschien is de onkunde van Chaum om zakelijke relaties op te bouwen wel de oorzaak voor de mislukking, zoals sommige voormalige werknemers concludeerden. Of misschien was de vraag naar anoniem digitaal geld, hoewel een verleidelijk verkooppunt in de vroege jaren '90, gewoon niet zo hoog als de baanbrekende cryptograaf aanvankelijk had verwacht. In plaats van micro-betalingen, werd een groot deel van het web uiteindelijk gefinancierd door advertenties, en privacy leek niet erg hoog op de prioriteitenlijst van de gemiddelde consument te staan.

Bovendien worstelde DigiCash met een kip-en-ei-probleem. eCash was alleen nuttig als mensen het ergens konden uitgeven: zonder plekken om het digitale geld te besteden, was er geen reden om het in de eerste plaats te bemachtigen. Tegelijkertijd was het voor handelaren alleen zinvol om eCash te accepteren, als er genoeg mensen waren die het wilden uitgeven.

'Het was moeilijk om voldoende handelaren te vinden die het wilden accepteren, zodat je genoeg consumenten kon vinden die het wilden gebruiken, of vice versa', herinnert Chaum zich in 1999. Ook zei hij: 'Naarmate het web groeide, nam de sofisticatie van de gebruikers af. Het was moeilijk om het belang van privacy aan hen uit te leggen.'[117]

De elektronisch geld-start-up van Chaum ging ten onder. De CyberBucks-server voor dubbele uitgaven ging ook offline. Zonder deze server was er geen manier om te weten welke valutaeenheden nog geldig waren. Het betekende, simpel gezegd, het einde van het experiment. Degenen die nog steeds CyberBucks bezaten, bleven achter met niets anders dan een stel waardeloze nummers op hun computer.

Hieruit hebben alle betrokkenen bij het nicheproject voor digitaal geld een waardevolle les getrokken. Hoewel blinde handtekeningen een zekere mate van privacy garandeerden, bleek de afhankelijkheid van CyberBucks van een vertrouwde partij in de vorm van DigiCash de fatale fout van het project te zijn.

Rond deze tijd probeerde iemand anders, toevallig en om een heel andere reden, een zeer vergelijkbaar soort fout te herstellen…

---

117 Julie Pitta, *Requiem for a Bright Idea*, Forbes, 1 november 1999, online

Scott Stornetta

Vers van de Stanford Universiteit met een PhD in natuurkunde, was Scott Stornetta enthousiast om zijn nieuwe baan te beginnen bij wat in 1989 het epicentrum van computerwetenschappelijke innovatie was: het in New Jersey-gevestigde telecom onderzoekscentrum Bellcore.

Bellcore had in feite de leiding over de architectuur van een groot deel van de Amerikaanse telecommunicatiesystemen in een periode waarin de informatietechnologie zich in een razend tempo ontwikkelde en het internet iedere dag groter werd. Bovendien maakte de cryptografie een ware renaissance door. Ze bevonden zich, zoals Stornetta later omschreef, in een 'gouden tijdperk van onderzoek'. Nieuwe medewerkers kregen zelfs geen specifieke taken toegewezen. De dertigjarige natuurkundige kreeg de instructie om *zelf* te ontdekken wat van belang was en vervolgens zijn aandacht hieraan te geven en hieraan te werken.

Het bleek zo te zijn dat Stornetta al iets belangrijks in gedachten had voordat hij überhaupt een voet in zijn nieuwe werkomgeving had gezet.

Voordat hij naar de oostkust verhuisde, bracht Stornetta enkele jaren door op Stanford, waar hij werkte vanuit het Xerox PARC-onderzoekscentrum in Palo Alto. De divisie van Xerox was een revolutionaire omgeving die baanbrekende innovaties zoals de personal computer, Ethernet en laserprinten mogelijk had gemaakt, maar de afgelopen jaren werd Stornetta ook geconfronteerd met een nieuw en lelijk probleem in het sterk gedigitaliseerde onderzoekscentrum: vervalsingen.

Vervalsing is natuurlijk geen nieuw fenomeen. Mensen hebben in feite geprobeerd om documenten te vervalsen sinds de uitvinding van het schrift. Maar digitale vervalsingen waren een relatief nieuw concept, en Stornetta was gaan geloven dat ze een nog uitdagender probleem vertegenwoordigden. Terwijl fysieke vervalsing vaak sporen achterlaat, kan een digitaal document, of het nu een arbeidscontract is, verzekeringspapieren, of een universitair diploma, smetteloos worden aangepast.

Digitale authenticatie loste inderdaad een deel van dat probleem op: cryptografische handtekeningen konden bewijzen dat een elektronisch document gecontroleerd (ondertekend) was door de juiste persoon. Maar dit zou niet voorkomen dat dezelfde persoon later gewijzigde documenten creëert en ondertekent. Je kan geen onderscheid maken tussen een oude bit en een nieuwe bit, dus hoe kan iemand

ooit zeker zijn dat ze kijken naar een origineel document in plaats van een latere vervalsing?

Stornetta voorzag een crisis in geloofwaardigheid en besloot zijn eerste periode bij Bellcore te besteden aan het oplossen van dit probleem.

Hij had ook al een mogelijke oplossing in gedachten. Stornetta wilde een tijdregistratiesysteem voor digitale documenten ontwerpen. Het is veel moeilijker om met een vervalsing weg te komen als mensen kunnen bewijzen dat het originele document op een eerder moment in de tijd bestond.

Stornetta had nog niet precies uitgevogeld hoe zo'n tijdregistratiesysteem zou werken, maar hij vermoedde dat cryptografie wel eens een belangrijk deel van de oplossing kon zijn. Hoewel hij zelf geen cryptograaf was, had hij het geluk dat de cryptograaf van Bellcore, Stuart Haber, tevens degene die Stornetta bij Bellcore in dienst nam, erin toestemde om met hem aan dit project te werken.

In de daaropvolgende weken brainstormden Stornetta en Haber over ideeën, speculerend over mogelijke strategieën om de uitdaging waarvoor zij stonden op te lossen.

Hash-ketens

Een van hun meest veelbelovende ideeën maakte gebruik van een hash-functie[118], een eenrichtingsfunctie die data omzet in een unieke en ogenschijnlijk willekeurige reeks cijfers van een vaste lengte. Alle digitale data kan worden gehasht, of het nu een enkele letter is, een heel boek, een muziekbestand of de broncode van een programma. Het cruciale aspect is dat dezelfde data altijd hetzelfde gehashte resultaat oplevert, maar zodra de oorspronkelijke data ook maar een beetje verandert, is de resulterende hash totaal anders. Verwijder je bijvoorbeeld een enkele komma uit een boek, dan lijkt de nieuwe hash totaal niet meer op die van het oorspronkelijke boek.

Stornetta en Haber stelden voor om documenten van een tijdstempel te voorzien via een speciale tijdstempeldienst. Een document werd samen met een tijdcode gehasht, die vastlegt wanneer de dienst het document heeft ontvangen.

118 Hash-functies werden voor het eerst voorgesteld door de wiskundige George B. Purdy van de University of Illinois at Urbana-Champaign in zijn artikel *A High Security Log-in Procedure*, Communications of the ACM 17, no. 8: 442–445.

Deze hash werd vervolgens cryptografisch ondertekend door de tijdstempelserver als een soort bewijs. Om aan te tonen dat een document op een bepaald moment bestond, kon de eigenaar het originele document en de tijdstempel tonen. Iedereen kon dit invoeren in een hashfunctie om te verifiëren dat er inderdaad een identieke hash door de tijdstempelserver was ondertekend.

Daarnaast speculeerden Stornetta en Haber dat verschillende documenten chronologisch gekoppeld konden worden in een hash-keten. Dit betekent dat elk nieuw document dat de tijdstempeldienst ontving, niet alleen werd gehasht met een tijdcode, maar ook met de hash van het vorige document. Deze nieuwe hash werd vervolgens samen met het volgende document gehasht, en zo ontstond een keten van hashes. Deze 'keten' kon precies bewijzen welke documenten in welke volgorde waren getijdstempeld, en zou zo een chronologisch *ruggengraatregistratie* vormen van alle verwerkte documenten.

Dit bracht echter met zich mee dat de tijdstempeldienst zelf te vertrouwen moest zijn om niet te rommelen met het centrale archief. In theorie kon deze dienst vervalsingen creëren door dezelfde documenten te hashen en ondertekenen met verschillende tijdstempels. Zo kon de chronologische volgorde van documenten worden gewijzigd, of konden documenten zelfs volledig uit het archief verdwijnen.

In de wereld van de informatica was het destijds vrij normaal om op zulke diensten te vertrouwen. Publieke sleutels werden bijvoorbeeld meestal verstrekt door een certificaatautoriteit die deze sleutels koppelde aan specifieke identiteiten. Voor Stornetta en Haber was dit echter geen ideale oplossing. Zij vonden dat veiligheid in de digitale ruimte niet afhankelijk zou moeten zijn van vertrouwen in een specifieke entiteit of persoon. Net zoals de cryptografische hulpmiddelen waarover zij beschikten, moest tijdstempeling idealiter onafhankelijk kunnen functioneren.

Dit bleek het meest uitdagende deel van het probleem te zijn.

Zolang één entiteit de tijdstempelservice verzorgde, was er altijd vertrouwen in die ene partij nodig. Het toevoegen van meerdere entiteiten om zo een systeem van *checks-and-balances* te creëren, bood ook geen oplossing. Zelfs als iemand de taak had om de eerlijkheid van de tijdstempeldienst te bewaken, bleef er een risico dat deze persoon samenspande met de dienst om de records te wijzigen. Om dezelfde reden bood het toevoegen van een derde, vierde of vijfde persoon

als toezichthouder geen garantie. Dit vergrootte hoogstens de omvang van de samenzwering die nodig was om historische records te vervalsen, maar sloot de mogelijkheid van vervalsing niet volledig uit.

Stornetta en Haber leken tegen een fundamenteel probleem te zijn aangelopen dat cryptografie niet kon oplossen. Na weken van vruchteloze brainstormsessies zagen de collega's van Bellcore uiteindelijk geen andere optie dan te concluderen dat wat ze echt wilden bereiken niet mogelijk was.

Als een soort van troost, besloten ze hun bevindingen te publiceren. Ook al hadden Stornetta en Haber het vertrouwensprobleem niet opgelost, ze konden nu tenminste aantonen dat dit probleem onoplosbaar was…

Het verdelen van vertrouwen

Pas toen Stornetta beargumenteerde dat het probleem onoplosbaar was, besefte hij dat ze daadwerkelijk fout zaten — althans technisch gezien.

Stornetta en Haber hadden geconcludeerd dat het toevoegen van meer entiteiten om controles uit te voeren op de tijdstempeldienst het probleem van vertrouwen niet oplost, maar alleen verandert hoe groot de samenzwering zou moeten zijn. Inderdaad, dit lijkt logischerwijs waar te zijn, en in de meeste gevallen is het inderdaad waar.

Maar Stornetta kwam nu tot het inzicht dat er een uitzondering op deze regel is: als iedereen de tijdstempeldienst controleert, kan niemand samenspannen: er zou niemand meer over zijn om tegen te samenzweren. Zolang iedereen iedereen in de gaten houdt, is er helemaal geen vertrouwde partij meer nodig!

Stornetta stelde: 'Als we in essentie een samenzwering kunnen creëren die zo groot is dat het de hele wereld omvat, dan zouden we in feite het probleem hebben omgekeerd en een systeem zonder vertrouwen hebben gecreëerd.'[119]

Het is uiteraard onwaarschijnlijk dat de groep die op vervalsingen controleert zo groot wordt dat letterlijk iedereen op aarde erbij hoort. Desalniettemin, deze nieuwe inzichten betekenden een echte doorbraak in het denken van Stornetta en Haber.

---

119 Scott Stornetta, *The Missing Link between Satoshi & Bitcoin: Cypherpunk Scott Stornetta*, interview by Naomi Brockwell, NBTV, with Naomi Brockwell, YouTube, 6 september 2018, online

Dit resulteerde uiteindelijk in de publicatie van hun onderzoek uit 1990: 'Hoe plaatst men een tijdstempel op een digitaal document?'[120] De paper stelde nieuwe normen in het domein van digitale tijdstempels en presenteerde twee enigszins verschillende benaderingen.

Het eerste voorstel leek sterk op hun idee van een hash-keten ruggengraatregistratie, waarbij de tijdstempeldienst elk update cryptografisch zou ondertekenen en chronologisch aan het record zou linken. Dit zou bewijzen dat het daadwerkelijk de tijdstempeldienst was die het nieuwe document toevoegde, en in welke volgorde. Maar belangrijk was dat in plaats van enkel de tijdstempeldienst te vertrouwen met het ruggengraatregistratie, dit nu met alle deelnemers gedeeld zou worden.

Het geniale van deze oplossing was dat als de tijdstempeldienst ooit zou proberen om te antidateren, te deleten of een eerder getijdstempeld document op een of andere manier te veranderen, elke gebruiker die een kopie van de ruggegraatrecord behield, de verandering zou opmerken. Als de inhoud of de tijdcodes van een document zelfs maar een klein beetje gewijzigd werd, zou dit de bijbehorende hash volledig veranderen, wat op zijn beurt weer elke volgende hash zou veranderen, waardoor het volledig onverenigbaar zou worden met de wijdverbreide record: de tijdstempeldienst zou nooit wegkomen met zijn vervalsingspoging.

De tweede oplossing die Stornetta en Haber beschreven, schafte zelfs de tijdstempeldienst volledig af. In deze variant, zou een groep deelnemende gebruikers om de beurt een nieuw document aan de hash-keten toevoegen. Wanneer iemand een document wilde voorzien van een tijdstempel, zou de willekeur van de hash van dit document worden gebruikt om te bepalen welke deelnemer het moest ondertekenen, als een soort hash-loterij.

Met niet één, maar twee briljante voorstellen, waarvan er één nog minder vertrouwen vereiste dan de andere, vormde de paper van Stornetta en Haber een grote sprong voorwaarts voor het digitaal tijdstempelen.

Dat gezegd hebbende, brachten hash-ketens wel een nieuw probleem met zich mee: ze waren niet bijzonder schaalbaar, vooral als je rekening hield met de

120 Stuart Haber and Scott W. Stornetta, *How to Time-Stamp a Digital Document*, Journal of Cryptology 3: 99–111.

bescheiden rekenkracht die een gemiddelde computergebruiker begin jaren '90 ter beschikking had. Voor elk document dat aan het hoofdrecord werd toegevoegd, was er een nieuwe hash nodig, dus na verloop van tijd zouden de deelnemende gebruikers heel wat data moeten opslaan als deze systemen echt populair zouden worden.

En aangezien deze gebruikers steeds meer data moesten opslaan om deel te kunnen nemen, zouden waarschijnlijk meer van hen ervoor kiezen om niet meer deel te nemen en gewoon het record te vertrouwen dat door de tijdstempeldienst en andere gebruikers wordt bijgehouden. Dit zou op zijn beurt weer (de nood aan) vertrouwen in deze systemen introduceren: om echt veilig te zijn, was het tijdstempelschema uitdrukkelijk afhankelijk van brede deelname.

Het was wiskundige Dave Bayer die dit raadsel hielp oplossen, met behulp van *Merkle Trees*.

Een boom van hashes

In de jaren na het afronden van zijn stage bij Martin Hellman, had Ralph Merkle een naam voor zichzelf gemaakt als een van de vooraanstaande cryptografen van zijn generatie. Onder zijn vele innovaties had hij een nieuwe eenrichtingsfunctie ontworpen, een sneller versleutelingsprotocol geïntroduceerd en zijn eigen handtekeningsalgoritme voorgesteld. Hoewel hij technisch gezien niet medeauteur was van het onderzoek, zagen veel cryptografen Merkle als de derde uitvinder van de Diffie-Hellman-sleuteluitwisseling.

Het meest opvallende is misschien wel dat Merkle in 1979 de Merkle Tree had uitgevonden.[121] Oorspronkelijk ontworpen als onderdeel van een systeem voor het produceren van authenticatiecertificaten voor een raadpleegbare lijst van publieke sleutels, bieden Merkle-bomen een compacte en veilige controle op de inhoud van allerlei soorten gegevenssets door hashes op een slimme wiskundige manier te combineren.

Concreet genomen, aggregeert een Merkle-boom verschillende stukken data cryptografisch via een aantal eenvoudige stappen. Allereerst worden de verschil-

121 Ralph C. Merkle, *A Certified Signature*, Advances in Cryptology — CRYPTO '89: Proceedings: 218–238.

lende stukken individueel gehasht, zodat elk stuk data zijn eigen unieke hash heeft. Vervolgens worden al deze hashes in paren van twee gegroepeerd. Elk paar hashes wordt dan samen gehasht, wat één nieuwe hash per paar produceert. Al de nieuwe hashes worden dan opnieuw gepaard, en deze paren worden weer samen gehasht. Dit proces herhaalt zich totdat er nog maar één hash over blijft, de zogenaamde *Merkle-wortel* (gevisualiseerd, lijkt de resulterende datastructuur op een soort stamboom, maar dan voor grote getallen in plaats van personen).

Merkle-bomen vergemakkelijken controles om te zien of de hash van een specifiek stuk data in de boom is opgenomen. Belangrijk is dat dit mogelijk is zonder dat men de overige data die gecodeerd werd, noch zelfs de meeste andere hashes, hoeft te zien. Alles wat nodig is, is een *Merkle-bewijs*, dat bestaat uit de relevante 'takken' van de boom. Dit dient in wezen als een compacte set van 'aanwijzingen' om het pad te vinden van de Merkle-wortel naar de hash van het specifieke stuk data.

Ondertussen is het strikt onmogelijk om iets in een boom te bewerken of te verwijderen zonder de hele boom te veranderen of, nauwkeuriger, zonder de wortel te veranderen. Als een stukje data wordt gewijzigd of verwijderd, zou de overeenkomstige hash ook veranderen, wat op zijn beurt noodzakelijkerwijs de weergave van zijn 'kind'-hash beïnvloedt, wat natuurlijk de volgende hash beïnvloedt, en zo verder, helemaal tot aan de wortel van de boom. Niet ongelijk aan hash-ketens tonen Merkle-bomen ondubbelzinnig aan of data is gewijzigd, maar dan in een veel compacter formaat.

Het zou een waardevol middel blijken te zijn in de strijd tegen digitale fraude.

Een keten van wortels

Goed bekend met de vele cryptografische voorstellen die in de anderhalf decennium vóór de publicatie van Stornetta en Habers eerste paper zijn geïntroduceerd, stelde Bayer aan de onderzoekers van Bellcore voor dat ze Merkle's hash-structuur konden gebruiken voor tijdstempels, wat het duo met plezier accepteerde. Hun tweede paper, *Improving the Efficiency and Reliability of Digital Time-Stamping*, werd

gepubliceerd in 1993, en Bayer werd opgenomen als derde auteur.[122]

Stornetta, Haber en Bayer stelden voor om meerdere documenten tegelijkertijd te tijdstempelen door ze te bundelen in één grote Merkle-boom, die dagelijks werd aangemaakt. Gebruikers hoefden dan niet voor elk getijdstempeld document een afzonderlijke hash bij te houden. In plaats daarvan volstond het om enkel de dagelijkse Merkle-wortel als basisregistratie te bewaren, samen met hun eigen Merkle-bewijzen om de hash van hun documenten in de betreffende boom te vinden.

Dit verbeterde de efficiëntie aanzienlijk, waardoor meer gebruikers konden deelnemen aan het tijdstempelproces. Het werd zelfs mogelijk om de dagelijkse Merkle-wortel te publiceren in een krant, waar deze publiek zichtbaar zou zijn en bewaard kon worden in fysieke krantenarchieven (Stornetta en Haber richtten later de tijdstempel-start-up *Surety* op, die inderdaad Merkle-wortels opnam in de geclassificeerde advertenties van de New York Times).

Daarnaast kan, zoals verder uitgewerkt in hun derde paper Secure Names for Bit-Strings[123], elke nieuwe Merkle-boom de vorige Merkle-wortel bevatten. Dit creëerde een reeks Merkle-wortels die zelf een chronologische hash-keten vormden. Bij het dagelijks creëren van een Merkle-boom werd de Merkle-wortel van gisteren opgenomen in de boom van vandaag, en de wortel van vandaag werd op zijn beurt verwerkt in de boom van morgen, enzovoort.

Op deze manier waren ook de Merkle-bomen zelf cryptografisch met elkaar verbonden. Vervalsing werd hierdoor nog moeilijker. Zelfs als iemand erin zou slagen om bijvoorbeeld één editie van de *New York Times* in het fysieke archief te vervalsen met een andere Merkle-wortel, zou dit niet overeenkomen met de Merkle-wortels die in alle kranten sinds die tijd zijn gepubliceerd, en ook niet met de persoonlijke archieven van mensen. Deze methode maakte het bijna onmogelijk om gegevens te vervalsen.

Als iemand zou proberen een document te antidateren, zou dit niet alleen de Merkle-wortel van die specifieke dag veranderen, maar het zou ook in strijd

122 Dave Bayer, Stuart Haber and Scott W. Stornetta, *Improving the Efficiency and Reliability of Digital Time-Stamping*, Conference Paper, Sequences II: Methods in Communication, Security, and Computer Science: 329–34.

123 Stuart Haber and Scott W. Stornetta, *Secure Names for Bit-strings*, CCS '97: Proceedings of the 4th ACM Conference on Computer and Communications Security,: 28–35.

zijn met elke tijdstempelregistratie die daarna is gepubliceerd. Vervalsing werd daarmee in de praktijk onmogelijk. Feitelijk ontwierpen Scott Stornetta en Stuart Haber hiermee een systeem voor historische gegevensverificatie.

De sleutel tot hun succes, was de verdeling van vertrouwen.

Hoofdstuk 7

De Extropianen

Friedrich Hayek wilde geld denationaliseren en David Chaum wilde het anoniem maken. Hoewel zowel de econoom als de cryptograaf een revolutionair idee hadden, hadden ze niet helemaal hetzelfde doel voor ogen.

Ze inspireerden echter wel dezelfde man.

Max O'Connor is opgegroeid in het bescheiden Britse stadje Bristol tijdens de jaren '60 en '70. Al op jonge leeftijd werd zijn fantasie geprikkeld door echte gebeurtenissen, zoals de maanlanding die hij op vijfjarige leeftijd op televisie gadesloeg, alsook door de fictieve verhalen uit de stripboeken die hij verslond. Hij droomde van een toekomst waarin de mensheid haar mogelijkheden op sciencefiction-achtige wijze zou uitbreiden. Hij fantaseerde over een wereld waarin mensen over röntgenvisie beschikten, desintegratiepistolen bij zich droegen en in staat waren dwars door muren te lopen.

In zijn tienerjaren had O'Connor een interesse in het occulte ontwikkeld. Hij dacht dat de sleutel om bovenmenselijk potentieel te realiseren misschien te vinden was in hetzelfde veld als astrale projectie, wichelroedelopen en reïncarnatie. Om deze mogelijkheden te onderzoeken, richtte hij de club voor Psychische Ontwikkeling en Onderzoek op bij zijn school, waar hij en zijn mede-junior-occultisten het bovennatuurlijke bestudeerden.

Maar O'Connor, die rond deze tijd bijzonder geïnteresseerd raakte in levensverlenging, vond niet precies wat hij zocht. Hij kwam tot het besef dat er consequent overtuigend bewijs ontbrak dat enige van de mystieke praktijken daadwerkelijk

werkten.

De tiener veranderde uiteindelijk volledig van gedachten over het occulte en kwam tot de conclusie dat er geen waarde te behalen was uit deze overtuigingen en praktijken. In plaats van het bovennatuurlijke, besloot hij dat de vooruitgang van de mensheid het beste gediend was door wetenschap en logica.

Zelfs zonder bovennatuurlijke krachten kon O'Connor zijn eigen potentieel ten minste maximaliseren door hard te werken. Op school was hij een gretige leerling en ook ambitieus, ten minste zolang de onderwerpen in de klas boeiend waren. Hij was vooral geïnteresseerd in onderwerpen over sociale organisatie, en hij slaagde uiteindelijk als beste van zijn economieklas op school.

Al dat harde werk wierp vruchten af toen O'Connor in 1984 werd toegelaten tot de Universiteit van Oxford. Zijn drive om te presteren en het beste uit zichzelf te halen, leek alleen maar toe te nemen op deze prestigieuze universiteit. Hij studeerde gedurende drie aaneengesloten jaren met grote inzet, waarbij hij cursussen volgde in politiek, economie en filosofie. Op zijn drieëntwintigste had hij in alle drie de disciplines een graad behaald.

Op dat moment was het tijd voor een verandering van omgeving. Als jong volwassene, wilde de verse Oxford-afgestudeerde schrijver worden, maar de oude universiteitsstad met haar vochtig klimaat, donkere winters en traditionele Britse waarden, bood hem niet de energie of inspiratie die hij zocht. Het was tijd om ergens anders heen te gaan, naar een nieuwe plek… een opwindende plek.

In 1987 vond O'Connor zijn nieuwe bestemming toen hij een beurs ontving om een PhD-programma in filosofie te volgen aan de Universiteit van Zuid-Californië. Hij verhuisde naar Los Angeles.

Bij aankomst in de Gouden Staat voelde O'Connor zich meteen thuis. Het zonnige weer van Los Angeles was een duidelijke verbetering ten opzichte van het sombere Oxford, en in scherp contrast met de conservatieve mentaliteit die heerste in Groot-Brittannië, stimuleerde het culturele klimaat aan de westkust van Amerika ambitie en het streven naar succes: Californiërs vierden prestaties, ze hadden respect voor het nemen van risico's, en ze prezen degenen die verandering teweegbrachten.

Hier zou O'Connor een nieuw leven beginnen, als een nieuwe man.

Om de nieuwe start te markeren, besloot hij zelfs zijn naam te veranderen: vanaf dat moment zou Max O'Connor door het leven gaan als *Max More*.

'Het leek echt de essentie van wat mijn doel is te vatten: altijd verbeteren, nooit stilstaan', legde hij later uit. 'Ik zou beter worden in alles, slimmer, fitter en gezonder worden. Het zou een constante herinnering zijn om vooruit te blijven gaan.'[124]

FM-2030

Het uitbreiden van menselijk potentieel en specifiek levensverlenging waren nooit echt populaire onderwerpen in Engeland. Maar in Californië ontdekte Max More dat hij niet de enige was met interesse in deze thema's.

Een van Max More's collega's aan de Universiteit van Zuid-Californië (USC) was een in België geboren Iraans-Amerikaanse auteur en leraar. Deze persoon werd geboren als Fereidoun M. Esfandiary, maar stond beter bekend onder de naam *FM-2030*. Gedurende de jaren '70 en '80 was hij druk bezig met het populair maken van een radicaal futuristische visie voor de mensheid.

Geïnspireerd door wereldwijde protestbewegingen in de jaren '60, waar hij mensen uit alle hoeken van de wereld zag opstaan tegen overheidsfraude en sociale onrechtvaardigheid, begon FM-2030 zich een toekomst voor te stellen waarin de mensheid grenzen zou overstijgen om een universele dialoog te vestigen, vrij van nationaliteit, politiek en erfdeel. Om dit te verwezenlijken, begon hij high-tech woningen en levenswijzen te bevorderen, zodat mensen in een onderling verbonden mondiale gemeenschap kunnen leven.

Bovendien, zo voorspelde FM-2030, zou de ontwikkeling van nieuwe technologieën ingenieurs de instrumenten geven om de wereld dramatisch ten goede te veranderen. Hij geloofde dat eventuele risico's verbonden aan technologische innovatie gecompenseerd zouden worden door de voordelen van vooruitgang: zonne- en atoomenergie zouden zorgen voor een overvloed aan energie, mensen zouden Mars koloniseren, robotwerkers zouden onze vrije tijd verhogen, en mensen zouden in staat zijn om vanuit het comfort van hun eigen huizen hun brood te verdienen dankzij de komst van telewerken.

Nog interessanter is dat FM-2030 voorspelde dat technologie binnenkort het punt zou bereiken dat het mensen zelf drastisch zou kunnen verbeteren.

124 Ed Regis, *Meet the Extropians*, Wired, 1 oktober 1994, online

Gezondheidszorg zouden aanzienlijk verbeteren aangezien meer ziekten genezen, en genetische fouten gecorrigeerd konden worden: toekomstige farmaceutica zou het menselijk potentieel kunnen verhogen door bijvoorbeeld de hersenactiviteit te verbeteren.

Uiteindelijk verwachtte hij dat de medische wetenschap zelfs in staat zou zijn het ouder worden te *genezen*, en dus dat eindige menselijke levensduur geen probleem meer zou zijn. Volgens FM-2030 zou de mensheid rond zijn honderdste verjaardag in het jaar 2030 de dood overwinnen. Het getal in zijn naam verwijst naar dit idee (*FM* stond dan weer voor verschillende benamingen zoals *Future Man*, *Future Marvel*, of *Future Modular* — en soms iets anders, afhankelijk van zijn stemming of wie het hem vroeg).

Omdat traditionele beperkingen op het menselijk potentieel, zoals eindige levensduur, zouden worden weggenomen terwijl bionische lichaamsdelen en andere kunstmatige verbeteringen steeds meer nieuwe mogelijkheden zouden ontgrendelen, voorspelde FM-2030 dat mensen uiteindelijk het meest radicaal zouden transformeren en zichzelf zouden omvormen tot synthetische, post-biologische organismen.

> *'Het is slechts een kwestie van tijd voordat we onze lichamen herschikken tot iets totaal anders, iets dat beter is aangepast aan de ruimte, iets dat levensvatbaar zal zijn in ons zonnestelsel en zelfs daarbuiten.'*[125]

Transhumanisme

FM-2030 was overtuigd dat technologische vooruitgang uiteindelijk de menselijke ervaing zou veranderen: de mensheid zou zichzelf upgraden om een nieuwe, verbeterde versie van de soort te creëren. Technologie zou een post-menselijke toestand tot stand brengen.

Voor velen klonken deze voorspellingen eerder fantastisch. Maar toen K. Eric Drexler, een onderzoeksmedewerker bij het *MIT Space Systems Laboratory*, rond dezelfde tijd een techniek beschreef voor het vervaardigen van machines op moleculair niveau, begon het fantastische al wat minder onwaarschijnlijk te klinken.

125 Douglas Martin, *Futurist Known as FM-2030 Is Dead at 69*, The New York Times, 11 juli 2000, online

Drexler was van mening dat nanotechnologie industrieën zoals computergebruik, ruimtevaart en productie, evenals oorlogvoering, fundamenteel kon veranderen.

Inderdaad, Drexler geloofde dat nanotechnologie ook de gezondheidszorg kon revolutioneren. Hij legde uit dat fysieke afwijkingen meestal veroorzaakt worden door verkeerd geordende atomen en stelde een toekomst voor waarin nanobots het menselijk lichaam binnen konden gaan om deze schade met ongeëvenaarde precisie te herstellen, waardoor het lichaam in wezen van binnenuit volledig kon genezen.

Als zodanig zou nanotechnologie in staat zijn om zo ongeveer elke ziekte te genezen, en uiteindelijk het leven zelf te verlengen, speculeerde Drexler.

'Veroudering is in wezen niet anders dan elke andere fysieke aandoening', schreef Drexler in zijn boek *Engines of Creation* uit 1986, 'het is geen magisch effect van kalenderdatums op een mysterieuze levenskracht. Broze botten, gerimpelde huid, lage enzymactiviteiten, trage wondgenezing, slecht geheugen, en de rest zijn allemaal het gevolg van beschadigde moleculaire machines, chemische onevenwichtigheden en verkeerd geordende structuren. Door alle cellen en weefsels van het lichaam weer een jeugdige structuur te geven, zullen reparatiemachines de jeugdige gezondheid herstellen.'[126]

Dit waren precies het soort ideeën die Max More als geen ander wisten te boeien.

Bovendien waren deze ideeën voor More niet enkel grappige speculaties. Hij was ervan overtuigd dat de soort voorspellingen die FM-2030 en Drexler deden, beschouwd verdienden te worden als iets fundamentelers. Hij was ervan overtuigd dat ze een nieuw perspectief boden op het menselijk bestaan, en zelfs op de realiteit zelf. Terwijl More de concepten van de futuristen verzamelde, bestudeerde en overdacht, formuleerde de PhD-kandidaat ze uiteindelijk tot een nieuw en onderscheidend filosofisch kader: *transhumanisme*.

Het algemene idee en de term *transhumanisme* werden al in de jaren '50 gebruikt door evolutionair bioloog Julian Huxley, maar het was More die het nu echt vestigde als een bijgewerkte versie van de humanistische filosofie. Net als het humanisme, respecteert het transhumanisme rede en wetenschap, terwijl het geloof, aanbidding en bovennatuurlijke concepten als een hiernamaals verwerpt.

126 K. Eric Drexler, *Engines of Creation*, 146.

Maar waar humanisten waarde en betekenis halen uit de menselijke natuur en het bestaande menselijke potentieel, zouden transhumanisten vooruit kijken en pleiten voor het overstijgen van de natuurlijke beperkingen van de mensheid.

'Transhumanisme', vatte More kort samen, 'verschilt van humanisme doordat het de radicale veranderingen erkent en voorziet in de aard en mogelijkheden van ons leven als gevolg van diverse wetenschappen en technologieën zoals neurowetenschap en neurofarmacologie, levensverlenging, nanotechnologie, kunstmatige ultra-intelligentie, en ruimtebewoning, gecombineerd met een rationele filosofie en waardesysteem.'[127]

Extropianisme

Alle transhumanisten willen het menselijk potentieel verbeteren. Echter, ondanks dat ze hetzelfde doel hebben, realiseerde Max More zich dat verschillende transhumanisten zeer uiteenlopende benaderingen kunnen voorstaan om dit doel te bereiken.

More geloofde zelf in een positieve, levendige en dynamische benadering van transhumanisme. Hij gaf de voorkeur aan een boodschap van hoop, optimisme en vooruitgang. Maar hij geloofde niet dat deze vooruitgang afgedwongen of zelfs gepland kon worden. Hij verwierp de Star Trek-achtige versie van de toekomst waarin de mensheid onder een enkele, alwetende, wereldregering valt die de soort vooruit moet leiden.

More was van mening dat transhumanisten konden profiteren van de inzichten van Friedrich Hayek.

Technologische innovatie vergt kennis en middelen, en Hayek had uitgelegd dat die kennis van nature verspreid is over de hele samenleving, terwijl middelen het best over de economie worden verdeeld door vrijemarktprocessen. Als mensen gewoon de vrijheid krijgen om te experimenteren, te innoveren en samen te werken op hun eigen voorwaarden, bedacht More, dan zou technologische vooruitgang vanzelf ontstaan.

Met andere woorden, een welvarender *morgen* werd het best gerealiseerd als de samenleving zichzelf *vandaag* als een spontane orde kon organiseren.

127 Max More, *Transhumanism: Towards a Futurist Philosophy*, maxmore.com, geraadpleegd online

More vond een vroege bondgenoot in mede USC-student Tom W. Bell. Net als More, omarmde Bell de transhumanistische filosofie en gaf hij de voorkeur aan More's vreugdevolle en vrije benadering om het te bereiken. Hij besloot dat hij zou bijdragen aan de verspreiding van deze relatief nieuwe ideeën door erover te schrijven onder zijn nieuwe pseudoniem: Tom Morrow.

En om hun visie te concretiseren, introduceerde Morrow de term *extropie*. Als tegenhanger van *entropie*, het proces van afbreuk en van verval, stond extropie voor verbetering en groei, zelfs oneindige groei. Degenen die, zoals Max More en Tom Morrow, deze transhumanistische visie onderschreven, zouden als Extropianen worden beschouwd.

Vervolgens schreef More de fundamentele beginselen van de Extropiaanse beweging uit in enkele pagina's tekst, getiteld *The Extropian Principles: A Transhumanist Declaration*. Het bevatte vijf hoofdrichtlijnen of, inderdaad, principes: *grenzeloze uitbreiding, zelftransformatie, dynamisch optimisme, intelligente technologie*, en — als een expliciete knipoog naar Hayek — *spontane orde*. In het kort, de principes (in het engels) vormden het acroniem B.E.S.T. D.O. I.T. S.O.

'Voortdurende verbeteringen betekenen dat we de natuurlijke en traditionele beperkingen van menselijke mogelijkheden uitdagen', vatte More de doelen van de beweging samen in De Extropiaanse Principes. 'Wetenschap en technologie zijn essentieel om beperkingen op levensduur, intelligentie, persoonlijke vitaliteit en vrijheid uit de weg te ruimen. Het is absurd om slaafs de *natuurlijke* grenzen aan onze levensduur te accepteren. Het leven zal waarschijnlijk verder gaan dan de grenzen van de aarde - de geboorteplaats van biologische intelligentie - om het heelal te bewonen.'[128]

Net als de transhumanistische visie die eraan ten grondslag lag, was de Extropiaanse toekomst ambitieus en spectaculair. Naast levensverlenging, wat mogelijk de centrale pijler van de beweging vertegenwoordigde, omvatten de vooruitzichten van Extropianen een breed scala aan futuristische technologieën. Deze variëerden van kunstmatige intelligentie tot ruimtekolonisatie en *mind uploading*, tot menselijk klonen, fusie-energie, en nog veel meer.

Het is belangrijk om te overwegen dat Extropianisme echter geworteld moest

128 Max More, *The Extropian Principles: A Transhumanist Declaration*, maxmore.com, geraadpleegd online

blijven in wetenschap en technologie, zelfs als het vaak over zeer speculatieve versies daarvan ging. In plaats van weg te drijven naar het domein van science-fiction, moesten Extropianen nadenken over hoe ze een betere toekomst kunnen realiseren door middel van kritisch en creatief denken, proactief zijn, en continu leren.

Deze oproep ging over *rationeel individualisme* of *cognitieve onafhankelijkheid*, schreef More. Extropianen moesten leven volgens hun 'eigen oordeel, weloverwogen en geïnformeerde keuzes maken, profiteren van zowel succes als tekortkoming', legde hij uit. Dat vereiste op zijn beurt vrije en open samenlevingen waarin diverse informatiestromen en verschillende zienswijzen de kans krijgen om te bloeien.

Anders gezien, geloven Extropianen dat staten en hun regeringen voornamelijk een obstakel voor vooruitgang vormen. Belastingen beroven mensen van middelen om te produceren en te bouwen, grenzen en andere reisbeperkingen kunnen verhinderen dat mensen zich op de plekken kunnen bevinden waar ze het meeste waarde toevoegen aan de globale samenleving, en overheidsregulaties beperken alleen maar het menselijke vermogen om te experimenteren en innoveren.[129]

'Centraal bevel over gedrag belemmert ontdekking, diversiteit en afwijkende meningen', concludeerde More.[130]

De subcultuur[131]

In de herfst van 1988 publiceerden Max More en Tom Morrow de eerste editie van een nieuw tijdschrift genaamd *Extropy*. Dit markeerde de officiële start van de Extropiaanse beweging.

Hoewel More en Morrow slechts vijftig exemplaren van deze eerste editie hadden gedrukt, wist het tijdschrift al snel wetenschappers, ingenieurs, onderzoekers en andere toekomstgerichte Californiërs uit diverse vakgebieden met elkaar te verbinden. Onder de abonnees waren computertechnici, raket-ingenieurs,

129 De Amerikaanse Food and Drug Administration was een bijzonder restrictief voorbeeld: de federale instelling maakte het knutselen aan en uitproberen van nieuwe soorten medicijnen en geneeskunde zo goed als onmogelijk.

130 More, *Extropian Principles*.

131 Een groot deel van deze sectie is gebaseerd op Finn Brunton's *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Built Cryptocurrency*, 118–134.

neurochirurgen, chemici en nog veel meer. Bovendien bevonden zich onder hen ook enkele opvallende namen, zoals de baanbrekende cryptograaf Ralph Merkle of de Nobelprijs winnende theoretisch fysicus Richard Feynman.

Wat ze gemeen hadden, was een wetenschappelijk geïnspireerd optimisme over de toekomst. Met *Extropy* hadden ze eindelijk een tijdschrift om kennis op te doen over de meest radicale futuristische ideeën die er waren, of ze konden hun eigen radicale ideeën delen als gastauteurs.

Bovendien bood het Extropianisme hen een uniek inzicht in het leven zelf.

Gewapend met een superieure gereedschapskist om het voorheen onverklaarde te verklaren, had de wetenschap in de afgelopen paar eeuwen een groot deel van de greep van religie op de samenleving weggenomen. Maar volgens More zou wetenschap alleen niet voldoende zijn om de religie volledig uit te roeien, omdat het nog een andere belangrijke functie vervult: het geeft mensen een gevoel van betekenis. Mensen houden, ondanks al het bewijs, vast aan religie, betoogde More, voornamelijk omdat ze vertrouwen op hun geloof om door moeilijke tijden heen te komen en zichzelf houvast te geven. En hoewel hij ontdekte dat de meeste religies feitelijk niet zo'n sterk gevoel van vervulling bieden (ze hebben de neiging om mensen onder een aantal krachtige wezens te plaatsen of dit leven te bagatelliseren ten gunste van een hiernamaals) vertegenwoordigde dit toch een vorm van houvast en betekenis.

Om religie volledig weg te werken, moesten mensen een alternatieve bron van zingeving krijgen, geloofde More:

> *'De extropiaanse filosofie kijkt niet buiten ons naar een superieure buitenaardse kracht voor inspiratie. In plaats daarvan kijkt het in ons en voorbij ons, en projecteert het vooruit naar een schitterende visie van onze toekomst. Ons doel is niet God, het is de voortzetting van het proces van verbetering en transformatie van onszelf naar steeds hogere vormen. We zullen onze huidige interesses, lichamen, geesten en vormen van sociale organisatie ontgroeien. Dit proces van expansie en transcendentie is de bron van betekenisvolheid.'*[132]

Dit Extropiaanse perspectief op het leven zou zich in de komende jaren ontwikkelen tot een kleine, lokale subcultuur in Californië, met unieke gewoonten en

132 Max More, *Transhumanism*.

rituelen. De Extropianen hadden hun eigen logo (vijf pijlen die vanuit het midden spiraalsgewijs naar buiten waren gericht, wat groei in elke richting suggereert) en ze kwamen samen in een officieus clubhuis (of *nerd house*) dat Nextropia heette. Ze ontwikkelden hun eigen handruk (het omhoog schieten van hun handen met verstrengelde vingers, net zo lang tot hun armen helemaal uitgestrekt waren: *The sky's the limit*!), ze organiseerden evenementen (waar sommigen van hen Extropiaanse kostuums droegen, bijvoorbeeld door zich als ruimtekolonisten te verkleden), en, onder leiding van Max More en Tom Morrow, veranderden diverse Extropianen hun namen: er was een MP-Infinity, een Skye D'Aureous en iemand die zichzelf R.U. Sirius noemde.

Toen de Extropiaanse gemeenschap uitgroeide van enkele tientallen tot honderden mensen, richtten More en Morrow in 1990 ook het Extropie Instituut op, waarbij FM-2030 zich aansloot als derde oprichtend lid. De non-profit onderwijsorganisatie zou een tweemaandelijkse nieuwsbrief produceren, Extropiaanse conferenties organiseren en (wat voor die tijd vooruitstrevend was) een e-maillijst hosten om online discussie te faciliteren. Hoewel e-mail in die tijd nog een niche technologie was, wisten de technisch onderlegde en toekomstgerichte Extropianen over het algemeen goed hoe ze het ontluikende internet moesten benutten.

Sommigen van hen werkten zelfs aan een bijzonder ambitieus internetnavigatieproject…

De *high-tech* Hayekianen

K. Eric Drexler, wiens werk een belangrijke inspiratiebron was voor Max More, werd niet lang na oprichting lid van de Extropiaanse gemeenschap, net als verschillende van zijn vrienden. Deze vrienden waren technologiefans die graag aan enkele van de meest innovatieve en uitdagende projecten van die tijd werkten.

Een van hen was Mark S. Miller, die destijds de hoofdarchitect was van Xanadu, het allereerste hypertext project ter wereld (Hypertext is de tekst waarop je kunt klikken om je naar verschillende delen van het internet te brengen). Het ambitieuze Xanadu-project, dat al in 1960 werd opgericht, was dertig jaar later

nog steeds in ontwikkeling.

In het kader van de projectontwikkeling publiceerden Drexler en Miller gedurende de jaren '80 diverse artikelen over het toewijzen van rekenkracht over computernetwerken. Kort gezegd, stelden ze voor dat computers in wezen hun overbodige CPU-cycli konden *verhuren* aan de hoogte bieder. Zelfzuchtige computers zouden hun middelen over het netwerk verdelen via virtuele markten om de efficiëntie te maximaliseren, en dat alles zonder de noodzaak van een centrale beheerder. Dit zou het gebruik van rekenkracht waar het het meest gewaardeerd werd mogelijk maken, terwijl het investeringen in meer hardware zou aanmoedigen als de vraag hiertoe voldoende was.

Inderdaad, Drexler en Miller gebruikten Hayeks inzichten over de vrije markt om computernetwerken te ontwerpen.

Drexler en Miller hadden het werk van Hayek bestudeerd op advies van een andere bijdrager aan Xanadu en wederzijdse vriend, Phil Salin. Salin, een futurist met economiediploma's van UCLA en Stanford, vond het leuk om inzichten van de vrije markt te vermengen met de laatste technologische ontwikkelingen. Het meest opmerkelijk was dat hij midden jaren '80 concludeerde dat de tijd rijp was voor het oprichten van een privé ruimtevaartindustrie, en lanceerde één van de meest ambitieuze start-ups van dat decennium in de vorm van het privé ruimtevaartbedrijf Starstruck.

De drie mannen, Drexler, Miller en Salin, werden door het economisch tijdschrift *Market Process* uitgeroepen tot de *high-tech Hayekianen*, een bijnaam die het trio met trots aanvaardde.[133]

AMIX

Ondanks de succesvolle lancering van een raket in de ruimte, eindigde Starstruck als een commerciële mislukking: Salin ontdekte dat de Amerikaanse overheid het praktisch onmogelijk maakte om een ruimtevaartbedrijf te runnen omdat de door de belastingbetaler gesubsidieerde Space Shuttle de markt continu ondermijnde.

Gelukkig was dit niet Salins enige project. Naast het adviseren van Drexler en

133 Don Lavoie, Howard Baetjer, and William Tulloh, *High-Tech Hayekians: Some Possible Research Topics in the Economics of Computation*, Market Process 8: 119–146.

Miller, publiceerde hij ook artikelen en essays over de economische effecten van de computerrevolutie die hij persoonlijk ervaarde,[134] en deze dienden als basis voor nog een ambitieus streven: Salin zou een online marktplaats voor het kopen en verkopen van informatie creëren. Hoewel misschien niet zo spectaculair als het lanceren van raketten in een baan rond de aarde, geloofde hij dat dit project de wereld op nog grotere schaal kon veranderen.

De *American Information Exchange*, kortweg AMIX, was een marktplaats waarbij in principe elk soort informatie verkocht kon worden waar mensen voor wilden betalen. Dat kon advies zijn van een monteur over het weer aan de praat krijgen van een oude auto, computercode voor het automatiseren van de boekhouding van een tandartspraktijk, of misschien wel een ontwerptekening voor een nieuw vakantiehuis in de Florida Keys. Als het informatie was, kon het op AMIX worden verkocht.

Salin was van mening dat het grootste voordeel van AMIX zou bestaan uit een aanzienlijke vermindering van de transactiekosten in de ruimste betekenis van het woord. Dat wil zeggen, alle kosten die verbonden zijn aan het maken van een aankoop, inclusief de zogenaamde opportuniteitskosten (de *kosten* van het mislopen van andere dingen). Zo kan een transactiekost bijvoorbeeld de opportuniteitskost zijn van het doen van marktonderzoek om uit te vinden welke verzekeraar de beste deal biedt, of de kosten van het bellen naar verschillende slijterijen om te weten te komen welke van hen een specifiek merk wijn verkoopt.

Op AMIX konden mensen ervoor kiezen om iemand anders te betalen om de beste verzekeringsmogelijkheid voor hen te vinden, of informatie aan te schaffen over slijterijen en hun voorraden. Als iemand op de informatiehandelsmarkt deze diensten aanbood voor minder geld dan het de potentiële kopers effectief zou kosten om de informatie zelf te vinden, zou de handel via AMIX de transactiekosten van de daadwerkelijke aankopen verminderen. AMIX kon het kopen van verzekeringen, wijn, en vele andere goederen en diensten goedkoper maken door de transactiekosten te verminderen.

Salin was van mening dat de maatschappij enorm baat zou hebben van zo'n efficiëntieverbetering, omdat lagere transactiekosten bepaalde ruilen mogelijk

134 E.g., Phil Salin, *Costs and Computers*, Release 1.0: 5–18; Phil Salin, *The Ecology of Decisions, or 'An Inquiry into the Nature and Causes of the Wealth of Kitchens'*, Market Process 8: 91–114.

zouden maken die anders niet rendabel zouden zijn geweest. Als iemand bijvoorbeeld niet de tijd heeft om een dozijn slijterijen te bellen, zou de mogelijkheid om in plaats daarvan iemand anders een kleine vergoeding te betalen om dit voor hen te doen, kunnen resulteren in de verkoop van nog een fles wijn. Dit zou de wijnkenner, de slijterij en ook de AMIX-onderzoeker beter af maken.

Kortom, meer handel betekent een betere verdeling van hulpbronnen over de economie — spontane orde.

Cryogenica

AMIX was een vooruitstrevend concept. Maar het was ook zijn tijd ver vooruit. Toen AMIX live ging in 1984, hadden Salin en zijn kleine team de marktplaats vanuit het niets opgebouwd. Het reputatiesysteem dat ze ontwikkelden was het eerste in zijn soort, net als hun tool voor de oplossing van geschillen, en aangezien er nog geen online betalingsverwerkers operationeel waren, moesten ze dit ook zelf implementeren. Zelfs websites bestonden op dat moment nog niet, wat betekende dat AMIX-gebruikers hun eigen netwerk moesten opzetten, waarop ze moesten inbellen via *dial-up*-modems, omdat breedbandinternet nog niet bestond. Het is dan ook niet verwonderlijk dat het project traag op gang kwam.

Helaas kreeg Salin de kans niet om AMIX verder te ontwikkelen: kort na de lancering van het project werd bij hem maagkanker vastgesteld. Salin verkocht AMIX uiteindelijk in 1988 aan het softwarebedrijf Autodesk, dat het project, in 1992, net na de dood van de innovatieve Hayekiaan op een leeftijd van eenenveertig jaar, stopzette.

Toch is er voor Extropianen altijd hoop… zelfs in de dood.

Als oneindige levensduur voor de mensheid werkelijk binnen handbereik is, zoals de Extropianen geloven, betekent net voor deze transhumane doorbraak sterven een extra bittere toevoeging aan de tragedie. Met de finishlijn in zicht struikelen, misschien slechts enkele decennia te vroeg, kan het verschil betekenen tussen sterven zoals alle mensen tot nu toe doorheen de geschiedenis hebben gedaan, en eeuwig leven door het ondergaan van de transformatie van de menselijke conditie. Een twintigtal jaren te vroeg sterven, kan betekenen dat je

de eeuwigheid misloopt.

Dit is waarom de Extropianen een noodplan ontwikkelden — een ontsnappingsroute om de kloof te overbruggen. De Extropianen omarmden cryogenica.

Vandaag de dag bewaren vijf faciliteiten verspreid over de VS, China en Europa[135] enkele honderden lichamen en hoofden van overleden individuen door ze te cryopreserveren. Voordat ze stierven, meldden deze mensen zich aan om hun lichamen (of alleen hun hoofden) zo snel mogelijk na klinisch overlijden in te vriezen en op te slaan bij temperaturen onder nul. Meer dan duizend andere mensen hebben zich ook aangemeld om hun lichamen of hoofden te laten conserveren na hun overlijden.

De Extropiaanse voorspelling stelt dat deze individuen misschien op een bepaald moment in de toekomst weer tot leven gebracht kunnen worden. Hoewel ze klinisch dood zijn, wachten de mensen die in biostase worden gehouden in wezen op voortgang van wetenschap en technologie tot op een punt waar ze kunnen worden ontdooid, opgewekt en genezen van welke kwalen dan ook hen hadden verslagen. Ze zouden enkele decennia in de toekomst ontwaken in goede gezondheid, klaar om deel te nemen aan de transhumane toekomst die hen wacht… zo gaat de theorie in ieder geval. Er is, natuurlijk, geen daadwerkelijke garantie dat dergelijke opwekkingen ooit mogelijk zullen zijn. Met de technologie van vandaag is het zeker niet haalbaar. Maar met de technologie van morgen, wie weet?

Zelfs als men inschat dat de kans op succes (zeer) klein is, zou je redelijkerwijs kunnen schatten dat de kans op uiteindelijke herleving groter is dan nul. Dat is een gok die Salin en andere Extropianen bereid waren te nemen.

De overgebleven, levende, Extropianen zullen in de tussentijd gewoon de vlam van het transhumanisme brandend moeten houden.

Digitale valuta

De Extropiaanse beweging was, net zoals Max More zelf, van nature thuis in Californië. Silicon Valley werd begin jaren ’90 steeds meer erkend als de wereldwijde

135 Faciliteiten omvatten Alcor en het Cryonics Institute, Kriorus, Tomorrow Bio en Yinfeng Biological Group.

hotspot voor innovatie. Dit trok enkele van de meest ambitieuze technologen, wetenschappers en ondernemers naar de Amerikaanse westkust.

Maar er was een opmerkelijke uitzondering. In de vroege jaren '90 raakten sommige van de Extropianen ervan overtuigd dat een bijzonder interessante en belangrijke technologie daadwerkelijk werd ontwikkeld door een kleine start-up aan de overkant van de Oceaan. Ze waren van mening dat de realisatie van elektronisch geld cruciaal was, en David Chaum leek alle kaarten in handen te hebben.

Voor ten minste één Extropiaan, een computerwetenschapper genaamd Nick Szabo, was dit een reden om naar Amsterdam te verhuizen en zelf voor DigiCash te gaan werken. Tegelijkertijd begon game-ontwikkelaar Hal Finney het belang van digitaal geld aan zijn mede-Extropianen te propageren, in de hoop dat meer van hen zich erbij zouden aansluiten. Verspreid over zeven pagina's in de tiende editie van Extropy, gepubliceerd begin 1993, beschreef Finney de interne werking van Chaums digitale geldsysteem en legde uit waarom Extropianen met hun libertaire ethos dit ter harte zouden moeten nemen.

'Vandaag zijn we op een pad dat, als er niets verandert, zal leiden tot een wereld met potentieel meer regeringsmacht, bemoeienis, en controle', waarschuwde Finney. 'We kunnen dit veranderen; deze technologieën [van digitaal geld] kunnen de relatie tussen individuen en organisaties revolutioneren, door ze voor het eerst op gelijke voet te zetten. Cryptografie kan een wereld mogelijk maken waarin mensen controle hebben over informatie over zichzelf, niet omdat de overheid hen die controle heeft gegeven, maar omdat zij zelf de enigen zijn die de cryptografische sleutels bezitten om die informatie te onthullen.'[136]

Finney kreeg gelijk: de community deelde over het algemeen zijn zorgen, en zij begrepen waarom elektronisch geld een belangrijk deel van de oplossing vormde. Toen zij meer te weten kwamen over cryptografisch beveiligd geld, begonnen sommige Extropianen bovendien met het idee te spelen dat de potentiële voordelen van elektronisch geld zelfs groter konden zijn dan enkel privacy.

Waar Chaum voornamelijk bezig was geweest met de anonieme functies van digitale valuta, begonnen deze Extropianen ook het potentieel van digitale valuta in het kader van monetaire hervorming in overweging te nemen.

136 Hal Finney, *Protecting Privacy with Electronic Cash*, Extropy 10: 14.

Tegen 1995 bereikte de hernieuwde interesse van de Extropianen een hoogtepunt in een speciale *Extropy*-editie: het vijftiende nummer van het tijdschrift was volledig gewijd aan digitaal geld. De omslag van het tijdschrift bevatte opvallend een blauw-rood achtig ontwerp van een bankbiljet waarop niet een staatshoofd, maar het portret van Hayek te zien was. 'Vijftien Hayeks', luidde de denominatie, en het zou naar verluidt uitgegeven zijn door de 'Virtuele Bank van Extropolis'.

In het tijdschrift bespraken ongeveer de helft van alle artikelen het potentieel van elektronisch geld, met verschillende auteurs die uiteenlopende mening uitdrukten met betrekking tot de digitalisering van geld. Natuurlijk omvatten deze ideeën de bekende privacyfuncties die het ontwerp van Chaum bood. Maar de meeste auteurs gingen ook op verkenning naar aanvullende ideeën.

In zijn *Introduction to Digital Cash*, speculeerde software-ingenieur Mark Grant bijvoorbeeld dat digitaal geld gebruikt kon worden om lokale munteenheden op te zetten. Hij stelde ook een bijzonder pittig alternatief voor om Chaumiaans geld te ondersteunen.

'Net zoals de *personal computer* en de laserprinter het voor iedereen mogelijk hebben gemaakt om een uitgever te worden, maakt digitaal geld het voor iedereen mogelijk om een bank te worden, of ze nu een groot bedrijf zijn of een straathoekdrugsdealer met een laptop en een mobiele telefoon', legde Grant uit. 'Sterker nog, naarmate de nationale schulden blijven toenemen, zouden veel mensen wellicht voordelen zien in het gebruik van contant geld dat wordt gedekt door, laten we zeggen, cocaïne in plaats van contant geld dat louter wordt gedekt door het vermogen van een regering om belastingen te innen.'[137]

Een andere bijdrager, web-ontwikkelaar Eric Watt Forste, schreef een lyrische recensie over het werk van George Selgin, een moderne onderzoeker van de vrije bankenschool, genaamd *The Theory of Free Banking*. In zijn boek doet Selgin nauwgezet verslag van hoe de bankeninfrastructuur zou kunnen evolueren in een omgeving van vrije banken. Watt Forste suggereerde dat dit boek ook als blauwdruk kon dienen voor de digitale wereld.

'Terwijl crypto-experts druk bezig zijn uit te leggen hoe deze banken technologisch zouden kunnen functioneren, legt de theorie van vrij bankieren uit hoe ze economisch zouden kunnen functioneren', concludeerde Watt Forste zijn

137 Mark Grant, *Introduction to Digital Cash*, Extropy 15: 15.

recensie.[138]

Lawrence White, de naaste ideologische bondgenoot van Selgin in de vrije bankbeweging, had zelfs een artikel bijgedragen aan het tijdschrift. Hoewel zijn bijdrage voornamelijk een meer technische vergelijking was tussen elektronische geldschema's en bestaande betaaloplossingen, hintte White ook aan hoe digitale valuta de internationale bankdynamieken drastisch konden veranderen: 'Een belangrijk potentieel voordeel van elektronische geldoverdracht via de persoonlijke computer is dat het gewone consumenten betaalbare toegang tot *offshore*-bankieren kan geven.'[139]

Maar misschien wel het meest opmerkelijke van alles, was het artikel van Max More waarin hij het op zich nam om Hayeks baanbrekende boek over concurrerende valuta samen te vatten en te presenteren.

Geld verder denationaliseren

Het werk van Hayek had het Extropianisme gevormd. Het inzicht van de Oostenrijker in gedistribueerde kennis, vrije markten en spontane orde was een centrale inspiratiebron voor Max More toen hij de organisatorische principes van de beweging formuleerde. Nu vroeg More zijn mede-Extropianen om ook een van Hayeks veel recentere voorstellen te overwegen: een radicaal idee dat tot dan toe beperkte aandacht had gekregen.

De oprichter van de Extropiaanse beweging betoogde voor de denationalisatie van geld.

In zijn artikel toonde More zichzelf een goed onderlegde student van Hayeks werk en een effectieve communicator van diens ideeën. Hij presenteerde een beknopte samenvatting van Hayeks bijdragen aan het bredere debat over monetair beleid en legde uit hoe het fiatgeldsysteem verantwoordelijk was voor vier *economische kwalen*: inflatie, instabiliteit, ongedisciplineerde staatsuitgaven en economisch nationalisme.

Inflatie wordt veroorzaakt door de uitbreiding van de geldvoorraad door de overheid in een Keynesiaanse poging om de werkloosheid te verlagen, legde More

138 Eric Watt Forste, *The Theory of Free Banking* , Extropy 15: 53.

139 Lawrence H. White, *Thoughts on the Economics of 'Digital Currency'*. Extropy 15: 18.

uit, maar in werkelijkheid verstoort dit de economie, verhoogt het de effectieve belastingen en heeft het bovendien een verslavend effect.

Ondertussen wordt onstabiliteit veroorzaakt door manipulatie van de rente door de centrale bank (More vat Hayeks conjunctuurcyclustheorie samen), niet door een inherente instabiliteit in de markt (zoals hij benadrukte dat zowel Keynesianen als Marxisten beweren).

'Economisch nationalisme (of wat Hayek eigenlijk monetair nationalisme noemde), tast bovendien op onnodige wijze verschillende delen van de economie aan op onvoorspelbare en nadelige manieren', schreef More.

En tenslotte, legde More uit, maakte het monetaire systeem ongedisciplineerde staatsuitgaven mogelijk: fiatgeld helpt bij het vergroten van de reikwijdte van de overheid.

'De staat breidt zijn macht grotendeels uit door meer welvaart van productieve individuen te nemen', schreef de Extropiaan. 'Belastingen bieden een manier om nieuwe agentschappen, programma's en macht te financieren. Het verhogen van belastingen wekt weinig enthousiasme op, daarom wenden regeringen zich vaak tot een ander middel van financiering: lenen en uitbreiden van de geldvoorraad.'[140]

Elk van deze kwalen belemmerde economische groei, wat vervolgens de menselijke vooruitgang beperkte. More vat het probleem bondig samen: fiatgeld frustreerde de missie van de Extropians.

More beweerde echter dat de problemen konden worden opgelost. Zoals Hayek in *Denationalisation of Money* had beschreven, was de oplossing om geld over te laten aan de vrije markt. Als het (de facto) staatsmonopolie op geld zou worden afgeschaft, zou concurrentie tussen valuta particuliere valuta-uitgevers stimuleren om werkelijk de meest wenselijke vorm van geld aan te bieden. Inflatie, instabiliteit, ongedisciplineerde staatsuitgaven en monetair nationalisme zouden verleden tijd zijn.

Dat gezegd hebbende, was More zich er ook van bewust dat dit niet gemakkelijk zou zijn. Terwijl Hayek altijd had geloofd dat het overtuigen van regeringen om zijn voorstel over te nemen een zware kluif zou zijn, was de Extropiaan waarschijnlijk nog pessimistischer over dit vooruitzicht dan de Oostenrijkse econoom

140 Max More, *Hayek's Denationalisation of Money*, Extropy 15: 20.

in zijn boek was geweest. Aangezien regeringen het meeste profijt hebben van hun monopolie, hadden ze geen enkele stimulans om het af te schaffen en alle reden om het juist niet te doen.

Maar nu zag More een nieuwe kans. Hij was van mening dat Hayeks visie kon worden gerealiseerd door gebruik te maken van de recente interesse en innovatie rond elektronisch geld. Het was voor overheden kinderspel om een geldmonopolie te handhaven wanneer banken makkelijk te lokaliseren, te reguleren, te belasten, te bestraffen en te sluiten waren, maar wanneer banken *gehost* kunnen worden op persoonlijke computers aan de andere kant van de wereld en kunnen opereren met anonieme digitale valuta, zou de situatie drastisch veranderen.

More dacht dat overheden formeel geen afscheid zouden nemen van het geldmonopolie. Maar, zo redeneerde hij, De juiste combinatie van technologieën kon dit monopolie wel veel lastiger afdwingbaar maken.

Via zijn artikel in het tijdschrift, riep de grondlegger van de beweging op om transactieprivacy en concurrentie in valuta gezamenlijk te overwegen.

'Concurrerende valuta zullen het huidige systeem aftroeven door inflatie te beheersen, de stabiliteit van dynamische markteconomieën te maximaliseren, de omvang van de overheid te beperken en door de absurditeit van de natiestaat te erkennen', schreef More. 'Deze hervorming combineren met de introductie van anoniem digitaal geld zou een mokerslag zijn voor de bestaande orde — digitaal geld maakt het moeilijker voor overheden om transacties te controleren en te belasten.'

Concluderend stelde hij: 'Ik betreur het recente overlijden van Hayek ten zeerste. […] Omdat hij niet in biostase is geplaatst, zal Hayek nooit de dagen van elektronisch geld en concurrerende privévaluta meemaken die zijn denken mogelijk zal helpen realiseren. Als we het voortouw willen blijven nemen in de toekomst, laten we dan kijken wat we kunnen doen om deze cruciale ontwikkelingen te versnellen. Wie weet zien we ooit nog een privévaluta die zijn naam draagt.'[141]

141 More, *Hayek's Denationalisation of Money*, 20.

Deel II

Cypherpunks

Hoofdstuk 8

De Cypherpunk-beweging

Tim May kon een glimp van de toekomst zien. Hij had de gave om als eerste het potentieel van nieuwe technologieën te herkennen en kon voorspellen hoe ze de samenleving zouden beïnvloeden.

Zo zag May al vroeg in hoe belangrijk persoonlijke computers en het internet zouden worden. In 1973 bemachtigde hij al een primitieve DARPA-account op de campus van de UC Santa Barbara, waar hij natuurkunde studeerde. Een jaar later kreeg hij een baan bij Intel, waar hij zou werken in de *Memory Products Division*. Hij was toen 22 jaar.

De jonge natuurkundige leverde een belangrijke bijdrage in de vroege geschiedenis van het bedrijf door het alfadeeltjesprobleem op te lossen: May ontdekte dat de geïntegreerde schakelingen van Intel onbetrouwbaar waren vanwege licht radioactief verpakkingsmateriaal. Dit zette hem op weg naar een geweldige carrière bij de snelgroeiende fabrikant van halfgeleiderchips.

Omdat hij een deel van zijn salaris in de vorm van aandelenopties ontving, had de natuurkundige van Intel ongeveer een decennium later, tegen midden jaren 80, een klein fortuin vergaard: op slechts vierendertigjarige leeftijd concludeerde May dat hij genoeg rijkdom had verzameld om voor de rest van zijn leven te doen wat hij wilde. Hij besloot vroegtijdig met pensioen te gaan en verhuisde naar Santa Cruz, een kustplaats zo'n veertig kilometer ten zuiden van San Jose, Californië. Het grootste deel van het daaropvolgende jaar bracht hij in een comfortabele strandstoel door met boeken over economie, technische papers en

cyberpunkromans.

Cyberpunkverhalen, een relatief nieuw genre in die tijd, speelden zich meestal af in high-tech dystopieën. De boeken schilderden over het algemeen een grimmige versie van de toekomst, maar eentje waarin het internet (of een geëvolueerde versie ervan) een toevluchtsoord bood voor hun vrijheidsgezinde hoofdpersonages. In *True Names* van Vernor Vinge, verbergen een groep hackers zich voor de sterke mannen van de regering door hun pseudonieme avatars vrijelijk te laten rondzwerven door een kleurrijke en driedimensionale representatie van het internet zelf. In *Snow Crash* van Neil Stephenson verloren naties grotendeels hun macht aan grote bedrijven en de maffia, terwijl mensen aan hun miezerig bestaan ontsnapten door in een virtuele wereld alternatieve levens te leiden. En *Neuromancer* van William Gibson presenteert evenzo een wereldwijd verbonden, virtuele realiteitsomgeving als een kleurrijk alternatief voor een vijandige onderwereldmaatschappij.

May was van plan om uiteindelijk zelf een cyberpunkroman te schrijven, gemodelleerd naar Ayn Rands *Atlas Shrugged*. In Rands verhaal, dat oorspronkelijk in 1957 werd gepubliceerd, omarmt een Amerika in verval socialistische doctrines, terwijl het Amerikaanse volk zich afkeert van de meest succesvolle ondernemers van het land. Sommige van deze ondernemers besluiten uiteindelijk om *in staking* te gaan: een kleine gemeenschap van doorwinterde vernieuwers vestigt zich in een afgelegen bergketen genaamd *Galt's Gulch*, waar ze zich verbergen met warmtestralingsschermen en reflectoren. De subtiele boodschap van het boek is dat Amerika's meest ijverige ondernemers niet gedemoniseerd, maar gekoesterd en gevierd zouden moeten worden.

Na het lezen van Rands meesterwerk *Atlas Shrugged* als tiener, had dit boek May op het spoor gezet om meer te leren over vrije markten en libertarisme. Uiteindelijk zou hij zich toeleggen op de studie van de Oostenrijkse economie, en in het bijzonder, op de theorieën van Friedrich Hayek.

Dit alles maakte dat de aspirant-schrijver zich als vanzelfsprekend thuis voelde in een niche subcultuur die in de jaren '80 in Californië opkwam. Via enkele van zijn lokale vrienden leerde May de Extropianen kennen en vond hij een ideologische thuis. Hoewel hij niet volledig mee was met enkele van de meer buitensporige toekomstvisies van de transhumanisten (ideeën zoals eeuwig leven, het uploaden van de hersenen of een AI singulariteit) was hij wel toegewijd aan

vrijheid en technologische vooruitgang.

In deze context raakte Tim May bevriend met Phil Salin, de *high-tech Hayekiaan* die tevergeefs had geprobeerd om een privé-ruimtetransportindustrie op te zetten met zijn start-up *Starstruck*. May en Salin deelden een passie voor zowel de Oostenrijkse economie als technologie. Beiden geloofden dat de voormalige verder kon worden ontwikkeld door de laatste te benutten.

BlackNet

May had ongeveer een jaar met boeken op het strand doorgebracht toen Salin hem vertelde over AMIX, het ambitieuze internetproject waar hij aan werkte. AMIX, legde Salin aan zijn vriend uit, zou een online marktplaats worden voor het kopen en verkopen van informatie. Hij vertelde May hoe dit transactiekosten sterk zou kunnen verlagen, wat enorme voordelen zou opleveren voor de vrije markt. Hij vroeg May wat hij van het idee vond: Salin wilde graag de feedback van zijn vriend horen.

Het concept leek May inderdaad interessant. Maar na er even over na te denken, kwam hij tot de conclusie dat zijn interesse voor heel andere redenen werd gewekt dan die van Salin. May vertelde zijn vriend dat hij dacht dat deskundig advies of winkeltips, de soorten informatie waar Salin aan had gedacht, waarschijnlijk niet echt waardevol zouden zijn. Maar hij geloofde wel dat er een hoge vraag zou zijn naar een heel andere categorie van informatie: geheime informatie.

Mensen zouden bereid zijn om veel geld te betalen voor bedrijfsgeheimen, geclassificeerde overheidsdocumenten, militaire inlichtingen, kredietgegevens, medische dossiers, verboden religieus materiaal of illegale pornografie, stelde May voor.[142] En belangrijk, sommige mensen die toegang hebben tot dit soort informatie zouden bijna zeker bereid zijn om het te verkopen voor de juiste prijs, als ze dat anoniem kunnen doen.

Natuurlijk wist May dat het kopen en verkopen van dit soort informatie in veel gevallen illegaal zou zijn. Als het op AMIX zou worden gezet, zou Salin naar alle waarschijnlijkheid gedwongen worden om de handel ervan te verbieden. Maar

142 Tim May, *Untraceable Digital Cash, Information Markets, and BlackNet*, The Computers Freedom & Privacy Conference, geraadpleegd online

May voorzag dat dit uiteindelijk geen echt verschil zou maken. De ontwikkelingen op het gebied van cryptografie die hij in academische tijdschriften had gelezen, zouden uiteindelijk in handen van mensen komen, legde hij aan Salin uit, dus het was slechts een kwestie van tijd totdat er een volledig anonieme variant van AMIX zou ontstaan waar gebruikers alleen bekend zijn bij hun pseudoniemen, en aankopen werden gedaan met anoniem digitaal geld. May gaf deze vorm van informatiemarkt de naam *BlackNet*.

In de maanden na zijn eerste gesprek met Salin, bleef May nadenken over de bredere implicaties die een dienst als BlackNet met zich mee zou brengen. Door zijn eigen ideeën verder uit te werken, kwam hij tot de conclusie dat anonieme informatiemarkten uiteindelijk het fundamenteel onveilig konden maken voor grote bedrijven om hun medewerkers überhaupt met gevoelige informatie te laten omgaan. Deze medewerkers zouden immers altijd in de verleiding kunnen komen om een extra zakcentje te verdienen door de data online te verkopen.

Volgens May zou dit een soort catch-22 situatie kunnen introduceren. Bedrijfsgeheimen zouden bedrijven vermoedelijk een voorsprong op hun concurrenten geven als ze op grote schaal binnen het bedrijf worden gebruikt, maar in dat geval zou het waarschijnlijk slechts een tijdelijke voorsprong zijn voordat de informatie naar de concurrenten lekte. Of, de bedrijfsgeheimen zouden op een zeer beperkte schaal gebruikt kunnen worden om lekken te voorkomen, in welk geval de voorsprong op de concurrenten ook niet zo groot zou zijn.

Mogelijk, zo stelde May voor, zou het simpele bestaan van een BlackNet de economische prikkels die grote bedrijven in de eerste plaats levensvatbaar maken, fundamenteel kunnen dooreen schudden. In plaats van miljardenbedrijven zouden we door radicale transparantie een meer verspreide en levendige economie kunnen zien, gekenmerkt door een veel diverser aanbod aan kleinere bedrijven.

En May realiseerde zich uiteindelijk dat deze dynamiek niet alleen grote bedrijven zou beïnvloeden. Het zou ook net zo goed regeringen en hun strijdkrachten kunnen beïnvloeden, evenals andere openbare instellingen die vertrouwelijke informatie verwerken. Een enkele corrupte overheidsmedewerker zou, met financieel gewin als motief, voldoende zijn om allerlei geclassificeerde dossiers te verspreiden naar de hoogste bieders op het internet. Niet in staat om gevoelige gegevens te beveiligen, zou de macht van de overheid aanzienlijk kunnen afzwakken. May was dol op dit idee. En ook een andere lokale vriend van hem…

Eric Hughes

Toen Eric Hughes in de late jaren 80, toen hij halverwege de twintig was, wiskunde studeerde aan Berkeley, had de cryptografische revolutie zijn weg al in het curriculum gevonden. Wanneer hij afstudeerde, was hij goed op de hoogte van recente innovaties van mensen zoals Whitfield Diffie, Martin Hellman, Ralph Merkle en David Chaum. En net zoals zij, begreep Hughes intuïtief het veelbelovende potentieel van hun doorbraken in de context van een steeds meer gedigitaliseerde samenleving.

Hughes ontdekte dat fundamentele mensenrechten constant onder druk stonden van overheden, zoals het recht op privacy. Hoewel sommige van deze rechten juridisch gewaarborgd waren, leek het erop dat overheden altijd een manier vonden om die rechten met de voeten te treden als ze daartoe de mogelijkheid kregen.

Voor Hughes bood moderne cryptografie een methode om individuele privacy te beschermen, zonder te moeten vertrouwen op wetten, of de interpretatie ervan door politici of rechters. Het recht op privécommunicatie kon in plaats daarvan gewaarborgd worden door technologieën zoals publieke-sleutelcryptografie en mixnetwerken.

Hughes besefte dat het niveau van privacy dat bereikt kon worden met sterke cryptografie, uiteindelijk volledige immuniteit tegen fysieke bedreigingen en dwang kon bieden. Zolang anonieme internetgebruikers hun werkelijke identiteit geheim konden houden, kon niets dat ze online zouden doen of zeggen hen mogelijk in fysiek gevaar brengen.

Toen de jonge wiskundige hoorde dat Chaum in Nederland een bedrijf had opgericht om een elektronisch geldsysteem te implementeren, besloot hij om er te solliciteren. Net als Chaum geloofde hij dat geld hoe dan ook digitaal zou worden, en een privacybehoudende vorm van valuta kon het verschil betekenen tussen een vrije samenleving en een totalitaire dystopie. Bovendien geloofde Hughes dat de cryptografische protocollen van Chaum het potentieel hadden om dat verschil te maken. Chaum, op zijn beurt, geloofde dat Hughes een goede aanvulling zou zijn voor zijn bedrijf; hij werd aangenomen.

Toen Hughes in 1991 in Amsterdam aankwam om zijn nieuwe avontuur te beginnen, raakte hij vrij snel gedesillusioneerd door wat hij in de kantoren van

DigiCash aantrof. Hij ontdekte tot zijn ontsteltenis dat Chaum smartcards (de fraudebestendige, creditcard-achtige computers speciaal ontworpen voor betalingen) tot hoeksteen van zijn ontwerp had gemaakt. In plaats van zich puur te richten op de kracht van wiskunde en het perfectioneren van de cryptografische protocollen die nodig waren om elektronisch geld voor het internet te implementeren, zag hij dat DigiCash zich concentreerde op dure en niet-controleerbare hardwareproducten om offline betalingen mogelijk te maken.

Hughes was van mening dat Chaum een ernstige strategische fout maakte door pragmatiek en kostenefficiëntie te onderschatten ten gunste van experimentele features. Uiteindelijk kwam de jonge wiskundige tot de conclusie dat DigiCash toch niet de plek voor hem was. Na slechts zes weken in Amsterdam vertrok hij bij de start-up.

Eenmaal terug in Californië, overwoog Hughes op zoek te gaan naar een woning die iets dichter bij de zee lag. Hij besloot een paar dagen in Santa Cruz door te brengen om een huis te zoeken. Hij kon er verblijven bij een oude vriend die daar een paar jaar eerder naartoe was verhuisd: Tim May.

Toen Eric Hughes in 1991 in Santa Cruz aankwam, deelde May zijn visie voor anonieme informatie markten met hem. Hij legde uit hoe BlackNets gebruik zouden maken van het soort privacy tools die Hughes had bestudeerd en wilde bouwen, en hoe deze de macht van grote bedrijven en overheidsinstellingen konden verminderen, of zelfs volledig beperken.

Hoewel Hughes zichzelf niet zozeer als een libertariër van de vrije markt beschouwde zoals Tim May dat deed, intrigeerde het concept van anonieme informatiemarkten hem net zo goed. De komende paar dagen konden ze het alleen maar hebben over het enorme potentieel van moderne cryptografie. Terwijl ze filosofeerden over de implicaties van anonieme netwerken, de levensvatbaarheid van pseudonieme reputatiesystemen, en de vooruitzichten van grenzeloze betalingen, moest de huizenjacht even wachten.

Maar na enkele dagen te hebben gediscussieerd over mogelijk baanbrekende toepassingen voor publieke sleutel-encryptie, remailers en digitaal geld, leidden hun gesprekken steeds weer terug naar dezelfde knagende vraag.

Waarom was er nog steeds geen software die deze protocollen implementeerden?

Geen van de baanbrekende crypto-innovaties die sinds de jaren 70 werden voorgesteld, werden in de praktijk gebracht door echte mensen, omdat er geen

computerprogramma's beschikbaar waren die deze protocollen implementeerden. Terwijl academische papers in detail uitlegden hoe Alice en Bob privé konden communiceren dankzij de Diffie-Hellman-sleuteluitwisseling of RSA-encryptie, was dit aan het eind van de dag volledig nutteloos zolang er geen software bestond die deze taken voor Alice en Bob uitvoerde.

Toegegeven, er waren wel een paar projecten in ontwikkeling. In feite werkte Chaum aan een elektronisch betaalsysteem, hoewel hij dat niet helemaal ontwikkelde op de manier die Hughes graag zou zien. Daarnaast werkte een van Mays collega-Extropianen, de computerwetenschapper en cryptograaf Phil Zimmermann, aan een op RSA-gebaseerde publieke sleutelencryptiesoftware genaamd *Pretty Good Privacy* (PGP).

Toch leken dit erg magere resultaten, als je bedenkt hoe groot de doorbraken waren die May en Hughes zo enthousiast maakten voor de toekomst. Hoewel de nieuwe golf van crypto zich ongeveer vijftien jaar door het academia had verspreid, en een serie succesvolle Crypto-conferenties een reeks baanbrekende concepten hadden voorgesteld, bleef de daadwerkelijke softwareontwikkeling ver achter.

De vergadering

Eric Hughes verhuisde uiteindelijk niet naar Santa Cruz. Maar de reis was zeker niet voor niets. Gedurende zijn bezoek kwamen Hughes en May overeen dat het tijd was om het gat tussen de academische wereld en de echte wereld te dichten, en concludeerden ze dat zij zelf het initiatief moesten nemen om dit te verwezenlijken. May en Hughes zetten zich in voor het bijeenbrengen van enkele van de slimste en meest bekwame cryptografen en hackers uit de Bay Area, en gingen aan het werk.

De eerste persoon die ze bij hun plan betrokken was John Gilmore, een vroege medewerker van *Sun Microsystems* en medeoprichter van de digitale rechtenorganisatie *Electronic Frontier Foundation* (EFF). Binnen lokale hackerskringen had hij al geruime tijd gesproken over hoe hij cryptografie naar het grote publiek zou kunnen brengen. De drie van hen (May, Hughes en Gilmore) begonnen vervolgens meer gelijkgestemde individuen uit te nodigen die volgens hen niet

zouden terugdeinzen voor enig *hands-on* technologie-activisme.

Een paar maanden verstreken, tot op een zaterdag in september een groep van ongeveer twee dozijn gelijkgestemde individuen zich verzamelde in Hughes' nieuwe en op dat moment nog ongemeubileerde appartement in Oakland. De meeste aanwezigen waren afkomstig uit de hackergemeenschap in de Bay Area, terwijl May ook een kleine Extropian-delegatie had geregeld. Dit zorgde voor een bijzonder technologiebewuste groep mensen.

May opende de bijeenkomst met een inleiding over cryptografie. Hij bracht de aanwezigen op de hoogte van het veelbelovende potentieel van publieke-sleutelcryptografie, en besprak enkele van de innovatieve schema's die sinds de doorbraak van Diffie en Hellman waren voorgesteld. Hierna deelde hij een door hemzelf samengesteld boekje uit, waarin de basisprincipes werden uitgelegd en belangrijke termen werden gedefinieerd. De groep begon vervolgens te discussiëren over de mogelijke gevolgen voor de samenleving als cryptografische hulpmiddelen op grote schaal beschikbaar zouden worden, maar ook de onrustbarende implicaties van een toekomst zonder dergelijke hulpmiddelen.

In de namiddag begon de hele bende, vanwege een gebrek aan meubels zittend op de vloer, op speelse wijze te experimenteren met analoge representaties van cryptoprotocollen. Ze creëerden het op papier gebaseerde *crypto-anarchie-spel*, waarbij enveloppen fungeerden als een protocol voor het anonimiseren van berichten, een prikbord fungeerde als een informatiebeurs en Monopolie-geld werd rondgegeven alsof het digitale contanten waren. Op een leuke manier kreeg iedereen een gevoel van hoe deze systemen zouden functioneren.

De bijeenkomst was een succes. Aan het eind van een dag vol mini-seminars, brainstormsessies en spelletjes, was iedereen die het appartement van Hughes voor deze speciale gelegenheid had bereikt, aangestoken met hetzelfde gevoel van enthousiasme dat May, Hughes en Gilmore had aangezet om deze unieke groep mensen bij elkaar te brengen. Belangrijker nog, ze deelden nu de visie van de organisatoren dat de cryptoprotocollen waarover ze hadden geleerd, geïmplementeerd moesten worden als werkende software en zo ver mogelijk verspreid moesten worden. Om de zaak verder te bevorderen, gingen ze ermee akkoord om van de bijeenkomst een maandelijks evenement te maken.

Op dit moment concludeerde de groep ook dat ze een pakkende naam nodig hadden om zichzelf mee te omschrijven. Hughes had het tot dan toe de Cryptolo-

gie Amateurs voor Sociale Onverantwoordelijkheid (of kortweg CASO) genoemd, maar nu overwogen ze suggesties zoals 'De Crypto Vrijheid Liga', 'Privacy Hackers', en 'De Crypto Cabal'. Middenin al dit gepraat riep Hughes' vriendin van dat moment, hacker Jude Milhon, gekscherend uit: 'Jullie zijn gewoon een stel Cypherpunks!'[143] Met de slimme samentrekking van *cipher* en *cyberpunk*, had de groep hun naam te pakken.

De Cypherpunks

De bijeenkomsten die volgden, werden op wisselende locaties gehouden, vaak bij iemand thuis of in iemands werkruimte, en vormden een centraal punt voor het delen van informatie, discussie en projectcoördinatie. Natuurlijk bood het iedereen ook de kans om elkaar wat beter te leren kennen, terwijl nieuwe mensen welkom waren om zich aan te sluiten en meer te leren over het initiatief en hoe ze konden deelnemen.

De Cypherpunks schetsten tijdens deze vroege bijeenkomsten toekomstige doelen en werkten hun strategieën uit om deze doelen te bereiken.

Allereerst hadden de Cypherpunks zich tot dusverre tot doel gesteld om een dystopische toekomst te voorkomen, een toekomst waarin digitale communicatie kan worden gemonitord, geanalyseerd en uiteindelijk misbruikt. Net zoals de cryptografen die hen inspireerden, waren ze bezorgd dat zo'n verlies aan privacy despoten en tirannen zou kunnen versterken, ten koste van de individuele vrijheden: May kondigde op een gegeven moment half-grappend aan dat George Orwells *1984* verplichte lectuur was voor iedereen binnen de groep.

Maar de Cypherpunks waren niet alleen van plan om privacy te promoten of te eisen. Ze zouden zich niet beperken tot het lobbyen bij verkozen ambtenaren, of werken via het politieke en juridische proces, zoals sommige bestaande belangenorganisaties (zoals de EFF) al deden.

Een belangrijk onderdeel van hun strategie was dat de Cypherpunks zelf de behoeder van hun privacy gingen worden.[144]

---

143 Tim May, *The Cyphernomicon*, oorspronkelijk verspreid via de Cypherpunk-mailinglijst, 10 september 1994, beschikbaar online

144 Hal Finney, *Chaum on the wrong foot?* oorspronkelijk via de Cypherpunk-mailinglijst, 22 augustus 1993, beschikbaar online

'We moeten onze eigen privacy verdedigen als we verwachten er nog enige te hebben', schreef Hughes in *The Cypherpunk-Manifesto*, dat de mede-oprichter van de groep hardop voorlas tijdens een Cypherpunk-bijeenkomst begin 1993. 'We moeten samenkomen en systemen creëren die anonieme transacties mogelijk maken. Mensen hebben eeuwenlang hun eigen privacy verdedigd met gefluister, duisternis, enveloppen, gesloten deuren, geheime handdrukken en koeriers. De technologieën van het verleden boden geen sterke privacy, maar elektronische technologieën doen dat wel.'

Ze hadden plannen om deze elektronische technologieën te ontwikkelen en deze als gratis software te verspreiden. In overeenstemming met de hackerethiek, hadden ze niet de intentie om iemand om toestemming te vragen om dit te doen.

'Cypherpunks schrijven code', verklaarde Hughes. 'We weten dat iemand software moet schrijven om privacy te verdedigen, en wij gaan dat doen.'[145]

Cypherpunks schrijven code. Dit werd de informele strijdkreet van de groep.

De mailinglijst

De maandelijkse bijeenkomsten van de Cypherpunks waren vrij en open van aard. Naast de vaste kern van reguliere deelnemers, kwamen er ook nieuwsgierige nieuwkomers om een indruk te krijgen van wat er gaande was. Om de coördinatie hiervan te vergemakkelijken, richtte Hughes een e-maillijst op, gehost op de computer van Gilmore, waar hij aankomende evenementen aankondigde. Elke abonnee ontving handig een bericht in hun inbox met daarin de datum en locatie.

Maar de mailinglijst van de Cypherpunks zou al snel een groter doel gaan dienen. Het duurde niet lang voordat de lijst werd gebruikt om discussies van de fysieke vergaderingen voort te zetten. Niet veel later werden er volledig nieuwe onderwerpen op de mailinglijst geïntroduceerd, die niets te maken hadden met wat er besproken was tijdens de persoonlijke bijeenkomsten. Toen het aantal berichten toenam, begon de mailinglijst van de Cypherpunks een eigen leven te leiden.

E-mail had natuurlijk als extra voordeel dat iedereen kon deelnemen, ongeacht

145 Eric Hughes, *A Cypherpunk's Manifesto*, oorspronkelijk via de Cypherpunk-mailinglijst, 17 maart 1993, beschikbaar online

de geografische afstand, en vanuit het comfort van hun eigen huis. Vrij voorspelbaar, groeide de Cypherpunk-mailinglijst snel en overtrof die de aantallen van de feitelijke Cypherpunk evenementen. Slechts weken na de lancering had de lijst al 100 abonnees, beduidend meer dan de paar dozijn hackers en cryptografen die de maandelijkse bijeenkomsten bijwoonden.

En de populariteit van de mailinglijst explodeerde pas echt toen het technologietijdschrift Wired in mei 1993 zijn cover-verhaal wijdde aan de Cypherpunks. 'Rebellen met een doel (jouw privacy)' stond er op de cover, net boven een foto van drie gemaskerde mannen die de Amerikaanse vlag vasthielden (de uitdrukkingsloze witte maskers met computercodecode erop gekrabbeld verborgen de gezichten van May, Hughes en Gilmore). Dankzij dit cover-verhaal had nu vrijwel iedereen met interesse in computers gehoord van de groep privacy-activisten en door hun wereldwijde bereik, stroomden honderden mensen van over heel de Verenigde Staten en de rest van de wereld toe om zich aan te melden voor hun e-maillijst.

In de daaropvolgende jaren werd de Cypherpunk-mailinglijst een klein fenomeen op het vroege internet. Met tot wel 2.000 abonnees en soms bijna evenveel e-mails per maand, bespraken de Cypherpunks een breed scala aan onderwerpen: van cryptoprotocollen, tot overheidsbeleid, tot implementaties van software, en tips voor boeken of films, evenals periodieke klaagzangen en verhitte discussies. De lijst bood een platform voor publieke discussie tussen enkele van de meest getalenteerde hackers op de planeet, terwijl Silicon Valley's CEO's en mainstream journalisten ook graag meelazen.

Tim May onderscheidde zich op de mailinglijst dankzij zijn vele mails: niemand was actiever dan hij, en niemand leverde een groter aanbod aan bijdragen. Hij schetste toekomstscenario's, deelde ideeën, nam deel aan discussies, gaf technische uiteenzettingen, stelde strategieën voor, gaf commentaar op actuele gebeurtenissen, linkte naar relevante artikelen en deelde regelmatig 'snel geschreven' essays, soms zelfs verscheidene op een dag.

Maar hij onderscheidde zich ook door zijn unieke gevoel voor humor. Soms voerde hij sarcastisch het woord tegen de Cypherpunk-agenda vanuit het perspectief van een Orwelliaanse overheid en kafferde hij andere deelnemers aan de lijst uit als *burgereenheden*. Andere keren maakte hij opzettelijk politiek incorrecte grappen om de grenzen uit te dagen van wat als sociaal acceptabel werd beschouwd.

Zo veranderde hij op een gegeven moment bijvoorbeeld zijn e-mailhandtekening in 'een bijbeltekst in afwachting van beoordeling onder de Communications Decency Act', waarbij de begeleidende tekst een incestueuze orgie beschrijft.[146] Of misschien overschreed hij de sociaal aanvaardbare grenzen ronduit, afhankelijk van wie je het zou vragen. May leek er hoe dan ook niet veel om te geven.

En zijn aanwezigheid op de mailinglijst diende ook nog een ander waardevolle doel. Hoewel de lijst volledig ongemodereerd was, speelde May vaak de rol van een onofficiële moderator, en begeleidde gesprekken waar nodig. Als een discussie dreigde te ontsporen, had hij de gewoonte om zijn kenmerkende analytische perspectief in te brengen, waarbij hij uitlegde waarom hij geloofde dat bepaalde opmerkingen of onderwerpen al dan niet geschikt waren voor de lijst, maar zonder daadwerkelijk iets te verbieden; hij wilde niet dat iemand die macht had, zelfs hijzelf niet. In plaats van anderen op te leggen hoe ze zich moeten gedragen, had May een manier om het voortouw te nemen door voorbeeld, en wanneer andere abonnees klaagden over de inhoud op de mailinglijst, moedigde hij hen ook aan om het voortouw te nemen door voorbeeld.

Voor veel van zijn abonnees was May in de maanden en jaren dat de lijst actief was waarschijnlijk de belichaming van wat de Cypherpunk-filosofie voorstelde. Door zijn sterke aanwezigheid, zowel qua inhoud als in zijn sturende rol, was hij een leidende en kenmerkende stem van de beweging geworden.

May zelf, daarentegen, benadrukte vaak dat hij niet de hele Cypherpunk-gemeenschap vertegenwoordigde. Net zoals hij geen enkele moderator in controle wilde hebben over de mailinglijst, verwierp hij ten stelligste het idee dat hij, of wie dan ook, als een formele leider of woordvoerder van de beweging beschouwd moest worden. Hij stond erop dat hij slechts één stem was van de velen.

'Hoewel ieder van ons wellicht zijn of haar persoonlijke (hiërarchische) rangorde van anderen heeft, is het belangrijk dat we nooit hebben geprobeerd deze rangordes te formaliseren of erover te *stemmen*. Of te stemmen om een Grote Leider te kiezen', betoogde May op een gegeven moment. 'Onze kracht zit in onze aantallen en in onze ideeën, niet in de man die we op een kantoor in Washington hebben geïnstalleerd zodat hij persconferenties kan geven en *oneliners* kan leveren

146 Tim May, *Degrees of Freedom*, oorspronkelijk via de Cypherpunk-mailinglijst, 8 februari 1996, beschikbaar online

voor journalisten. Onze kracht zit in ons meerkoppige (durf ik *Medusa* te zeggen?), multinationale, informeel gebrek aan structuur.'[147]

Inderdaad, de Cypherpunks waren geen organisatie in de traditionele zin van het woord. Het was een bewust informele, ongestructureerde en open groep. De Cypherpunks hadden geen stemprocedure, geen vertegenwoordigers, en ze gaven zelfs geen gezamenlijke verklaringen. Iedereen kon een Cypherpunk worden, maar alle Cypherpunks zetten zich uiteindelijk in als individuen. Ze hadden geen specifieke taken of regels, noch kon iemand anderen verantwoordelijk houden voor hun eigen acties.

Toch werd actie aangemoedigd. Als iemand vond dat de Cypherpunks een specifieke technologie moesten ontwikkelen, aan een bepaald evenement moesten deelnemen of op een andere manier tot de zaak konden bijdragen, was het aan die persoon om het initiatief te nemen en te kijken of anderen ook wilden helpen.

In feite werkte de Cypherpunk-beweging niet alleen aan een ander type toekomst. Voor May vertegenwoordigde het die toekomst al. Hij zag de open, toestemmingloze en non-hiërarchische manier waarop de Cypherpunks en hun e-maillijst opereerden als een model voor een opkomende *crypto-anarchistische* samenleving.

Crypto-anarchie

De Extropians speculeerden soms over het creëren van vrije gebieden om te ondermijnen, zich te verbergen, of te ontsnappen aan staatscontrole over hun levens. Sommigen van hen stelden voor om steden te bouwen op grote drijvende eilanden in de zee – het zogenaamde *seasteading* – als de weg voorwaarts. Anderen geloofden dat het misschien mogelijk zou zijn om een klein eiland op te kopen om er een libertaire samenleving te stichten. Weer anderen suggereerden dat ze allemaal naar een specifieke jurisdictie moesten verhuizen en proberen lokale politieke structuren te beïnvloeden om zoveel mogelijk wetten en regulaties aan de kant te zetten. Maar Tim May had eigenlijk niet echt zin om te verhuizen. Hij had een beter idee.

147 Tim May, *Who shall speak for us?*, oorspronkelijk via de Cypherpunk-mailinglijst, beschikbaar online

Nadat May de puzzelstukken bij elkaar had gevoegd en daarmee het ontwrichtende potentieel van anonieme informatiemarkten liet zien, was hij een toekomst gaan visualiseren die sterk leek op de werelden uit zijn cyberpunk boeken, terwijl hij tegelijkertijd analogieën maakte met *Atlas Shrugged*. Hij besefte dat het soort samenleving dat hij wilde beschrijven in zijn aankomende roman, werkelijkheid kon worden.

In de roman van Rand maken de productieve ondernemers hun ontsnapping mogelijk met behulp van futuristische technologie. Hoewel May erkende dat warmtestralingsschermen nog steeds tot het domein van de sciencefiction behoorden, was de medeoprichter van de Cypherpunk-beweging gaan inzien dat het internet en sterke cryptografie uiteindelijk een vergelijkbare ontsnapping uit de macht van de staat konden faciliteren, net als in de verhalen van de cyberpunkgenre.

May schetste deze visie in *The Crypto Anarchist Manifesto*.[148] Hij schreef het oorspronkelijk voor de editie van de Crypto-conferentie in 1988, las het korte manifest voor tijdens de allereerste bijeenkomst van de Cypherpunks in Hughes' appartement en deelde het later ook via hun mailinglijst.

'Een spook waart rond in de moderne wereld, het spook van de crypto-anarchie', begon het manifest met een knipoog naar het Communistisch Manifest van Karl Marx en Friedrich Engels, voordat het voorspelde dat computertechnologie en cryptografische protocollen 'de aard van de overheidsregulering volledig zullen veranderen, het vermogen om de economische interacties te belasten en te controlen, het vermogen om informatie geheim te houden, en zelfs de aard van vertrouwen en reputatie zullen veranderen.'

Om een paar paragrafen verder te concluderen:

'Net zoals de technologie van drukken de macht van de middeleeuwse gilden en de sociale machtsstructuur heeft veranderd en verminderd, zo zullen cryptologische methoden de aard van bedrijven en de inmenging van de overheid in economische transacties fundamenteel veranderen.'[149]

148 De titel en tekst waren een soort parodie op het Communistisch Manifest van Karl Marx en Friedrich Engels, terwijl de term crypto-anarchie een soort woordspeling is die verwijst naar crypto-fascisme, de geheime steun voor fascisme.

149 Tim May, *The Crypto Anarchist Manifesto*, oorspronkelijk via de Cypherpunk-mailinglijst, 22 november 1992, beschikbaar online

Het internet was nog niet getransformeerd naar de kleurrijke 3D-wereld zoals die in de romans van Vinge, Stephenson en Gibson werd voorgesteld. Maar als je deze verhalen meer als metaforische representaties van online domeinen beschouwde, had May ze toch als visionair leren waarderen. Terwijl het internet verder zijn onvermijdelijke pad naar massa-adoptie vervolgde, en mensen stapje voor stapje zouden leren om zichzelf online te organiseren, geloofde May dat de instellingen van de reële wereld uiteindelijk zouden worden vervangen door hun cyber-equivalenten. Het internet zou in toenemende mate dienen als facilitator voor een parallelle, digitale samenleving, met eigen gemeenschappen, ondernemingen en uiteindelijk ook eigen economieën.

'Dit maakt snelle experimentatie, zelfselectie en evolutie mogelijk', stelde May voor op de Cypherpunk-mailinglijst. 'Als mensen een bepaalde virtuele gemeenschap beu raken, kunnen ze deze verlaten. De cryptografische aspecten zorgen ervoor dat hun lidmaatschap van een bepaalde gemeenschap onbekend blijft voor anderen (vis-a-vis de fysieke of buitenwereld, oftewel, hun *echte namen*) en fysieke dwang vermindert.'

Verdergaand: 'De elektronische wereld is geenszins volledig, aangezien we nog steeds een groot deel van ons leven in de fysieke wereld zullen doorbrengen. Maar de economische activiteit in het domein van het Net neemt sterk toe en deze ideeën van *crypto-anarchie* zullen de macht van fysieke staten om inwoners te belasten en te dwingen verder ondermijnen.'[150]

Dit alles werd mogelijk gemaakt door de kracht van cryptografie. Niet alleen zouden crypto-middelen gebruikers helpen hun echte identiteit te beschermen, waardoor ze beschermd werden tegen fysiek geweld, maar zouden dezelfde middelen ook toestaan dat twee personen zaken konden doen zonder dat een van hen ooit wist met wie ze te maken hadden.

'[…] sterke cryptografie is het *bouwmateriaal* van cyberspace', schreef May aan zijn mede-Cypherpunks, 'de mortel, de bakstenen, de steunbalken, de muren. Niets anders kan de *permanentie* bieden… zonder crypto zijn de muren bij de eerste aanraking door een kwaadwillend persoon of organisatie onderhevig aan instorting. Met crypto kan zelfs een 100 megaton waterstombom de muren niet

150 Tim May, *Libertaria in Cyberspace*, oorspronkelijk via de Cypherpunk-mailinglijst, 9 augustus 1993, online

doorbreken.'[151]

May voorzag dat Cypherpunk-tools mensen zouden helpen om hun economische activiteit voor de staat te verbergen en zo een *Galt's Gulch in cyberspace* zouden creëren. Hij keek uit naar een toekomst waarin dit uiteindelijk zou leiden tot de volledige ineenstorting van regeringen. Zonder gedwongen herverdeling van welvaart, zou deze toekomstige economie zichzelf organiseren rondom vrijwillige interactie en vrije markten. Er zou een *spontane orde* ontstaan via het internet.

'In feite heeft Hayek héél véél met de Cypherpunks te maken!' schreef May op de Cypherpunk-mailinglijst. 'Van *The Road to Serfdom* tot *Law, Legislation, and Liberty*, zijn werken hebben een enorme invloed op mij, en op vele anderen, gehad. […] Ik zou zelfs zeggen dat Hayek een kandidaat zou zijn geweest om op de cover van *Wired* te staan… natuurlijk ervan uitgaande dat hij 60 jaar jonger was, sommige van zijn lichaamsdelen had gepiercet, en beter nog, een Netchick was.'[152]

Code

Tim May was er zich goed van bewust dat de crypto-anarchistische ideeën die hij verspreidde niet precies aantrekkelijk waren voor een breed publiek; niet iedereen hoopt op een ineenstorting van regeringen. Waarschijnlijk zou het nog erger worden als men erachter zou komen dat onkraakbare encryptie en anonieme mixnetwerken grootschalige verspreiding van kinderpornografie mogelijk maakten en veilige communicatie voor terroristische cellen faciliteerden. Veel mensen zouden deze nieuwe instrumenten waarschijnlijk met angst en woede bekijken.

Maar May weigerde de risico's die deze nieuwe technologieën introduceerden te bagatelliseren.

'Privacy heeft zijn prijs', betoogde hij simpelweg. 'Het vermogen van mensen om achter gesloten deuren misdaden te beramen en te plegen is evident, en

151 Tim May, *Cyberspace, Crypto Anarchy, and Pushing Limits*, oorspronkelijk via de Cypherpunk-mailinglijst, 3 april 1994, online

152 Tim May, *Hayek*, oorspronkelijk via de Cypherpunk-mailinglijst, 27 augustus 1996, online. Als een grappige noot sloot Tim May een andere e-mail af met een compliment aan een van zijn mede-Cypherpunks: 'Ik wil gewoon eindigen op een positieve noot voordat ik vertrek voor de feestdagen.' Zie: Tim May, *Re: The War on Some Money [long]*, oorspronkelijk via de Cypherpunk-mailinglijst, 21 december 1995, online

toch eisen we geen verborgen camera's in woningen, appartementen en hotelkamers!'[153]

Voor May was crypto-anarchie bovendien geen verre utopie die brede steun voor zijn ideeën vereiste: integendeel, hij beschouwde het bijna als een voldongen feit. Hij begreep dat de weg ernaartoe bezaaid kon zijn met tegenslagen en onderdrukkende wetten, gerechtvaardigd door beleidsmakers die angst inboezemden over de *vier ruiters van de infocalyps*: terroristen, pedofielen, witwassers en pornografen. Maar Cypherpunk-tools waren goedkoop te verspreiden, makkelijk te gebruiken en konden niet on-uitgevonden worden. Op de lange termijn, geloofde May, was succes vrijwel gegarandeerd.

Dit betekende niet dat elke Cypherpunk Mays nogal radicale visie deelde, noch hoefden ze dat te doen. Vaker wel dan niet waren Cypherpunks libertariërs, maar velen onderschreven ook een gematigder wereldbeeld dan May. Sommige Cypherpunks waren zelfs helemaal geen libertariërs, met meerdere van hen die zichzelf identificeerden als socialist.

'Ik ben geen libertariër, en het is onwaarschijnlijk dat ik dat ooit zal zijn', schreef Hughes aan de mailinglijst. 'Het streven naar privacy staat los van de meeste partijpolitieke standpunten. Zo sterk als de libertarische aanwezigheid op deze lijst is, is het geenszins de enige visie. Juist omdat Cypherpunk-kwesties dwars door het politieke spectrum snijden, zijn ze zo krachtig.'[154]

Wat van belang was, stemden May en Hughes mee in, was dat de Cypherpunks, ongeacht hun politieke overtuiging, aan een gezamenlijk doel konden werken: het ontwikkelen en verspreiden van tools voor privacy. *Cypherpunks schrijven code*.

Inderdaad, de groep was nauwelijks gestart toen Hughes een vroege versie ontwikkelde van de eerste remailer ooit, gebaseerd op het mixnetwerkvoorstel van David Chaum. De eerste uitvoering van deze remailer zou e-mails accepteren, details die naar de afzender verwezen verwijderen en vervolgens doorsturen naar, of de volgende remailer, of naar de bedoelde ontvanger van de e-mail. Deze uitvoering van Hughes omvatte echter nog geen encryptietools; het was nog altijd in ontwikkeling.

---

153 Tim May, '*Stopping Crime* Necessarily Means Invasiveness', oorspronkelijk via de Cypherpunk-mailinglijst, 17 oktober 1996, online

154 Eric Hughes, *No digital coins*, oorspronkelijk via de Cypherpunk-mailinglijst, 24 augustus 1993, online

Gelukkig kreeg Hughes al snel hulp van een andere Cypherpunk. Hal Finney, een van de Extropianen die zich bij Tim May hadden aangesloten voor de Cypherpunk-bijeenkomsten, was net begonnen met het bijdragen aan de implementatie van Phil Zimmermanns PGP. Met zijn nieuw verworven kennis van publieke-sleutelcryptografie duurde het niet lang voordat Finney PGP integreerde in de remailer-code van Hughes.

Slechts enkele weken na de eerste samenkomst hadden de Cypherpunks al een volledig werkende remailer ontwikkeld. En die gingen ze ook zelf gebruiken. Finney en een aantal andere Cypherpunks namen het initiatief om de remailer-programma's uit te voeren, en ze verspreidden software en beginnershandleidingen zodat anderen zich bij hen konden aansluiten. Op deze manier werden remailers operationeel. Tegen het einde van 1992 kon iedereen met een computer en internetverbinding e-mails versturen zonder hun metadata te onthullen.

Rond diezelfde tijd was Zimmermann van plan om PGP 2.0 te lanceren. De bijdragen van Finney aan deze nieuwe versie hadden tot aanzienlijke verbeteringen geleid ten opzichte van de eerste versie, en de software beschikte nu over een *web-of-trust* systeem, wat gebruikers in staat stelde om cryptografisch te garanderen dat een publieke sleutel werkelijk aan een bepaald persoon toebehoort.

Met de gloednieuwe remailer-software van Hughes en de verbeterde encryptietool van Zimmermann, gingen de Cypherpunks goed van start. Maar het zou niet lang duren voordat ze in de verdediging werden gedwongen…

De crypto-oorlogen

Toen Bill Clinton in januari 1993 het ambt van de 42e President van de Verenigde Staten op zich nam, waren er door zijn nieuwe administratie snel zorgen geuit omtrent het mogelijk onheilspellende gebruik van persoonlijke computers en het internet. Ze kondigden aan dat wetshandhavingsinstanties nieuwe tools nodig zouden hebben om mee te kunnen gaan met het recente tempo van technologische vernieuwing. Dit bleek een voorbode te zijn van de *crypto-oorlogen* van de jaren negentig: de Amerikaanse overheid zou proberen het gebruik van cryptografie te beperken.

De eerste klap viel toen Zimmermann het onderwerp werd van een strafrech-

telijk onderzoek. In deze periode werden cryptografische protocollen die sleutels gebruikten die groter waren dan 40 bits in de Verenigde Staten geclassificeerd als munitie onder de definitie van de *Arms Export Control Act*. Het verzenden of meenemen van een sterk cryptosysteem naar het buitenland vereiste een vergunning, vergelijkbaar met de vergunning die nodig is voor internationaal vervoer van vuurwapens, munitie of explosieven.

Zimmermann bezat geen dergelijke licentie, maar hij verspreidde zijn gratis software wel via het internet. Omdat het internet geen landsgrenzen kent, insinueerde de overheid dat Zimmermann zijn software en de daarin opgenomen cryptoprotocollen illegaal geëxporteerd had.

En toen was er de Clipper-chip, een chipset ontwikkeld door de NSA en ondersteund door de regering Clinton. De Clipper-chip gebruikte cryptografie met publieke sleutels om data te versleutelen, maar de NSA had een speciale ontcijfersleutel toegevoegd aan het protocol. Het plan was dat telecombedrijven zoals AT&T de chipset zouden adopteren, zodat gebruikers hun telefoongesprekken konden versleutelen. De telecombedrijven zouden echter een ontcijfersleutel bewaren, die op verzoek aan de regering kon worden overhandigd. Dergelijke *sleutelbewaring* was noodzakelijk voor nationale veiligheidsredenen, stond de regering Clinton erop: de autoriteiten moesten in staat zijn om de telefoongesprekken van potentiële en verdachte terroristen te beluisteren.

De Clipper-chip werd tegengewerkt door voorstanders van privacy en belangenorganisaties voor burgerlijke vrijheden in het hele land, waaronder de *Electronic Frontier Foundation* (EFF), het *Electronic Privacy Information Center* (EPIC) en de *American Civil Liberties Union* (ACLU). Ook technologietijdschriften zoals *Wired*, cryptografie-start-ups zoals RSA van Ron Rivest, Adi Shamir en Leonard Adleman, en enkele politici (zowel Democraten als Republikeinen) voerden oppositie. Critici waren van mening dat de zogenaamde sleutelbewaring de kans vergrootte dat burgers onderworpen zouden worden aan verhoogde en mogelijk onwettige overheidssurveillance.

Uiteraard wezen de Cypherpunks de Clipper-chip ook af. De weerstand tegen de NSA-chip werd een van de eerste regelmatig terugkerende onderwerpen op de mailinglijst. Het was duidelijk dat het overhandigen van decoderingssleutels aan telecombedrijven (en, in verlengde daarvan, aan overheidsdiensten die de telecoms reguleren) deze cryptografische protocollen bijna nutteloos zou maken.

Voor de Cypherpunks betekende privacy in grote mate vrijheid van overheidsinmenging. Alleen zo konden ze een Orwelliaanse toekomst voorkomen. Uiteraard zou de crypto-anarchistische visie waarschijnlijk niet ver komen met hun eigen *Galt's Gulch in cyberspace* als de cryptografische bouwstenen die hen beschermden tegen de staat poreus bleken te zijn.

Tegelijkertijd stelden de Cypherpunks dat het verplichten van het gebruik van gecompromitteerde of zwakke encryptieprotocollen de wereld in geen enkele zin betekenisvol veiliger zou maken. Kwaadwillende actoren zouden nog steeds degelijke encryptie kunnen gebruiken onder de zwakke laag van Clipper-chip encryptie om de inhoud van hun communicatie te verbergen. Dus zelfs als overheidsagenten hun toegewezen decoderingssleutel zouden gebruiken, zouden ze enkel meer versleutelde tekst tegenkomen.

Tim May was van mening dat de Cypherpunks een cruciale rol konden spelen in de naderende cryptografische conflicten. In tegenstelling tot gevestigde belangengroepen die beter georganiseerd, beter gefinancierd en beter in contact stonden met beleidsmakers en toezichthouders, zag May in het anarchistische organisatiemodel van de Cypherpunks juist een sterkte. Verspreid over de Verenigde Staten en daarbuiten, en zonder formeel leiderschap of organisatiestructuur, waren de Cypherpunks niet te coöpteren. Terwijl organisaties zoals EFF, EPIC en ACLU bereid waren tot zachtaardige onderhandelingen, weigerden de Cypherpunks elke vorm van gematigdheid te adopteren.

'Op een bepaalde manier vervullen de Cypherpunks een belangrijke ecologische niche door het voeren van de radicale, buitensporige oppositie… misschien een beetje zoals de rol die de Zwarte Panters, Yippies en Weather Underground een generatie geleden speelden', schreef May.[155]

Inderdaad, het verzet van de Cypherpunks nam allerlei vormen aan: juist omdat ze geen formele organisatie hadden, handelden de Cypherpunks uiteindelijk uit eigen beweging. Sommigen van hen verspreidden flyers met informatie over de Clipper-chip in lokale winkelcentra. Anderen analyseerden hoe de chip werkte om te proberen fouten in het ontwerp te vinden. En natuurlijk was de voornaamste strategie van de Cypherpunks om code te schrijven.

155 Tim May, *Crypto Activism and Respectability*, oorspronkelijk via de Cypherpunk-mailinglijst, 21 april 1993, online

'Potentiële inbreuk in de echte wereld zou het volledig verbieden van sterke crypto kunnen zijn, waarbij ciphers door de overheid goedgekeurd moeten worden', opperde May in zijn denken over verdere escalatie van de crypto-oorlogen. 'Zo'n verbod zal een verwoestend effect hebben op onze privacy, op ons vermogen om cyberspace-werelden te bouwen die ik heb beschreven, en op computer-gemedieerde markten in het algemeen.'

Hij concludeerde: 'Ons onmiddellijke doel moet zijn om ervoor te zorgen dat de *geest uit de fles is*, dat voldoende crypto-tools en kennis wijdverspreid zijn zodat zo'n overheidsverbod zinloos wordt.'[156]

Sucessen

De Cypherpunks waren gemotiveerd en gedreven, maar stonden tegenover de volle kracht van de Amerikaanse overheid. Weinigen hadden verwacht dat ze als overwinnaars uit de crypto-oorlogen zouden komen. Toch boekten ze het ene succes na het andere.

Een van de meest opmerkelijke overwinningen kan worden toegeschreven aan Matt Blaze, een beveiligingsonderzoeker bij Bell Labs en een frequente deelnemer aan de Cypherpunks mailgroep. In 1994 deelde Blaze een pijnlijke klap uit aan de Clipper-chip door een paper te publiceren die een fout aantoonde in het ontwerp van de chip, die gebruikers toestond om de speciale decoderingssleutel uit te schakelen. Terwijl de reputatieschade van de chip al groeide door de hevige tegenstand die het te verduren had, blijkt nu dat de Clipper-chip zelfs niet deed waarvoor hij verondersteld werd ontworpen te zijn.

Het was voldoende om telecombedrijven ervan te overtuigen de NSA technologie niet te adopteren. Het project zou geheel ter ziele gaan tegen 1996.

Zo wisten Cypherpunks Ian Goldberg en David Wagner in 1995 ook de gesloten broncode, en *export-grade* encryptiestandaard van Netscape te kraken. Dit deden ze in het kader van een wedstrijd, ontworpen door Hal Finney, en ze hadden hier slechts enkele uren voor nodig. Het schaadde het imago van een van de vooraanstaande bedrijven van Silicon Valley.

156 Tim May, *Opportunities in Cyberspace*, oorspronkelijk via de Cypherpunk-mailinglijst, 8 september 1993, online

Als reactie hierop, beweerde Netscape dat ze wettelijk verhinderd waren om sterkere encryptiestandaarden aan te bieden in het buitenland. Hoewel dit maar een deel van het probleem was, bood het weinig geruststelling aan potentiële klanten buiten de VS. Het incident benadrukte ook een ander probleem als gevolg van de classificatie van encryptie als munitie: Amerikaanse technologiebedrijven liepen het risico marktaandeel te verliezen aan buitenlandse concurrenten.[157]

Weer een andere Cypherpunk, Brad Huntting, kwam in 1994 met een slim idee om de exportrestricties op dergelijke cryptoprotocollen uit te dagen: hij publiceerde code in fysieke vorm om aan te tonen dat elk verbod op software-distributies in strijd is met fundamentele rechten.

'Het recht op vrije meningsuiting wordt beschermd door de Amerikaanse grondwet. We hoeven alleen maar aan te tonen dat encryptiesoftware gelijk staat aan spraak', schreef hij aan de mailinglijst. 'Dit zou niet te moeilijk moeten zijn (misschien een beetje pijnlijk, maar niet moeilijk). De daad zou een gepubliceerd werk moeten betreffen (bij voorkeur in de gedrukte zin).'[158]

Ongeveer een jaar later publiceerde Zimmermann *PGP: Broncode en Interne Werking*: hij had de volledige PGP-broncode in een boek afgedrukt. Zoals Huntting inderdaad had aangegeven, vallen boeken (inclusief de export ervan) in de VS onder de bescherming van het Eerste Amendement. Door dezelfde informatie die hem onderwerp van een strafrechtelijk onderzoek had gemaakt, vrij en legaal in harde kaft te verspreiden, legde Zimmermann de absurditeit van de regelgeving rondom crypto-export bloot.

Hoewel het nooit werd bevestigd dat het iets te maken had met de publicatie van zijn boek, liet de Amerikaanse overheid Zimmermanns zaak vroeg in 1996 vallen.

Bovendien zouden de exportverboden tegen het einde van dat jaar volledig worden opgeheven. Een combinatie van juridische uitdagingen, economisch schadelijke beperkingen op de Amerikaanse technologie-industrie, en de onomkeerbaar wijdverbreide verspreiding van cryptoprotocollen buiten de Verenigde Staten bewoog de Clinton administratie om commerciële encryptie volledig van

157 Michelle Quinn, *The Cypherpunks Who Cracked Netscape*, San Francisco Chronicle, 20 september 1995, online

158 Tim May, *Re: Stalling the crypto legislation for 2-3 more years*, oorspronkelijk via de Cypherpunk-mailinglijst, 23 juli 1994, online

de munitielijst te schrappen.

De Cypherpunks hadden dit niet alleen gedaan: de beweging om cryptografie tijdens de crypto-oorlogen te verdedigen was breder dan enkel zij. Maar, zij hadden onmiskenbaar een belangrijke rol gespeeld. Het losse collectief van hackers en cryptografen, verenigd door weinig meer dan een mailinglijst op het internet, was de strijd aangegaan met de Amerikaanse overheid, en had gewonnen.

Hoofdstuk 9

Cypherpunk-valuta

De Cypherpunks hadden zich tot doel gesteld om privacy in het digitale tijdperk te verdedigen. Ze begrepen dat de privacy die contant geld biedt, in gevaar was. Als elektronische betalingen papiergeld en metalen munten zouden vervangen, konden banken en andere transactieverwerkers (en bij uitbreiding de regeringen die hen reguleren) alle economische activiteit monitoren.

Cryptograaf David Chaum en zijn eCash-systeem dienden als grote inspiratiebron en zijn waarschuwingen echoden na. De Cypherpunks waren van mening dat dit uiteindelijk het einde van de menselijke vrijheid zou kunnen betekenen.

'[…] als de overheid deze cashloze samenleving creëert, dan zal de overheid ongekende controle hebben over vrijwel elk aspect van ons leven', zo zou Tim May stellen op de Cypherpunk-mailinglijst.

'Elke transactie, hoe onbeduidend ook, zal worden vastgelegd, bewaard en geanalyseerd. Er zal een volledige audittrail bestaan van alle aankopen, voedselvoorkeuren, entertainmentkeuzes, contacten met anderen, enzovoort', schreef hij. 'Bovendien kunnen transacties die als politiek incorrect worden beschouwd, en er zijn tientallen duidelijke voorbeelden om uit te kiezen, simpelweg worden …verboden… door het typen van een paar regels instructies in de relevante databanken.'[159]

May gaf in zijn bericht vrij alledaagse voorbeelden om dit punt duidelijk

159 Tim May, 'Scenario for a Ban on Cash Transactions', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, November 24, 1992, online

te maken. Iemand die ooit was gearresteerd voor rijden onder invloed zou zo bijvoorbeeld kunnen worden verboden om bier te kopen bij een slijterij, of zwangere vrouwen ('en onder Clintons geautomatiseerde zorgsysteem zal dit allemaal bekend zijn') zouden kunnen worden verhinderd sigaretten te kopen. Overheidscontrole over transacties zou niet alleen invloed hebben op gevaarlijke criminelen of extreme politieke dissidenten, benadrukte de Cypherpunk, het zou uiteindelijk leiden tot totale controle over alle burgers: 'Vergis je niet, een door de overheid gerunde maatschappij zonder contant geld zal erger zijn [dan] het allerergste van Orwell.'[160]

Dit is waarom May tijdens de allereerste bijeenkomst van de Cypherpunks het concept van elektronisch geld presenteerde, en waarom de losse verzameling van hackers en cryptografen die samenkwamen in het ongemeubileerde appartement van Eric Hughes het idee direct omarmden. De creatie van een digitaal betalingssysteem met sterke privacygaranties, zo geloofden de Cypherpunks, kon helpen zo'n dystopische toekomst te voorkomen.

Maar dit was niet de enige reden waarom de Cypherpunks digitaal geld wilden creëren; ze waren van mening dat internetgeld hun beweging op meer dan één manier kon bevorderen.

Behalve privacy, waren sommige Cypherpunks ook zeer geïnteresseerd in andere functies die elektronisch geld mogelijk kon bieden, zoals snelle transactieafhandeling, onomkeerbaarheid, of kostenefficiëntie. Ze waren enthousiast over de nieuwe mogelijkheden die dergelijke functies mogelijk konden maken: internetgeld kon online diensten en spellen ten goede komen, speculeerden ze, of *machine-to-machine* betalingen mogelijk maken. Dit zou op zijn beurt misschien innovatieve nieuwe soorten markten kunnen faciliteren, zoals de markten voor het toewijzen van computerrekenkracht voorgesteld door de high-tech Hayekianen.

Dichter bij huis zou digitaal geld voordelen kunnen bieden voor Cypherpunkprojecten zoals remailers. De door Eric Hughes en Hal Finney ontwikkelde remailers werden aanvankelijk gratis aangeboden door Cypherpunks, maar het was niet duidelijk of deze regeling stand kon houden. Naarmate deze diensten in de loop van de tijd populairder werden, zou het beheren van een remailer uiteindelijk een

160 Tim May, 'Scenario for a Ban.'

te grote belasting kunnen worden voor vrijwillige hobbyisten; Hughes verwachtte dat beheerders op een dag kosten zouden moeten gaan rekenen. Om wille van voor de hand liggende redenen zouden dergelijke betalingen anoniem moeten zijn: gebruikers zouden hun identiteit niet moeten onthullen om remailers te gebruiken.

Evenzo was de ontwikkeling van anonieme informatiemarkten, BlackNets, afhankelijk van het bestaan van een privacybeschermende vorm van digitaal geld. Mensen zouden pas bereid zijn geclassificeerde documenten of geheime rapporten via internet te verkopen, als ze er zeker van waren dat hun bazen bij hun overheidsinstantie of bedrijf niet konden ontdekken dat zij het waren die deze gegevens voor een beetje extra geld verkochten: dit betekende dat dit beetje extra geld vrij van elke identificerende eigenschap moest zijn.

En elektronisch geld was uiteindelijk een cruciale bouwsteen in Tim Mays crypto-anarchistische visie voor de toekomst. Het opzetten van een parallelle samenleving in de digitale ruimte — een 'Galt's Gulch in cyberspace' — vereiste dat mensen hun inkomen en rijkdom verborgen konden houden voor hun overheid. Een anonieme digitale valuta zou mensen in staat stellen belastingheffing te ontlopen.

May begreep goed dat elektronisch geld op zichzelf niet meteen de belastingambtenaar overbodig zou maken. Mensen die zichtbaar deelnemen aan de economie ('de man die werkt bij Lockheed of achter de toonbank bij Safeway') zouden nog steeds de rekening betalen voor diensten van de overheid. Maar volgens May zou, als een significant deel van de economie succesvol en consequent belastingen kon ontduiken, dit uiteindelijk een verandering in het publieke sentiment veroorzaken dat dan weer een veel grotere sociale verandering zou teweegbrengen.

'Wanneer het nieuws zich verspreidt dat veel consultants, schrijvers, informatieverkopers en dergelijke een groot deel van hun inkomen afschermen door gebruik te maken van netwerken en sterke crypto, zal de impact een ondermijning van de steun voor belastingen zijn', schreef May. 'Het belastingstelsel is al wankel, een nationale schuld van $5 biljoen, die elk jaar groeit, en het zou niet veel van een duw nodig kunnen hebben om een 'faseverandering' te veroorzaken; een

belastingopstand.'[161]

En tot slot was er nog de mogelijkheid van monetaire hervorming.

In het bijzonder zagen sommige van de Cypherpunks, zoals Tim May, die ook deel uitmaakte van de Extropiaanse gemeenschap, in elektronisch geld een instrument voor de verwezenlijking van Friedrich Hayeks vrije bankeneconomie. Ze beseften dat aangezien elektronisch geld in alles wat de markt wil kan worden uitgedrukt, dit concurrentie tussen valuta veel praktischer kon maken en veel moeilijker te stoppen. Vrije banken konden overal ter wereld gevestigd zijn, terwijl iedereen met een internetverbinding hun valuta, anoniem, zou kunnen gebruiken.

'De sterke encryptie die wordt gebruikt, biedt meer flexibiliteit in het omzeilen van normale valutaregels en kan gebruikers in staat stellen om onderling overeen te komen welke valuta ze willen gebruiken', schreef May op de Cypherpunk-mailinglijst.[162] En: 'een van de potentiële voordelen van sterke encryptie is de vaak besproken denationalisatie van geld.'[163]

In zijn geheel, stelde elektronisch geld iets voor, dat vergelijkbaar is met de heilige graal van de Cypherpunks.

Het compromis van Chaum

Toen de Cypherpunks in de vroege jaren '90 net op het toneel verschenen, was David Chaums eCash het enige elektronische geldproject dat sterke privacy garandeerde. In hun discussies over digitaal geld tijdens bijeenkomsten of op de Cypherpunk-mailinglijst, maakten Tim May en de andere Cypherpunks vaak expliciet of impliciet verwijzingen naar Chaums ontwerp. Hij had met zijn methode van blinde handtekeningen een cruciaal onderdeel van de privacy-puzzel opgelost.

Verschillende van de Cypherpunks gingen zelfs persoonlijk naar Amsterdam, om een tijdje bij Chaums start-up voor digitale valuta te werken. Naast mede-

161 Tim May, 'Crypto Anarchy, the Government, and the National Information Infrastructure', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, November 29, 1993, online

162 Tim May, 'DigiCash can use whatever currencies are valued', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, May 4, 1994, online

163 Tim May, 'Re: Hettinga's e$yllogism', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, June 28, 1997, online

oprichter van de Cypherpunks Eric Hughes en computerwetenschapper (en Extropiaan) Nick Szabo, waren dit bijvoorbeeld ook beveiligingsspecialist Bryce 'Zooko' Wilcox-O'Hearn en Cypherpunk Lucky Green.

Chaum daarentegen, was niet bijzonder gecharmeerd door de meer radicale crypto-anarchistische aspiraties die May en sommige van de andere Cypherpunks voorstonden. De cryptograaf werkte niet aan een digitaal cashsysteem om digitale zwarte markten te faciliteren en hij had geen verlangen om door middel van massale belastingontduiking mensen te helpen regeringen omver te werpen. Chaum vond privacy noodzakelijk om de democratie te redden, niet om ervan af te komen. Hoewel niet alle Cypherpunks Mays meer radicale visie deelden, zou Chaum geen enkele associatie met hun beweging willen en hij heeft zich nooit aangesloten bij hun mailinglijst.

Intussen waren ook niet alle Cypherpunks zonder meer tevreden met Chaum en zijn werk. Hughes had natuurlijk na slechts enkele weken bij het bedrijf besloten om DigiCash te verlaten; zijn teleurstelling in Chaums zakelijke strategie diende uiteindelijk als motivatie om de Cypherpunk-beweging op te richten. In de daaropvolgende jaren toonde Hughes zich op de mailinglijst van de Cypherpunks als een consequente en soms harde criticus van zijn voormalige werkgever: hij bekritiseerde regelmatig de voortdurende focus van de start-up op hardwareproducten.

De hoop van de Cypherpunks dat Chaum de belofte van digitaal geld zou waarmaken, brokkelde verder af toen men ontdekte dat eCash werd ontworpen zonder sterke privacygaranties voor verkopers (ontvangers van eCash transacties). Hoewel het elektronische geldsysteem van DigiCash robuuste privacy bood voor kopers (zenders van transacties), kon de echte identiteit van een eCash-ontvanger worden onthuld als de zender en de bank samenwerkten. Kortom, de zender zou de onbeschermde digitale contanten met de bank moeten delen, zodat wanneer de ontvanger de eCash-fondsen stortte, de bank dit kon koppelen aan de echte naam die bij de rekening van de ontvanger hoorde.

Tot verbazing van veel Cypherpunks, beschouwde Chaum dit als een aantrekkelijke eigenschap. Chaum, de CEO van DigiCash, redeneerde dat eCash, met de optie om ontvangers te deanoniemiseren, minder snel gebruikt zou kunnen worden voor afpersing, ontvoering of andere verontrustende criminele activiteiten. Daarnaast zou het zijn digitale geldsysteem waarschijnlijk aantrekkelijker maken

voor banken en andere financiële instellingen, en (vooral) voor toezichthouders op deze instellingen.

Privacy zonder compromissen

Voor de meeste Cypherpunks was het compromis over de anonimiteit van verkopers in eCash een grote teleurstelling.

Hun voornaamste doel was om de bestaande privacy die contant geld al bood te behouden. Dit omvatte anonimiteit aan beide zijden van een transactie: bij het wisselen van een dollarbiljet onthullen noch kopers, noch verkopers hun persoonlijke gegevens. Bovendien *vereiste* Mays crypto-anarchistische visie volledige anonimiteit van zowel kopers als verkopers: niemand zou gestolen legerdocumenten te koop aanbieden op een BlackNet als het voor de koper heel eenvoudig was om hun echte naam te achterhalen.

De meeste Cypherpunks hadden daarom geen enkele wens of intentie om compromissen te sluiten op het gebied van privacy om elektronische geldtechnologie minder aantrekkelijk te maken voor criminelen. Noch waren ze geïnteresseerd in het ontwerpen van softwaretools om digitaal geld acceptabeler te maken voor regelgevers: overheden werden *zelf* beschouwd als de grootste mogelijke bedreiging voor hun privacy, zeker in de dystopische toekomst die ze probeerden te voorkomen. Ze waren ervan overtuigd dat elk zwak punt in privacy-systemen misbruikt zou worden.

'Ieder systeem dat de overheid in staat stelt om een transactie te traceren, of om een bericht te traceren, of om toegang te krijgen tot sleutels, gooit in feite de vrijheidsbevorderende voordelen van cryptografie volledig weg', betoogde May op de mailinglijst. 'Vraag jezelf eens af of de regering van Myanmar, bekend als SLORC, haar 'Overheidstoegang tot Sleutels' niet zou gebruiken om dissidenten in de jungle op te pakken. Zouden Hitler en Himmler 'sleutelherstel' hebben gebruikt om te achterhalen met wie de Joden communiceerden zodat ze allemaal konden worden opgepakt en vermoord? Zou de Oost-Duitse Stasi eCash transacties hebben getraceerd? Voor elke regering op de planeet […] kan men makkelijk tientallen voorbeelden bedenken waar toegang tot sleutels, toegang tot dagboeken, toegang

tot uitgavenlogboeken, etc., misbruikt zou worden.'[164]

En hoewel het waar is dat afpersers, ontvoerders en andere criminelen ook zouden profiteren van een volledig anoniem betalingssysteem, geloofde May niet dat de soorten privacycompromissen die Chaum nastreefde ook maar iets konden oplossen in de realiteit. Hij merkte op dat de situatie waarin een ontvoerder wordt gepakt omdat zijn identiteit wordt onthuld door samenwerking tussen de betaler en de bank waarschijnlijk nooit echt zou voorkomen, omdat de ontvoerder in eerste instantie geen systeem met aangetaste privacyfuncties zou gebruiken.

Eerder zou, zolang er ergens in de wereld *een* privé-betaaloplossing bestond, de kans groot zijn dat ontvoerders eisten dat het geld gewoon via dat systeem naar hen wordt verzonden… en er zou waarschijnlijk altijd wel *ergens* een privé-betaaloplossing bestaan.

'Het kan een fysieke bank zijn, zoals de Bank van Albanië, of het kan een ondergronds betalingssysteem zijn, zoals de maffia, de Tongs, de Triades, of wat dan ook', suggereerde May. 'Helaas voor [financiële toezichthouders], en jammer genoeg voor de slachtoffers van dergelijke misdaden, lijkt een wereldwijde stopzetting van dergelijke systemen niet mogelijk, zelfs met draconische politiestaatsmaatregelen. Er zijn gewoon te veel tussenruimtes waarin de bits zich kunnen verstoppen. En er is te veel economische prikkel voor sommige personen of banken om dergelijke fondsoverdrachtmethoden aan te bieden.'[165]

Chaum had, door middel van eCash, mede vorm gegeven aan hoe May en zijn collega privacy-activisten dachten over online privacy en elektronische betalingen. Maar een paar jaar na het starten van zijn digitale geldproject, maakte deze baanbrekende cryptograaf fundamenteel andere afwegingen dan de meeste van de Cypherpunks.

Teleurgesteld schreef May naar de Cypherpunk-mailinglijst: 'Als het gaat om volledig ontraceerbaar digitaal geld, het echte e-geld, dan zijn wij misschien wel de vaandeldragers hiervan.'[166]

---

164 Tim May, ''Stopping Crime' Necessarily Means Invasiveness', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, October 17, 1996, online

165 Tim May, 'Untraceable Payments, Extortion, and Other Bad Things', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, December 21, 1996, online

166 Tim May, 'Stopping Crime'.

Octrooien

Sommige van de Cypherpunks kwamen wel met oplossingen om een eCash-achtig systeem met volledige privacy voor zowel kopers als verkopers te creëren

Zooko stelde bijvoorbeeld dat het probleem makkelijk opgelost kon worden als gebruikers pseudonieme bankrekeningen mochten hebben: banken kunnen een eCash-betaling niet aan een echte identiteit koppelen als ze de echte identiteit van hun rekeninghouders überhaupt niet kennen (de Cypherpunks spraken soms over offshore bankieren in deze context).

Nick Szabo stelde een andere aanpak voor. Verkopers zouden misschien de eCash die ze hebben ontvangen kunnen ruilen met de eCash van een ander persoon, en dan deze 'nieuwe' eCash naar de bank sturen. Op deze manier zou de oorspronkelijke betaling niet gelinkt kunnen worden aan de echte identiteit van de ontvanger. Natuurlijk zou dit wel vertrouwen vergen in de persoon die de eCash uitwisselt. De uitwisselaar zou immers nog steeds kunnen samenwerken met de bank om de identiteit van de eCash-ontvanger te onthullen, of zelfs de eCash kunnen stelen door halverwege de transactie af te haken.

Een derde optie werd voorgesteld door een anonieme deelnemer aan de mailinglijst die een plan bedacht waarbij de verkoper betrokken was bij de aanvankelijke creatie van de eCash. In het originele eCash-protocol zijn alleen de koper en de bank betrokken bij de generatie van blinde sleutels en blinde handtekeningen. Echter, in dit protocol zou ook de uiteindelijke ontvanger van de elektronische valuta een laag van versleuteling toevoegen.

Maar voor al deze oplossingen was er één groot probleem: David Chaum bezat het patent op het algoritme voor de blinde handtekening. En de Cypherpunks waren van mening dat hij zijn product alleen zou licenseren aan 'respectabele' organisaties die zijn technologie, naar zijn mening, niet in diskrediet zouden brengen. Het spreekt voor zich dat de Cypherpunks concludeerden dat hij het niet aan hun gevarieerde groep van crypto-anarchisten en privacyfundamentalisten zou licenseren.[167]

Deze realiteit was een bron van frustratie voor de Cypherpunks, wellicht het best verwoord in een uitgebreide post op een mailinglijst door Tim May. Door

167 Douglas Barnes, 'Re: cypherpunks digicash bank?', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, October 8, 1995, online

zowel de hackerethiek als de Extropian-filosofie te belichamen, betoogde de medeoprichter van de groep dat technologische vooruitgang het best werd bereikt door experimenteren en concurrentie. Hij bepleitte dat softwarepatenten beide belemmerden.

Fysieke producten, zelfs als ze gepatenteerd zijn, kunnen na aankoop tenminste naar wens gebruikt worden, merkte May op. Gepatenteerde microchips, bijvoorbeeld, werden in de jaren '80 vrijelijk gebruikt door onafhankelijke technologen om hun eigen computers te bouwen, wat de revolutie van de persoonlijke computer in gang zette. In vergelijking daarmee leggen softwarelicentieregelingen allerlei beperkingen op hoe de software gebruikt kan worden, zelfs nadat deze is aangeschaft, wat verdere innovatie effectief doodt.

'[…] het heikele punt is dat de patenten op de software-ideeën en -concepten betekenen dat experimenteerders, ontwikkelaars, en hackers geen licentie kunnen kopen voor digicash op dezelfde manier als ze zouden doen voor sommige IC's; en vervolgens experimenteren, ontwikkelen en hacken', legde May uit. 'De man in zijn garage die een 'digitale postzegel' probeert te ontwikkelen, kan bijvoorbeeld de Chaumiaanse verblindingsprotocollen niet gebruiken zonder advocaten in te huren, Chaum zijn voorafgaande vergoeding te betalen, en zijn ontwerpen en bedrijfsplannen (die hij waarschijnlijk zelfs niet heeft!) te openbaren.'[168]

Hierdoor verwachtte May dat de ontwikkeling van digitaal geld tot stilstand zou komen. Hoewel David Chaum op dit gebied ongetwijfeld een pionier was, begonnen de Cypherpunks de cryptograaf steeds meer te zien als iemand die de toekomst van het elektronisch geld eerder hinderde dan bevorderde.

Alternatieven

Als de Cypherpunks het eCash protocol wilden verbeteren, moesten ze daarvoor nog een decennium wachten tot de patenten van Chaum verlopen waren, en dat leek een eeuwigheid. Tim May, Eric Hughes en John Gilmore hadden de Cypherpunk beweging juist opgezet omdat ze al gefrustreerd waren door het gebrek aan voortgang in de cryptografie, en dat al ruim tien jaar na de publicatie

168 Tim May, 'Software Patents are Freezing Evolution of Products', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, October 7, 1995, online

van Chaums eerste ontwerpen voor elektronisch geld.

Het was tijd voor een elektronische vorm van geld, en de *Cypherpunks schrijven code*; ze zouden een manier moeten vinden om de patenten te omzeilen. Een manier om dit te doen was door naar alternatieven te zoeken. Chaums voorstellen uit de jaren 80 hadden het begin gemarkeerd van een reeks publicaties in de jaren 90: binnen enkele jaren werden ongeveer 200 papers gepubliceerd over het onderwerp elektronisch geld en werden enkele tientallen nieuwe patenten ingediend.[169] Als een van de meer opvallende voorbeelden ontwierpen Ron Rivest en Adi Shamir (bekend van RSA) in 1996 twee *micropayment*-schema's genaamd PayWord en MicroMint, terwijl in datzelfde jaar de NSA ook een elektronisch geldschema zou presenteren.[170]

Van tijd tot tijd stelden diverse Cypherpunks op de mailinglijst ook alternatieve ontwerpen voor elektronisch geld voor. Als een vroeg, en nogal origineel, voorbeeld presenteerde de informaticastudent Hadon Nash een digitaal valutaschema dat hij 'Digitaal Goud' noemde. In zijn bericht beschreef Nash een systeem waarbij gebruikers 'eigenaar' zouden zijn van getallen; om het even welk getal, maar lagere getallen zouden een lagere waarde hebben. Een getal claimen was net zo simpel als het produceren van een cryptografische handtekening met dat getal, en de eerste persoon die het claimde zou het 'bezitten'. Het overdragen van het eigendom van een getal werd gedaan met een bericht dat de nieuwe eigenaar bevatte, alleen geïdentificeerd met een publieke sleutel, en een cryptografische handtekening die aantoonde dat de oorspronkelijke eigenaar de overdracht goedkeurde. De eigendomsgeschiedenis van elk getal kon dan worden gevolgd door een reeks cryptografische handtekeningen.[171]

De meeste ontwerpen voor elektronisch geld introduceerden echter niets baanbrekends. Als het over privacyfuncties gaat, waren er veel, waaronder het door de NSA voorgestelde schema, die slechts variaties waren op of iteraties van het ontwerp van Chaum. En degenen die wel een vernieuwende aanpak

169 Eduard de Jong, 'Electronic Money: From Cryptography and Smart Cards to Bitcoin and Beyond', Fraunhofer SmartCard Workshop 2017 .

170 Laurie Law, Susan Sabett, and Jerry Solinas, 'How To Make a Mint: The Cryptography of Anonymous Electronic Cash', National Security Agency Office of Information Security Research and Technology, Cryptology Division, June 18, 1996, online

171 Hadon Nash, 'Digital Gold', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, August 24, 1993, online

introduceerden, hadden vaak andere fundamentele beperkingen. Zo konden de elektronische geldschema's van Rivest en Shamir bijvoorbeeld alleen echt nuttig zijn voor tamelijk specifieke soorten betalingen van lage waarde, omdat de geldigheid van de valuta-eenheden snel zou verlopen.

Andere ideeën waren op een fundamenteler niveau gebrekkig, zoals Nash's 'Digital Gold'-oplossing, die geen rekening hield met het probleem van dubbel uitgeven. Zoals Hal Finney op de Cypherpunk-mailinglijst aangaf, als hetzelfde nummer werd overgedragen aan meerdere publieke sleutels, zouden verschillende gebruikers kunnen eindigen met uiteenlopende eigendomsregistraties (Nash stelde wel een systeem voor waarin gebruikers bij 'agentschappen' zouden moeten controleren of een munt door hen zou worden geaccepteerd voordat ze deze zelf accepteerden, wat zou bewijzen dat het nummer niet dubbel werd uitgegeven, maar dit deel van het voorstel was niet erg goed uitgewerkt).

'Ik moet echter wel zeggen', schreef Finney, 'dat ondanks het feit dat ik niet echt denk dat het voorstel voor digitaal goud technisch haalbaar is, het idee om eigenaar te zijn van getallen enorm brutaal en behoorlijk creatief is.'[172]

De experimenten

Omdat er maar weinig veelbelovende alternatieven leken te zijn, was een populaire methode om Chaums patenten te omzeilen dus om onder de radar te blijven.

Verschillende Cypherpunks zouden uiteindelijk hun eigen versies van eCash implementeren, maar om rechtszaken te voorkomen, waren deze digitale geldsystemen alleen bedoeld voor testdoeleinden. Ze gingen ervan uit dat hun experimentele projecten getolereerd zouden worden, zolang ze geen commerciële intenties hadden en niet gebruikt werden om echte waarde over te dragen.

Midden 1994 vertegenwoordigden de speelgeldschema's een kleine trend onder de Cypherpunks. Zo lanceerde Matt Thomlinson, een bijdrager aan de mailinglijst, een implementatie van eCash die hij Ghostmarks noemde. Tegelijkertijd lanceerde Pr0duct Cypher, een pseudoniem individu die ook bijdroeg aan PGP, Magic Money. En Mike Duvos, een andere terugkerende gast op de mailinglijst,

172 Hal Finney, 'Digital Gold, a bearer instrument?', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, August 26, 1993, online

beheerde een Magic Money implementatie die hij Tacky Tokens noemde.

Bovendien presenteerde iemand die zichzelf Black Unicorn noemt, zelfs het 'volledig gedekte' DigiFrancs systeem:

'DigiFrancs worden gedekt door 10 kratten Light Cola, die zich in de 'kluis' van UniBank in Washington, DC bevinden. DigiFrancs kunnen worden ingeruild voor hun equivalent in ongekoelde Light Cola blikjes op aanvraag, in Washington, DC. Deze regeling impliceert geen overeenkomst tussen enige van de partijen en de Coca-Cola maatschappij.'[173]

Hoewel dit uiteraard als grap bedoeld was (zelfs de door Light Cola gedekte DigiFrancs waren niet daadwerkelijk bedoeld om als geld te worden gebruikt), kregen de verschillende soorten elektronisch geld toch enige bekendheid als ruilmiddel. Sommige Cypherpunks accepteerden deze speelvaluta in ruil voor digitale snuisterijen zoals GIFs.

Het waren niet bepaald grote waardeoverdrachten, maar het riep wel een interessante vraag op.

'Nu, als je nog wakker bent, komt het leuke deel', kondigde Pr0duct Cypher aan, nadat hij de technische details van Magic Money op de mailinglijst had uitgelegd. 'Hoe introduceer je echte waarde in je digicash systeem? Hoe krijg je mensen eigenlijk zover dat ze het willen proberen?'

Chaum wilde zijn eCash-systeem implementeren via bestaande financiële instellingen, waar digitale geld-eenheden inwisselbaar zouden zijn voor echte dollars (of andere fiatvaluta). eCash zou in feite gedekt worden door geld op de bank, wat — hopelijk — mensen genoeg vertrouwen zou geven om dit nieuwe type geld als betaling te beginnen accepteren.

Maar Pr0duct Cypher stelde nu voor dat deze inlosbaarheid voor een dollar misschien niet echt nodig was. Misschien, speculeerde hij, zou digitaal geld helemaal geen dekking nodig hebben.

'Wat maakt goud waardevol?' vroeg hij retorisch. 'Het heeft enkele nuttige eigenschappen: het is een goede geleider, is bestand tegen corrosie en chemicaliën, enzovoorts. Maar die zijn pas recent van belang geworden. Waarom is goud al duizenden jaren waardevol? Het is mooi, het glanst, en het allerbelangrijkste, het

173 Black Unicorn, 'DigiCash Announcement', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, May 10, 1994, online

is schaars.' Pr0duct Cypher concludeerde: 'Jouw digitaal geld moet schaars zijn.'[174]

Gedekt digitaal geld

Gedurende de volgende paar jaar, midden jaren negentig, kwamen onderwerpen als de aard van geld, waarde en dekking van valuta regelmatig ter sprake op de mailinglijst van de Cypherpunks. Het was logisch dat de Cypherpunks deze kwesties bespraken, want om elektronisch geld te creëren, moesten ze begrijpen wat het eigenlijk waarde zou geven. Waarom zou iemand echte producten of diensten opgeven in ruil voor een nummer op een scherm?

Het bleek dat diverse leden van de lijst hierover zeer uiteenlopende ideeën hadden.

Sommigen beschouwden digitaal contant geld echt niet als iets waardevols en dachten zelfs dat het een beetje ongepast was om er in monetaire termen over te praten. Software-ontwikkelaar Perry Metzger, een van de actievere leden in discussies over digitaal geld, beweerde bijvoorbeeld dat een term zoals 'anonieme digitale bankcheques' in feite een nauwkeurigere beschrijving zou zijn.

'Hetzelfde geldt voor een cheque die kan worden GEBRUIKT voor geld, maar in feite een manier is om geld OVER TE DRAGEN, digicash is van zichzelf geen bron van waarde, het is een boekhoudsysteem voor iets dat waarde heeft', schreef hij. 'Dat iets kan dollars zijn, goud, cocainefutures gecontracteerd op de Bogota Commodity Exchange, koekjes, of alles wat mensen besluiten een goed ruilmiddel te vinden.'[175]

Anderen, zoals Eric Hughes, hadden er geen probleem mee om digitaal contant geld als een vorm van geld te beschouwen, maar waren het ermee eens dat de bits en bytes gedekt moesten worden door *iets* van waarde; in de meeste gevallen zou een conventionele fiatvaluta zoals de dollar of het pond de voor de hand liggende keuze zijn. Hij geloofde dat voor de popularisatie van elektronisch geld, gebruikers de garantie moesten krijgen dat ze hun digitale geld kunnen inruilen voor een vastgesteld bedrag aan 'echt' geld.

---

174 Pr0duct Cypher, 'Magic Money Digicash System', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, February 4, 1994, online

175 Perry E. Metzger, 'Re: Virtual Cash', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, May 3, 1994, online

Een andere visie kwam van Robert Hettinga, een Cypherpunk die (in zijn eigen woorden) ooit in 'de kooi van Morgan Stanley in Chicago' werkte.[176] Als een andere zeer actieve deelnemer in discussies over geld en elektronisch geld op de Cypherpunk-mailinglijst, betoogde Hettinga dat de behoefte aan inwisselbaarheid voor 'echt' geld na verloop van tijd zou verdwijnen, aangezien mensen langzaam vertrouwen zouden krijgen in de nieuwe digitale munteenheid.

Hij maakte een analogie met de evolutionaire biologie, en schreef:

'Vergeet niet dat de eerste vleugels geëvolueerd zijn door op vijvers scherende insecten zodat ze sneller over vijvers konden glijden. Na verloop van tijd, toen die beginnende vleugels uiteindelijk volledige vleugels werden, hadden de vliegende insecten geen vijvers meer nodig. Met dat idee in gedachten, zullen digitale waardepapieren voorlopig nog moeten interfacen met de wereld van fysieke boekhouding, om te kunnen worden omgezet in andere activa.'

Maar, zo voorspelde Hettinga: 'Uiteindelijk zullen die activa op een gegeven moment niet langer boekvermeldingen zijn.'[177]

Tim May daarentegen geloofde niet dat geld überhaupt door iets gedekt moest zijn. In lijn met Hayeks vooruitziende principe van vrije banken, stelde hij dat het uiteindelijk allemaal neerkwam op toekomstige verwachtingen: mensen hadden slechts vertrouwen nodig dat geld zijn koopkracht zou behouden.

'Ik geloof dat alle vormen van geld, of het nu harde valuta of fiat is, voortkomen uit de verwachting dat het geld in de toekomst ongeveer dezelfde waarde zal hebben', schreef hij. 'Noem het 'de theorie van de grotere dwaas van geld.' Alles wat je belangrijk vindt, is dat een grotere dwaas het geld zal aanvaarden.'[178]

Maar toch zag May elektronische valuta niet echt als geld op zich. Hij beschouwde het eerder als iets nieuws, een manier om geld over te maken van de ene bankrekening of opslagplaats naar de andere, eerder vergelijkbaar met cheques of bankoverschrijvingen. Hoewel hij dus niet geloofde dat digitale valuta op de traditionele manier 'gedekt' hoefde te worden, ging May er wel van uit dat banken of bankachtige instanties die valuta uitgeven, uiteindelijk controle

176 Robert Hettinga, 'Re: digital cc transactions, digital checks vs real digital cash', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, May 3, 1997, online

177 Robert Hettinga, 'Re: Bypassing the Digicash Patents', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, April 29, 1997, online

178 Tim May, 'Re: alternative b-money creation', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, December 11, 1998, online

zouden hebben over de daadwerkelijke munteenheid die het elektronisch geld dekt: 'Wat digitale valuta echt ondersteunt, is de reputatie van de instanties (die ze uitgeven).'[179]

Tenslotte was er een Britse Cypherpunk die dacht dat elektronisch geld helemaal niet gedekt hoefde te zijn…

Adam Back

Adam Back, een post-doctoraatsstudent in de informatica aan de Universiteit van Exeter en midden in de twintig, had nog nooit in persoon een Cypherpunk bijeenkomst bijgewoond. De mailinglijst had hij wel online gevonden. Hij raakte bijzonder geïnteresseerd in elektronisch geld en werd snel een van de meest actieve deelnemers in de discussies over dit onderwerp.

Back had zelf een beetje geëxperimenteerd met CyberBucks en had uit eerste hand ervaren dat mensen waarde konden toekennen aan puur digitale, ongedekte munten. CyberBucks, gebaseerd op niet veel meer dan een belofte over het totale aanbod, werden verhandeld voor echt geld en gebruikt in echte handel, ook al was het maar in een kleine niche in een obscure hoek van het internet.

Hoewel CyberBucks direct waardeloos werden op het moment dat de server van DigiCash offline ging, zag Back geen enkele reden waarom een nieuw en beter elektronisch geldsysteem op dezelfde manier geen waarde kon krijgen, en het zelfs beter kon doen.

'Waarom koppel je je eCash systeem niet los van dollars door kredietkaarten / debitkaarten / cheques / cash, en zet je een volledig op zichzelf staand systeem op?' stelde hij voor op de Cypherpunk-mailinglijst in april 1997.[180]

'Wat we willen, is volledig anonieme eenheden van uitwisseling, met ultra lage transactiekosten en overdraagbaarheid. Als we dat voor elkaar krijgen […] dan zullen de banken verworden tot de verouderde [dinosaurussen] die ze verdienen te zijn', voegde Back een paar dagen later toe in een volgende e-mail. 'Ik denk dat dit een goede uitkomst zou zijn, en ik zie dit liever gebeuren dan dat iemand veel

179 Tim May, 'What backs up digital money?', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, March 27, 1996, online

180 Adam Back, 'Re: Bypassing the Digicash Patents', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, April 30, 1997, online

moeite doet om de banken erbij te betrekken.'[181]

Back geloofde dat de krachten van vraag en aanbod de waarde van digitale valuta zouden bepalen (net als elk ander product dat op de vrije markt wordt verhandeld). Gebruikers zouden het kopen en verkopen voor traditionele valuta en het accepteren in ruil voor goederen en diensten. Zodra er een marktwaarde werd vastgesteld, kon deze elektronische valuta worden gebruikt om met een simpele muisklik waarde over het internet te verzenden. En vooral: je hoefde niet te maken te hebben met financiële instellingen.

De waarde die mensen aan een ongedekte digitale valuta zouden hechten, voorspelde Back, zou uiteindelijk afhangen van de eigenschappen ervan. Een digitale valuta die, net als contant geld, anoniem gebruikt kon worden, zou naar verwachting meer gewaardeerd worden dan een vergelijkbare digitale valuta die sporen van uitgavenpatronen van gebruikers naliet, bijvoorbeeld. Een digitale valuta die kan blijven bestaan, ongeacht het faillissement van een specifiek bedrijf, zou waarschijnlijk meer waard zijn dan een valuta die het risico loopt 's nachts nutteloos te worden door het offline gaan van een enkele server. En zo verder.

Back presenteerde uiteindelijk een lijst van zes wenselijke eigenschappen voor elektronisch geld[182]:

1. Anoniem (privacy behoudend, zowel ontvanger als betaler blijven onbekend)
2. Gedistribueerd (om het moeilijk te maken het te stoppen)
3. Hebben enige ingebouwde schaarste
4. Vereist geen vertrouwen in een individu
5. Bij voorkeur offline (moeilijk te realiseren met alleen software)
6. Herbruikbaar.

Elk systeem dat deze zes eigenschappen kon bieden, zou echte waarde aantrekken, voorzag Back, en zou zo een echte, ongedekte, digitale munteenheid worden.

Het klonk misschien simpel, maar de post-doctorale onderzoeker in de informatica wist dat het dat zeker niet was. Sommige eigenschappen waren zelfs in

181 Adam Back, 'digital cc transactions, digital checks vs real digital cash', oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, May 2, 1997, online

182 Adam Back, 'Re: Bypassing.'

de meest algemene informatica context lastig te realiseren, terwijl het integreren daarvan in een digitaal valutasysteem hoogstwaarschijnlijk aanzienlijk moeilijker zou zijn. Het succesvol combineren van alle zes in één systeem zou nog veel moeilijker zijn.

Desalniettemin praatte Adam Back niet alleen over elektronisch geld. In echte Cypherpunk-stijl, schreef hij computercode…

Hoofdstuk 10

Hashcash

Adam Back groeide op in de East Midlands van Engeland en had op dertienjarige leeftijd genoeg gespaard om de populaire Sinclair ZX81 te kopen. Dit apparaat kwam voor het eerst op de markt in januari 1981, en had ongeveer de grootte van een faxmachine. Het had een ingebouwd toetsenbord en kon worden aangesloten op de televisie van het gezin. Zo kon de jongen de 8-bits wonderen van het apparaat ontdekken, gewoon in het comfort van zijn eigen woonkamer.

Toen hij na schooltijd met de computer speelde, naast daadwerkelijke videogames soms gewoon door berekeningen te maken om een bepaald effect te bereiken dat hij interessant vond, raakte de jonge Adam Back gefascineerd door de mogelijkheden van de computerwereld.

En hij had er ook talent voor. Omdat er geen *native assembler* beschikbaar was om mens-leesbare broncode om te zetten naar machine-leesbare binaire code (enen en nullen), bedacht de jongen hoe hij zelf een assembler voor de ZX81 kon coderen. Dit vereiste van hem dat hij de meest basale interne werking van de computer *reverse-engineerde*, waarbij hij zelfs binaire codering moest terugvertalen naar broncode om te begrijpen hoe andere programma's werkten.

Toen Back op ongeveer zestienjarige leeftijd naar de universiteit ging, had hij al een geavanceerd begrip van de werking van computers en wist hij dat hij deze discipline wilde blijven verkennen. Hoewel informatica op zijn school op dat moment geen officieel vak was, was er wel een computerlab op de campus. Back maakte er dankbaar gebruik van en besteedde vaak lange dagen in het lab om

zelfstandig meer geavanceerde programmeertalen te leren.

Na het college ging Back computerwetenschappen studeren aan de Universiteit van Exeter, gelegen in het zuidwesten van Engeland. Tijdens zijn studies raakte hij bijzonder geïnteresseerd in gedistribueerd computergebruik, waarbij meerdere computers via een netwerk aan hetzelfde probleem samenwerken, meestal door het probleem op te delen in kleinere stukken (*parallell computing*).

De enorm gemotiveerde Back was regelmatig de primus van zijn klas. Het zette hem begin jaren '90 op weg om zijn interesse diepgaand te kunnen nastreven. Op eenentwintigjarige leeftijd stond de Universiteit van Exeter Back toe om zijn Master over te slaan, en accepteerde ze hem direct in een PhD-programma gefocust op gedistribueerd computergebruik. Gedurende de volgende vier jaar zou hij verschillende coördinatiemethoden voor netwerkcomputers bestuderen, en de mogelijke foutmodi ervan.

Hier werd Back geconfronteerd met langlopende uitdagingen in gedistribueerd computergebruik, zoals het Byzantijnse Generaalsprobleem, waarmee computerwetenschappers al worstelden sinds de late jaren '70. De kern van dit probleem was dat coördinatie over meerdere computers lastig kon zijn op open netwerken, waar kwaadwillige (of zelfs per ongeluk onbetrouwbare) knooppunten zich konden aansluiten en de pogingen van eerlijke deelnemers om een consensus te bereiken konden frustreren.

Het klassieke metaforische verhaal, voor het eerst beschreven door computergoeroe Leslie Lamport, ging over een groep (inderdaad) Byzantijnse generaals die een stad omsingelden.[183] Terwijl elk van hen de situatie inschatte, zouden ze via boodschappers communiceren om te coördineren of ze zouden aanvallen of zich terugtrekken. Hoewel beide opties acceptabel waren, zouden ze allemaal dezelfde keuze moeten maken; het zou een ramp zijn als sommige generaals zouden aanvallen, terwijl anderen besluiten zich terug te trekken.

Het probleem is echter dat er ook verraderlijke generaals (en/of boodschappers, afhankelijk van de versie van de allegorie) zijn, die tegenstrijdige boodschappen (*aanval* of *terugtrekken*) aan verschillende generaals konden sturen, wat tot onenigheid kon leiden. Omdat directe communicatie tussen verschillende partijen

183 Leslie Lamport, Robert Shostak, and Marshall Pease, *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems: 382–401.

onmogelijk is, zouden sommigen eerst de ene instructie (*aanval*) te zien krijgen, terwijl anderen aanvankelijk de andere instructie (*terugtrekken*) zouden zien.

De uitdaging was dus om een protocol te ontwerpen dat elke eerlijke deelnemer onafhankelijk zou kunnen volgen, zodat ze allemaal tot dezelfde conclusie kwamen. Of dit nu de beslissing was om een stad wel of niet aan te vallen, of om consensus te bereiken over hoe een gedeelde computertaak te coördineren.

Dit waren precies het soort uitdagingen waar Adam Back graag zijn hersenen over kraakte.

De Cypherpunk

Als PhD-kandidaat aan dezelfde universiteit kwam Back in contact met een masterstudent die het RSA-encryptieprotocol probeerde te optimaliseren voor parallele berekening. Het leek Back een interessant project, en leunde dicht aan bij zijn eigen onderzoeksgebied. Hij besloot dus om te helpen, wat betekende dat hij zich moest verdiepen in het RSA-algoritme. Het leidde hem op zijn beurt ook naar het bestuderen van Phil Zimmermanns nieuwe PGP-project.

Inmiddels had Back ook een interesse in vrije markten ontwikkeld, en had hij enige sympathie voor anarcho-kapitalisme. De hyperlibertaire ideologie waarin alle functies van de staat volledig worden vervangen door op de markt gebaseerde oplossingen leek op de toekomstige samenleving beschreven in een van zijn favoriete boeken: de cyberpunk-klassieker *Snow Crash*.

Zo vond Back de cryptografische hulpmiddelen waar hij over leerde op sociologisch vlak zeer interessant.

'Minder privacy is negatief voor de vrijemarkteconomie, omdat een afname van privacy leidt tot een toename van overheidsinterventies, grotere overheidsapparaten, fascisme, etc. waardoor de vrijemarkteconomie naar de knoppen gaat', zou hij later verklaren. 'Hierdoor zullen armoede en voedseltekorten ontstaan, vergelijkbaar met wat er gebeurde in de voormalige USSR, die nog steeds langzaam herstelt van de ondergang die veroorzaakt werd door fascistisch overheidsbeleid.'[184]

184 Adam Back, *Re: 'why privacy' revisited*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 22 maart 1997, online

Daarnaast realiseerde de student zich snel dat dit soort technologieën individuen de middelen konden bieden om fundamentele rechten uit te oefenen zoals vrijheid van meningsuiting en vrijheid van vereniging. In wezen ontdekte Back dat cryptografie aanzienlijke implicaties kon hebben voor het machtsevenwicht tussen individuen en de staat.

Toen hij op het internet naar plaatsen zocht om deze onderwerpen te bespreken, ontdekte de jonge PhD-kandidaat uit Exeter dat hij niet de enige was die tot dit inzicht was gekomen.

Aan de overkant van de Oceaan hadden de Cypherpunks net hun reguliere bijeenkomsten georganiseerd en, nog belangrijker, de Cypherpunk-mailinglijst gelanceerd. Back, al programmeur van in zijn kindertijd, was erg geïnspireerd door hun doel om software te schrijven die een positieve sociale impact had en hij meldde zich snel aan voor de mailinglijst.

'Dat was een interessante uitlaatklep', herinnerde Back zich later aan zijn eerste interacties met de Cypherpunks-mailinglijst, 'want mensen waren bezig met andere dingen dan PGP, andere dingen die je kon bouwen met encryptie en cryptografie. Ik heb een groot deel van mijn doctoraat eigenlijk niet besteed aan werken aan gedistribueerde systemen, maar aan leren over cryptografische protocollen, voornamelijk met als toegepaste interesse om te denken over wat een bepaald cryptografie-artikel je zou toestaan om te bouwen.'[185]

In de loop der jaren werd Back een van de meest actieve deelnemers aan de mailinglijst. Soms droeg hij zelfs tientallen e-mails bij in een maand. Hij had een sterke interesse in filosofische onderwerpen zoals privacy, vrije meningsuiting en libertarisme, en nam aan diepgaande technische discussies deel over onderwerpen zoals anonieme remailers of versleutelde bestandssystemen (technologieën waaraan hij ook heeft bijgedragen).

Back raakte ook betrokken bij de *crypto-oorlogen* die niet al te lang na zijn toetreding tot de mailinglijst uitbraken, en werd op veel manieren zeer direct beïnvloed door deze strijd. Toen de Amerikaanse overheid cryptografie reguleerde onder de *US Munitions List*, was het Amerikanen wettelijk niet langer toegestaan om, bijvoorbeeld, het RSA-algoritme met Back te delen, of met een van zijn

185 Adam Back, *The Bitcoin Game #59: Dr. Adam Back*, interview door Rob Mitchell, The Bitcoin Game, YouTube, 25 oktober 2018, online 10:47–11:19.

landgenoten (in het geval van RSA kende Back natuurlijk het algoritme al).

Het verbod raakte bij de jonge Cypherpunk een gevoelige snaar. Hij was van mening dat de betwiste cryptografische protocollen in werkelijkheid individuen alleen maar toestonden om rechten uit te oefenen die zij juridisch gezien al moesten hebben: als privégesprekken zijn toegestaan, waarom zou publieke-sleutelcryptografie dan niet toegestaan zijn? En wellicht nog belangrijker, cryptografie was in feite gewoon wiskunde. Back vond het zowel absurd als zorgwekkend dat de VS in feite het delen van bepaalde getallen en vergelijkingen illegaal maakten.

Het zette de Britse Cypherpunk ertoe aan om op een unieke manier zijn punt te bewijzen. Volgens de activistische ethos van de groep, maakte Back *munitie*-shirts: zwarte t-shirts met het RSA-protocol in witte letters erop gedrukt. Volgens de wet was iedereen die Backs kleding droeg bij het verlaten van de Verenigde Staten, technisch gezien, een wapenexporteur. Hij zou de shirts verkopen aan zijn mede-Cypherpunks en, passend, DigiCash's proefvaluta CyberBucks als betaling accepteren. Passend genoeg, want mogelijk meer dan wat dan ook, was Adam Back bijzonder geïnteresseerd in elektronisch geld.

In actie komen

Toen Adam Back zich bij de mailinglijst aansloot, was DigiCash werkelijk onbetwistbaar op gebied van anonieme digitale valuta. Maar de voortgang van eCash verliep minder snel dan hij en vele anderen hadden gewenst.

Back deelde de visie van de Cypherpunks dat dit grotendeels kwam omdat David Chaum zijn patenten gebruikte om zijn technologie exclusief te houden. Hij vond dat het beleid van DigiCash, met zijn ingewikkelde licentieschema's en beperkingen op wat gebruikers wel en niet met de eCash-technologie konden doen, ervoor zorgde dat hackers en knutselaars geen kans kregen om met de technologie te experimenteren en ze te verbeteren. Door dit beleid was de technische vooruitgang vrijwel tot stilstand gekomen.

Back verpersoonlijkte de Cypherpunk-filosofie en was niet het type dat rustig zou afwachten tot de zaken veranderden. In de hoop dat het de zaken zou versnellen, schreef Back initieel software-*libraries* (broncode die door andere

ontwikkelaars kon worden gebruikt) voor zowel eCash als Brands Cash. Laatstgenoemde is een op eCash geïnspireerd elektronisch geldsysteem ontworpen door voormalig DigiCash-medewerker Stefan Brands. Terwijl hij hiermee bezig was, ontdekte Back ook hoe hij Brands' systeem kon uitbreiden om offline transacties te vergemakkelijken, zonder de noodzaak om bij elke betaling bij de bank op dubbele uitgaven te controleren (hoewel bleek dat iemand anders dat probleem al eerder had opgelost toen hij het met Brands besprak).

Toen eCash te midden de jaren 90 nog steeds niet echt van de grond kwam, begon Adam Back pas echt ongeduldig te worden. 'Technologie voor blinde handtekeningen bestaat al geruime tijd, maar er is niet één voorbeeld van een praktisch, echt wereldwijd gebruik van deze technologie', schreef Back gefrustreerd naar de Cypherpunk-mailinglijst in oktober 1995.[186]

Hij merkte op dat niet-anonieme internetbetaalsystemen snel marktaandeel veroverden, wat betekende dat de toekomst van digitale transacties een gevaarlijke richting insloeg. Als deze privacy-schendende alternatieven zich eenmaal in de gewoonten van mensen zouden verankeren als hun standaard online betalingsoplossingen, geloofde hij dat het aanzienlijk moeilijker zou zijn om internetgebruikers over te laten stappen naar anoniem digitaal geld.

Het was tijd om actie te ondernemen. Aangezien Back niet veel vertrouwen had in de voortgang van DigiCash, en het leek alsof niemand anders aan haalbare alternatieven voor eCash werkte, concludeerde hij dat de snelste weg naar succes misschien wel was om met Chaum samen te werken. Hij stelde voor dat een groep Cypherpunks een start-up bank zou oprichten en eigenlijk de technologie van DigiCash zou licentiëren om zelf door fiatgeld gedekte eCash uit te geven.

'Ik meen het serieus en zou erin willen investeren', maakte Back duidelijk op de mailinglijst. 'Wat denken jullie ervan? De eerste DigiCash-bank, *gerund* en eigendom van een groep Cypherpunks?'[187]

De enige persoon die reageerde op zijn voorstel wees erop dat dit plan waarschijnlijk ook niet zou werken: Chaum wilde tenslotte zijn technologie niet

186 Adam Back, *Re: cypherpunks digicash bank?*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 8 oktober 1995, online

187 Adam Back, *cypherpunks digicash bank?*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 7 oktober 1995, online

in licentie geven aan een bende Cypherpunks.[188] Het idee stierf een stille dood.

Twee jaar later, in de zomer van 1997, keerde Back terug naar de mailinglijst om het idee van een gedistribueerde bank voor te stellen. Nu hij met succes zijn doctoraatsprogramma had afgerond en als postdoc-onderzoeker aan de universiteit werkte, maakte hij deze keer echt gebruik van zijn expertisegebied. Hij legde uit dat de operaties van een bank over een netwerk van verschillende mensen of entiteiten verspreid konden worden. Ze zouden in staat zijn om een virtuele computer te simuleren door berichten uit te wisselen en gecodeerde functies te berekenen, opperde Back, waarbij de virtuele computer in feite zou functioneren als een reguliere bank.

Door de bank op te splitsen in meerdere, onderling afhankelijke, partijen, zou er geen enkele entiteit volledig vertrouwd hoeven te worden met de bankoperaties. En hoewel het Byzantijnse Generaalsprobleem nog steeds niet volledig was opgelost, kon het systeem alleen worden misleid als een bepaald aantal deelnemers samenspanden.

'De bank zou bestaan binnen het netwerk, in deze virtuele CPU', schreef Back. 'Individuele deelnemers kunnen komen en gaan, maar de beveiligde softwareentiteit, die de bank en de accountinformatie is, zou blijven voortbestaan.'[189]

Hij kreeg geen antwoord op zijn e-mail.

Spam

In de tweede helft van de jaren '90 moest elke e-mailservice op het internet omgaan met ogenschijnlijk steeds toenemende hoeveelheden ongewenste mail, of *spam*: ongevraagde berichten die in bulk werden verzonden, doorgaans door adverteerders. De Cypherpunks werden hierbij niet gespaard; promoties voor afslankpillen, producten voor penisvergroting en aanbiedingen om snel rijk mee te worden veroorzaakten alsmaar meer vervuiling op de mailinglijst.

Het probleem was vooral ernstig voor de remailers. De anonimiserende diensten die door verschillende Cypherpunks werden beheerd, werden gemakkelijk en vaak misbruikt om spam te versturen. Sommige van de beheerders vermoedden

188 Barnes, *cypherpunks digicash*.

189 Adam Back, *distributed virtual bank*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 27 augustus 1997, online

zelfs dat hun remailers het doelwit waren van zogenoemde *denial-of-service* (DOS) aanvallen; het doel zou zijn geweest om de remailers te overladen met nutteloze e-mails om hun dienst onbruikbaar te maken voor legitiem gebruik.

Adam Back, die zelf ook een remailer beheerde, was lid van een groep Cypherpunks die zich toelegde op het oplossen van dit probleem. En nog belangrijker, ze probeerden dit probleem op te lossen zonder terug te vallen op oplossingen die internetgebruikers verplichtten zich te identificeren. Want voor remailers was privacy het belangrijkste punt.

Ze wilden ook niet afhankelijk zijn van wetten en regelgeving. Hoewel er stemmen opgingen om spam e-mails eenvoudigweg illegaal te maken, was het niet de stijl van de Cypherpunks om de overheid in te schakelen om hun problemen op te lossen.

De overheid het probleem niet laten oplossen, was ook belangrijk omdat het niet altijd duidelijk was wat precies als spam beschouwd kon worden. Als de staat de autoriteit krijgt om dat onderscheid te maken, zou dat effectief regeringen toestaan om te bepalen welke vormen van communicatie tussen internetgebruikers acceptabel zijn en welke niet. Dit zou de deur kunnen openen voor politiek gemotiveerde censuur, waarschuwden Cypherpunks zoals Tim May.[190]

Adam Back benadrukte dat om spammers wettelijk verantwoordelijk te kunnen houden, ze ook geïdentificeerd dienen te worden. Als een overheidsdienst tegen spam de taak krijgt om de daders te vangen, waarschuwde Back zijn mede-Cypherpunks, dan zouden remailers waarschijnlijk een groot doelwit worden, met mogelijk ernstige gevolgen voor online privacy in het algemeen.[191]

'De gevaren van het inzetten van de overheid om spammers aan te vallen, is dat dit het internet is, en we willen geen regulering van de inhoud door overheden, noch pogingen tot afdwingen van *escrow van identiteit*, *internetrijbewijzen* of iets anders', schreef Back aan de Cypherpunk-mailinglijst. 'We lossen het zelf wel op zonder de behoefte aan overheidsinterventie, hartelijk dank.'[192]

De Cypherpunks waren het er over het algemeen over eens dat een digitaal

190 Tim May, *Re: More on digital postage*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 15 februari 1997, online

191 Adam Back, *Re: bulk postage fine* , oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 3 augustus 1997, online

192 Adam Back, *no government regulation of the net*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 3 augustus 1997, online

equivalent van postzegels een betere oplossing zou zijn. Spammers zouden ontmoedigd worden indien het verzenden van e-mails een kost had. Dit was vooral relevant omdat spammers vaak tienduizenden, zo niet miljoenen ongewenste e-mails moesten versturen om winst te maken. Het zou ook de overbelasting van remailers voorkomen, aangezien zo'n DOS-aanval een grote hoeveelheid ongewenste e-mails vereiste.

Digitale postzegels konden op verschillende manieren worden ingezet. Remailers konden bijvoorbeeld kosten rekenen voor het doorsturen van e-mails. Dit zou niet alleen spam via deze diensten ontmoedigen, maar het zou ook een financiële prikkel bieden om remailers te beheren. Daarnaast kon een vergoeding worden toegekend aan de ontvanger, wiens e-mailsoftware zo geprogrammeerd zou zijn dat berichten zonder voldoende vergoeding werden geweigerd.

De postzegels zelf konden op verschillende manieren worden ontworpen, maar de meeste ideeën omvatten een uitgever van elektronische zegels. Deze uitgever genereerde bijvoorbeeld unieke grote getallen en verkocht deze (mogelijk in ruil voor digitaal geld). Het unieke nummer werd dan opgenomen in een e-mail, en zodra een remailer of de e-mailsoftware van de ontvanger het bericht ontving, controleerde het bij de uitgever of het nummer een geldige postzegel was. Als dat het geval was, kon de remailer of ontvanger mogelijk een klein bedrag terugkrijgen van de uitgever, afhankelijk van de kenmerken van het systeem. Was de postzegel niet geldig, dan werd de e-mail simpelweg geweigerd.

Een andere optie was om digitale contanten direct als postzegel te gebruiken. In dat geval bevatte de e-mail een klein beetje digitale valuta in een speciaal veld, die de ontvanger vervolgens kon innen. Er was een periode waarin dit een veelbelovende toepassing voor eCash leek te zijn.

In de praktijk bleek dit echter ingewikkelder dan verwacht. Ten eerste waren de vroege versies van eCash nog niet in staat om de specifieke soorten transacties die voor postzegels nodig waren te verwerken. Daarnaast betekende het gebrek aan anonimiteit in Chaums elektronische geldsysteem dat de verzender van een bericht zou kunnen samenwerken met de bank om de echte identiteit van een remailer-operator of e-mailontvanger te onthullen. Het maakte DigiCash's eCash grotendeels ongeschikt voor postzegels.

De eerste elektronische postzegel

Wat Adam Back niet wist, was dat het postzegelprobleem al een paar jaar eerder was opgelost, en op een heel andere manier dan de Cypherpunks hadden overwogen.

In de vroege jaren '90 realiseerden Cynthia Dwork en Moni Naor, twee computerwetenschappers bij IBM, zich dat een elektronisch mailsysteem veel voordelen had ten opzichte van de traditionele post: e-mail was veel sneller, veel goedkoper, en bood veel meer mogelijkheden dan de postdienst ooit zou kunnen bieden. Maar ze realiseerden zich ook dat e-mail zijn eigen uitdagingen met zich meebracht. Ze voorzagen dat met de toenemende populariteit van e-mail, ook spam zou toenemen.

'Met name de eenvoud en lage kosten om elektronische post te versturen, en dan vooral het gemak om eenzelfde bericht naar veel verschillende partijen te sturen, nodigen in principe uit tot misbruik', legden ze uit in hun paper uit 1992, getiteld *Pricing via Processing of Combatting Junk Mail.*[193].

Er was een oplossing nodig, stelden ze vast, en dat was precies wat het artikel leverde. Dwork en Naor stelden een systeem voor waarbij afzenders een beetje extra data aan hun e-mail moeten toevoegen. De data zou de oplossing voor een wiskundig probleem zijn, afgeleid van de eigenschappen van de e-mail zelf, en dus uniek voor die e-mail. Zonder de correcte oplossing, zouden e-mail*clients* de e-mail volledig moeten afwijzen.

In hun artikel stelden Dwork en Naor drie mogelijke puzzels voor, gebaseerd op cryptografische algoritmen zoals handtekeningsschema's. In alle gevallen zou het toevoegen van de juiste oplossing aan een e-mail niet al te moeilijk zijn (voor een computer): het zou wellicht een paar seconden aan rekenkracht vereisen. Toch zou dit een kleine kostenpost betekenen. Controleren of de oplossing correct is, zou daarentegen zeer makkelijk zijn en nauwelijks enige rekenkracht kosten.

De kerngedachte achter dit systeem was dat het oplossen van een juiste oplossing voor een puzzel niet veel moeite zou kosten voor individuele gebruikers die af en toe een e-mail willen sturen naar collega's, familie of vrienden. Maar voor spammers zou het snel oplopen. Om duizenden of zelfs miljoenen berichten op

193 Cynthia Dwork and Moni Naor, *Pricing via Processing or Combatting Junk Mail*, Advances in Cryptology — *Crypto* '92: 139–147.

een enkele dag te sturen, zouden zij evenveel puzzels moeten oplossen, wat in totaal aanzienlijke hoeveelheden rekenkracht zou vereisen.

'Het idee is om een gebruiker een matig moeilijke, maar niet onoplosbare, functie te laten berekenen om toegang te krijgen tot de hulpbron, en zo lichtzinnig gebruik te voorkomen', legden Dwork en Naor uit. Ze stelden voor om spammen in een dure aangelegenheid te veranderen.

Hoewel Dwork en Naor de term zelf niet hebben voorgesteld, zou de soort oplossing die zij introduceerden later bekend komen te staan als een *proof-of-work*-systeem. Het oplossen van het wiskundeprobleem zou bewijzen dat er daadwerkelijk *werk* is verricht.

Het was een elegante oplossing. Maar of het nu kwam omdat het idee voor die tijd iets te vooruitstrevend was, of omdat het simpelweg niet breed genoeg werd geadverteerd, kreeg het voorstel uit de vroege jaren 90 niet veel aandacht buiten een beperkte groep academici. Het postzegelsysteem van Dwork en Naor is nooit in de praktijk gebracht, laat staan gebruikt, en veel van de Cypherpunks kenden het idee zelfs niet. Gelukkig zou het concept weldra opnieuw worden uitgevonden.

Hashcash

[MEDEDELING] implementatie van hash cash porto

Op 28 maart 1997 kregen de inmiddels ongeveer 2000 abonnees van de Cypherpunk-mailinglijst een bericht in hun inbox.[194] Het bericht werd verstuurd door Adam Back en bevatte een beschrijving en vroege implementatie van wat hij *hashcash* noemde: een 'postzegelsysteem gebaseerd op gedeeltelijke hash-botsingen'. Hij had een werkende implementatie van een postzegel-oplossing voor e-mail ontworpen.

Net als het schema van Dwork en Naor, zou de hashcash porto niet betaald worden aan operators van remailers, of aan de ontvangers van een e-mail, of aan wie dan ook. In plaats daarvan zou het alleen extra kosten met zich meebrengen voor de verzenders.

---

194 Adam Back, *ANNOUNCE hash cash postage implementation*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 28 maart 1997, online

Een week eerder had Back al nagedacht over het tegengaan van spam door de kosten van massa-mail te verhogen, hoewel nog vrij oppervlakkig: 'Een nevenvoordeel van het gebruik van PGP is dat PGP-versleuteling enige meerkost zou betekenen voor de spammer: hij kan waarschijnlijk minder berichten per seconde versleutelen dan hij kan spammen via een T3-link', merkte hij op in een discussie over het toevoegen van extra privacy aan remailers.[195]

Het nieuwe voorstel van Back maakte dit algemene idee nog explicieter: het zou vereisen dat afzenders een bewijs van geleverd werk aan hun e-mails toevoegen. Inderdaad, hashcash was op verschillende manieren vergelijkbaar met het postzegelschema van Dwork en Naor: het *proof-of-work* zou uniek zijn voor de e-mail, en het zou een beetje rekenkracht vereisen om te produceren.

Zoals de naam al doet vermoeden, was het voorstel van Back echter gebaseerd op hashing. Hashing – de cryptografische truc die alle data in een unieke en schijnbaar willekeurige reeks getallen van een specifieke lengte omzet – is een volkomen onvoorspelbaar proces. Hoewel dezelfde data altijd hetzelfde hashresultaat oplevert, is de enige manier om te ontdekken hoe de hash van een stuk data er in de eerste plaats uit zal zien, om het daadwerkelijk te hashen. Het is deze onvoorspelbaarheid waar hashcash op slimme wijze gebruik van maakte.

Om *hashcash* te genereren, moest een gebruiker een hash creëren uit de metadata van een e-mail (zoals het adres van de verzender, het adres van de ontvanger, de tijd enz.) en een willekeurig nummer, een zogenaamde *nonce*. Maar hier zat een addertje onder het gras: niet elke resulterende hash werd als *geldig* beschouwd. De binaire versie van een geldige hash moest beginnen met een vastgesteld aantal nullen. En er was maar één manier om een hash te genereren die met voldoende nullen begon: de gebruiker moest verschillende nonces proberen en nieuwe hashes maken tot er één toevallig aan de norm voldeed. *Trial and error* dus.

Het aantal vereiste voorafgaande nullen bepaalt hoe moeilijk het is om een geldige hash te vinden. Meer nullen maken het moeilijker, omdat computers gemiddeld meer pogingen moeten doen.

'De basisgedachte achter het gebruik van partiële hashes is dat ze willekeurig moeilijk te berekenen kunnen zijn,' legde Back uit, 'maar ze kunnen tegelijkertijd

195 Adam Back, *Re: Remailer problem solution?* 23 maart 1997, online

onmiddellijk worden geverifieerd.'

Net als bij de oplossing van Dwork en Naor was het doel dat gewone gebruikers binnen enkele seconden een geldige hash moesten kunnen vinden om een e-mail te versturen. Tegelijkertijd moesten spammers niet in staat zijn om dit duizenden of miljoenen keren te doen en toch winstgevend te blijven.

'[…] als het geen 20 bit hash heeft […] heb je een programma dat het terugstuurt met een bericht waarin de vereiste porto wordt uitgelegd, en waar de software te vinden is', legde Back uit op de Cypherpunk-mailinglijst. 'Dit zou spammers van de ene op de andere dag wegwerken, aangezien 1.000.000 x 20 = 100 MIP jaren, wat meer rekenkracht is dan ze hebben.'

Een subtiele verandering ten opzichte van Dwork en Naors oplossing was dat hun *proof-of-work* systeem niet onderhevig was aan toeval. Hun postzegelschema vereist in principe het oplossen van een vrij eenvoudige puzzel, wat betekent dat een krachtigere computer de puzzel altijd sneller zou oplossen dan een zwakkere computer.

Het genereren van een geldige hash is daarentegen een kwestie van gokken. Hoewel een krachtigere computer meer pogingen per seconde kan doen, kan een zwakkere computer soms geluk hebben en sneller een geldige hash vinden. Voor spammers, die toch duizenden of miljoenen geldige hashwaarden moeten genereren per spamsessie, maakt deze kleine variatie bij het genereren van een enkele hashcash proof-of-work weinig verschil, althans niet binnen de context van het tegengaan van ongewenste e-mails.

'Hashcash kan een tussentijdse oplossing bieden totdat digicash breder wordt toegepast', concludeerde Back in zijn aankondiging. 'Hashcash is gratis, het enige dat je hoeft te doen is wat processorkracht van je PC gebruiken. Het sluit aan bij de online cultuur van vrije communicatie, waarin de financieel minder bedeelden op gelijke voet kunnen concurreren met miljonairs, gepensioneerde overheidsfunctionarissen en dergelijke.'

En: 'Hashcash kan ons een alternatieve methode bieden om spam te beheersen als digicash misloopt (verboden wordt of vereist dat gebruikersidentiteiten in escrow worden gehouden).'

Digitale schaarste

Hashcash werd in de jaren na de aankondiging van Adam Back enigszins geadopteerd. Apache's open source platform *SpamAssassin* implementeerde de oplossing, terwijl Microsoft het idee in hun incompatibele *Postmark* systeem uitprobeerde. Adam Back en enkele andere academici botsten ondertussen op alternatieve toepassingen voor het proof-of-work systeem, waaronder oplossingen tegen DoS-aanvallen.

Maar de hashcash postzegel is nooit echt mainstream gegaan. De innovatieve aard van de oplossing was waarschijnlijk niet voldoende om de opstarthindernis te overwinnen: iemand kon niet echt beginnen met het eisen van hashcash voor binnenkomende e-mails als niemand anders het gebruikte, omdat dit zou leiden tot afwijzing van alle binnenkomende berichten door hun e-mailclient. Tegelijkertijd was er geen reden om hashcash voor uitgaande e-mails te gebruiken als niemand zo'n postzegel eiste. Net als David Chaums eCash, leed ook het elektronische porto-systeem van Back aan een kip-en-ei-probleem, waar geen gemakkelijke oplossing voor leek te zijn.

Adam Back maakte zich hier echter niet zoveel zorgen om. Back, die inmiddels onderzoeker was bij de Universiteit van Exeter en aan een versleuteld berichtensysteem voor medische data werkte, dacht vrijwel onmiddellijk na de publicatie van zijn voorstel al verder dan enkel hashcash. Het oplossen van het postzegelprobleem was een goede uitdaging, maar de computeringenieur was vooral gefascineerd door de gedachte om digitaal geld voor algemene doeleinden te creëren.

En hoewel veel Cypherpunks nog steeds aannamen dat een elektronisch geldsysteem zou moeten worden geïntegreerd in de bestaande financiële infrastructuur, zoals eCash, had Back een andere visie. Hij geloofde dat hashcash een totaal nieuwe richting van onderzoek kon betekenen om die visie te verwezenlijken.

De innovatieve aard van hashcash was dat het puur digitale data (in wezen getallen) aan echte hulpbronnen in de fysieke realiteit koppelde. Een proof-of-work creëren vereiste rekenkracht en verbruikte elektriciteit, die op zijn beurt energie kost om te produceren. Terwijl de meeste digitale dingen kosteloos en bijna eindeloos gekopieerd kunnen worden, kon het proof-of-work op een bepaalde manier de fundamentele schaarste aan energie in de fysieke realiteit naar

de digitale wereld overbrengen.

Inderdaad, hashcash was digitaal, maar toch schaars. Het totale aantal hashcash *valuta-eenheden* (bij gebrek aan een beter woord) was in zekere mate beperkt: er zou nooit meer hashcash zijn dan er kon worden geproduceerd met de hoeveelheid energie die mensen bereid en in staat zouden zijn om eraan te spenderen.

Dit was een cruciaal inzicht, omdat ingebouwde schaarste een van de zes eigenschappen was die Adam Back op zijn lijstje voor een ideaal elektronisch geldsysteem had gezet. Tot voor kort kon digitale schaarste slechts gecreëerd worden als een belofte, zoals DigiCash's belofte om een harde limiet te stellen aan het totale aantal CyberBucks dat ze zouden creëren. Maar beloftes kunnen natuurlijk gebroken worden. Back geloofde dat proof-of-work de mogelijkheid bood om schaarste te garanderen op een veel fundamenteler niveau.

Tegelijkertijd wist hij dat hashcash niet als volwaardig digitaal geld kon functioneren. Hoewel het anoniem kon worden gebruikt, moeilijk te stoppen was, geen vertrouwen in een individu vereiste en ook enige mate van schaarste had, voldeed het eigenlijk slechts aan drie van de zes criteria op de shortlist van Back.

Het grootste probleem was dat hashcash niet herbruikbaar was. Elke munteenheid was op maat gemaakt om bij een specifieke e-mail te passen, en kon dus niet elders opnieuw worden uitgegeven en leverde geen extra voordeel op voor de ontvangers.

Back overwoog daarom dat hashcash, of meer algemeen het proof-of-work-principe, de basis zou kunnen vormen voor een nieuw soort elektronisch geldsysteem.

Een van zijn eerste suggesties was een Chaumiaans systeem, waarin de bank elektronisch geld zou uitgeven in ruil voor hashcash. Gebruikers creëerden dan proof-of-work en ontvingen daarvoor in ruil ongedekt digitaal geld. Dit geld zou anoniem, herbruikbaar en enigszins schaars zijn — al was de schaarste in de praktijk vrij beperkt. Als mensen het wilden konden ze immers altijd meer bewijzen creëren. En met steeds krachtigere computerprocessors zou het produceren van geldig proof-of-work in de loop van de tijd alleen maar goedkoper worden.[196]

196 Back, *Re: Bypassing.*

De fundamentele schaarste van hashcash was dan ook vooral technisch van aard. Als het daadwerkelijk als basis voor een valuta zou dienen, zouden nieuwere en krachtigere computers de markt uiteindelijk overspoelen met nieuwe valuta-eenheden, wat zou leiden tot hyperinflatie.

Daarnaast moest men vertrouwen hebben in de bank dat deze geen geld uit het niets zou creëren. Net als bij elk elektronisch geldsysteem gebaseerd op Chaums ontwerp, moest de entiteit die de digitale valuta uitgaf en dubbele uitgaven voorkwam, zelf ook te vertrouwen zijn om niet onterecht zichzelf te verrijken.

Back geloofde, echter, dat vrijemarktcompetitie kon helpen om dit probleem op te lossen. 'Wellicht zou je dus meerdere banken kunnen hebben en reputatie het werk laten doen, als je de protocollen zo kunt regelen dat het duidelijk zou zijn of een bank meer geld aan het drukken was dan het aan hash-botsingen had ontvangen. […] Maar als je meerdere banken hebt dan moet je een uitwisselingsmechanisme hebben. De markt zou hier waarschijnlijk zorg voor kunnen dragen, door wisselkoersen te bepalen op basis van de reputaties van banken', suggereerde hij, in wat nu heel erg leek op een vrijbankiersysteem zoals beschreven door Friedrich Hayek.

Desalniettemin geloofde de jonge Cypherpunk uit Exeter dat ze het misschien zelfs nog beter konden doen dan dat:

> *'Het zou beter zijn om iets te hebben dat geen vertrouwen vereist en waarin geen mogelijkheid is voor bedrog, in plaats van te vertrouwen op reputatie om ze te sorteren.'*[197]

197 Back, *Re: Bypassing.*

Hoofdstuk 11

Bit Gold

De vader van Nick Szabo was een van de 200.000 Hongaren die hun land verlieten nadat Sovjettroepen de anti-communistische opstand van 1956 hadden neergeslagen. Terwijl tienduizenden van zijn mede-vrijheidsstrijders werden opgesloten of geïnterneerd, en in sommige gevallen zelfs geëxecuteerd, besloot hij alles achter te laten. Uiteindelijk vond hij een nieuwe thuis aan de andere kant van de Atlantische Oceaan, in *het land van de vrijheid*.

Hoewel dit bijna een decennium voor zijn geboorte gebeurde, zou de ervaring van zijn vader Nick vormen. Als zoon van een vluchteling, opgroeiend ver weg van het onderdrukkende Sovjetgezag over Oost-Europa, werd bij de Amerikaanse jongen van de tweede generatie al vroeg een diep wantrouwen tegen alles wat ook maar enigszins leek op communisme of overheidsinmenging ingeplant.[198]

Uiteindelijk vond Szabo een grote bron van inspiratie in de werken van Friedrich Hayek. Het boek *The Road to Serfdom* leek de transformatie van de Sovjet-Unie naar een totalitaire staat nauwkeurig te hebben beschreven, met de onderdrukking van de Hongaarse revolutie als een van de eerste grote voorbeelden hiervan buiten het Russische thuisland. Szabo zou later Hayeks boek uit 1988, *The Fatal Conceit* — een andere, meer politieke, weerlegging van het socialisme, dat de historische belangrijkheid van privé-eigendom benadrukte — noemen als een van de belangrijkste boeken die hij ooit heeft gelezen.[199]

198 Nick Szabo, *Why Cryptocurrency? Governments Abuse Their Power — Nick Szabo Interview Part 1*, interview by Zulu Republic, Zulu Republic, YouTube, 25 oktober 2018, online

199 Nick Szabo , *Some of the most important books I've read*, *X*, 31 januari 2016, online

Ondertussen raakte de jonge Szabo geïnteresseerd in computers, een nieuwe technologie die in die tijd snel evolueerde in de VS en de rest van de Westerse wereld, terwijl het communistische Oosten ver achterbleef. Toen in de late jaren '70 en vroege jaren '80 de eerste computers hun weg vonden naar Amerikaanse huizen en kantoren (zijn moeder nam regelmatig haar Apple II mee naar huis van haar werk) zag hij al snel de mogelijkheden van deze machines. Tegen het midden van de jaren '80 bracht dit hem ertoe om informatica te gaan studeren aan de Universiteit van Washington in Seattle.

Tijdens zijn studie, deed Szabo een jaar stage bij het *Jet Propulsion Laboratory* (JPL), een onderzoekscentrum van NASA, voordat hij in 1989 zijn diploma in de informatica behaalde. Nu midden in zijn twintiger jaren, besloot hij zo'n 1300 kilometer naar het zuiden te verhuizen, naar de San Francisco Bay Area, waar zijn vaardigheden bijzonder gewild waren. Hij vond een programmeerbaan bij IBM, dat gedurende de jaren '80 met zijn relatief goedkope microcomputers de standaard had gezet voor thuiscomputers.

Szabo's persoonlijke interesses waren echter altijd breder dan alleen informatica. Als een echte veelweter, genoot hij ervan om in zijn vrije tijd een scala aan onderwerpen te bestuderen: van politiek tot biologie en van geschiedenis tot economie, met een speciale focus op vrijemarkteconomie. Net als Hayek, die vooral in deze latere fase van zijn carrière economische concepten gebruikte om hardnekkige politieke realiteiten uit te leggen, waardeerde Szabo hoe het combineren van multi-disciplinaire kennis hem kon helpen nieuwe inzichten op te doen. Hij hield ervan deze inzichten te benutten om te speculeren over de toekomst van technologie, samenleving en mensheid, waardoor hij perfect bij de Extropianen paste.

De techno-utopische, futuristische beweging kreeg tijdens zijn eerste jaren in de Bay Area steeds meer aanhangers, met name in en rond Silicon Valley, en Szabo zou zichzelf profileren als een vooraanstaand lid van de gemeenschap. De informaticus publiceerde essays en brieven in het *Extropy* magazine over onderwerpen als ruimtekolonisatie (geïnspireerd door zijn ervaring bij JPL), kunstmatige intelligentie, nanotechnologie en meer. Via de Extropiaanse gemeenschap maakte Szabo ook kennis met Tim May.

De Crypto-anarchist

Op een dag nodigde May Szabo uit om deel te nemen aan een bijeenkomst van de Cypherpunks. Szabo ging graag op de uitnodiging in; hij was zelf ook ongerust over de schijnbare erosie van privacy in het opkomende digitale tijdperk.

Toen Szabo een paar weken later de groep privacy-activisten ontmoette, wist hij dat hij op de juiste plek was.

Gedurende de volgende paar jaar hielp Szabo, waar hij kon, aan de zaak van de Cypherpunks. Het meeste opvallend was zijn voortrekkersrol in het verzet tegen de Clipper Chip van de NSA, zowel op de mailinglijst van de Cypherpunks als in het echte leven: hij gaf tijdens verschillende evenementen lezingen over het onderwerp en deelde soms flyers uit om mensen te informeren over de risico's verbonden aan dit soort surveillancetechnologie. Hij had een manier om de verontrustende implicaties van de opdoemende inbreuken op de privacy over te brengen naar een niet-technisch publiek, en was blij om zijn aanpak te delen met de andere Cypherpunks, zodat zij hetzelfde konden leren doen.

Maar Szabo's interesse in digitale privacy was uiteindelijk slechts een deel van een veel groter geheel. Hij omarmde het idee van een *Galt's Gulch in cyberspace*. Zoals uitvoerig beschreven in de vele posts op de mailinglijst door zijn vriend Tim May, had Szabo zich gerealiseerd dat de benodigde instrumenten om individuen te beschermen tegen staatsmacht niet langer alleen voorbehouden waren aan fictieliteratuur. De computerwetenschapper met Hongaarse roots was het eens met het feit dat cryptografie het ideaal van echte vrije markten, ongevoelig voor het gebruik van fysieke macht of staatsdwang, dichter bij kon brengen.

'Als we een stap terug nemen en kijken naar wat veel Cypherpunks proberen te bereiken, dan is er een hoofdthema van een Ghandiaanse cyberspace waar geweld slechts een illusie kan zijn, of het nu in Mortal [Kombat] of *flame wars* is', schreef hij in de Cypherpunk-mailinglijst. 'Cypherpunks willen dat onze telefoonnetwerken, internetbedrijven, etc., zowel beschermd zijn tegen geweld als onafhankelijk zijn van geweld voor hun bestaan. Onze informatiesystemen uit de 20e eeuw, van uitgeverijen tot kredietkaarten, zijn vaak sterk afhankelijk geweest van de dreiging van geweld, meestal via wetshandhaving, om intellectuele eigendomsrechten te beschermen, fraude te voorkomen, schulden in te vorderen, enzovoort.'

Zijn voorstel was:

'Er is geen utopie in zicht waar dergelijke bedreigingen volledig kunnen worden geëlimineerd, maar we kunnen erkennen dat ze bestaan en zorgvuldig werken aan het verminderen van onze afhankelijkheid ervan.'[200]

Slimme contracten

Misschien wel meer dan wie dan ook, was Szabo zich er sterk van bewust dat voor het realiseren van Mays visie op crypto-anarchie, private communicatie slechts een eerste stap was.

Als leerling van Hayeks werk (inclusief diens latere, meer politieke geschriften) was de Cypherpunk tot het inzicht gekomen dat welvarende samenlevingen zo goed presteerden omdat ze bepaalde regels hadden aangenomen, in de vorm van wetten, die menselijk gedrag reguleerden. Hij vergeleek het met het gelaagde ontwerp van computerprotocollen, en erkende dat de wetten die de basis van de samenleving vormden (zoals grondwetten) de meest basale, maar ook de belangrijkste regels van allemaal waren. Alle andere regels zijn gebaseerd op deze fundamenten.

Szabo stelde dat twee van de fundamentele bouwstenen in de *basislaag* van elke welvarende samenleving inderdaad eigendomsrechten en contractrecht waren. Eigendomsrechten vergemakkelijken en stimuleren investeringen, productie en uitbreiding, terwijl contractrecht handel en specialisatie mogelijk maakt. Hij geloofde dat een samenleving die eigendomsrechten en contractrecht handhaaft, uiteindelijk kan evolueren tot een moderne kapitalistische samenleving.

Maar Szabo was zich ervan bewust dat eigendomsrechten en contractrecht in moderne kapitalistische samenlevingen worden gehandhaafd door de staat. Eigendom en de overdracht van eigendom worden uiteindelijk afgedwongen door rechtbanken en de politie, die gebruikmaken van het staatsmonopolie op geweld. Dit kan impliciet gebeuren door (de dreiging van) boetes of gevangenisstraf, of expliciet door iemands eigendom met geweld te beschermen of terug te geven.

Om een staatloze en geweldloze cyberspace-economie te creëren, concludeerde Szabo dat crypto-anarchisten eerst een nieuwe basis moesten leggen.

---

200 Nick Szabo, *Re: Crypto + Economics + AI = Digital Money Economies*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 19 september 1995, online

Het eerste deel van deze basis, de eigendomsrechten, kon met behulp van publieke-sleutelcryptografie worden gerealiseerd, zoals uitvoerig door Tim May is uitgelegd; persoonlijke gegevens zouden worden beveiligd met wiskunde in plaats van met fysieke kracht.

Maar het was niet meteen duidelijk hoe twee mensen deze gegevens konden uitwisselen zonder risico op wanprestatie van de tegenpartij, oftwel *tegenpartijrisico*. Een partij moest altijd eerst hun gegevens verzenden of hun deel van de afspraak afronden. Op dat moment kon de tegenpartij verdwijnen en zijn verplichting niet nakomen. In cyberspace waren er geen rechtbanken of politie om contractrecht te handhaven.

Een mogelijke oplossing was het gebruik van arbitrage om geschillen te beslechten, waarbij een scheidsrechter de middelen zou krijgen om de betreffende data te verplaatsen van de ene handelspartner naar de andere (op eigen discretionaire bevoegdheid, of wellicht in samenwerking met een van de handelspartners). Dit zou echter vereisen dat beide partijen de arbiter vertrouwen om niet te stelen of samen te zweren met hun tegenpartij. Dit vertrouwen zou misschien na verloop van tijd kunnen worden opgebouwd door de reputatie van de arbiter: een onberispelijke staat van dienst van de arbiter zou op een bepaalde manier kunnen dienen als een haalbaar alternatief voor de handhaving door de staat, hoewel het nooit volledig risicovrij zou zijn.

Maar halverwege de jaren 90 meende Szabo dat hij een beter idee had. Hij bedacht een oplossing die niet door een van de handelspartijen kon worden bedrogen en geen betrouwbare scheidsrechter nodig had. Szabo stelde *slimme contracten* voor; digitale contracten die uit zichzelf hun eigen voorwaarden zouden afdwingen, zoals vastgelegd in computercodes.[201]

Stel dat Alice, bij wijze van vereenvoudigd voorbeeld, een geheime code van Bob wil kopen voor $ 10. Een slim contract kan dan zo worden geprogrammeerd dat zodra Bob de geheime code invoert op een vooraf afgesproken plek waar Alice hem kan vinden (misschien door het toe te voegen aan het contract zelf, niet ongelijk aan een digitale handtekening), de code van het contract dit herkent en verifieert, om vervolgens *automatisch* $ 10 van Alice's account af te trekken en over te maken naar Bob (Szabo gebruikte een frisdrankautomaat als een primitieve

201 Nick Szabo, *Smart Contracts: Building Blocks for Digital Free Markets*, *Extropy* 16 : 50–64.

analogie: het *contract* tussen een consument en een frisdrankautomaat stelt dat als de consument een muntje in de automaat stopt, de machine — door een geautomatiseerde respons — een blikje frisdrank of een reep chocolade teruggeeft, zonder verdere menselijke tussenkomst).

In theorie zouden *smart contracts* (slimme contracten) buitengewoon complex kunnen worden opgesteld, en kunnen ze in principe alle soorten contractuele clausules bevatten, waaronder pandrechten, obligaties, of omschrijving van eigendomsrechten. Dit zou zelfs volledig nieuwe zakelijke regelingen mogelijk maken, opperde Szabo, waarbij hij het voorbeeld gaf van een smart contract voor een autolening die, bij het niet terugbetalen van de lening, automatisch de controle over de digitale autosleutels terug zou geven aan de bank.

Nick Szabo geloofde dat de meeste eigenschappen en kenmerken die een slim contract zou moeten bevatten, konden worden geïmplementeerd door gebruik te maken van de steeds groter wordende gereedschapskist van de Cypherpunks: 'Protocollen gebaseerd op wiskunde, genaamd *cryptografische protocollen*, zijn de fundamentele bouwstenen die de verbeterde afwegingen tussen waarneembaarheid, verifieerbaarheid, privaatrechtelijkheid, en afdwingbaarheid in slimme contracten implementeren', schreef hij.[202]

De grootste uitdaging was echter om ervoor te zorgen dat het contract automatisch, betrouwbaar en onvoorwaardelijk uitgevoerd zou worden. Dit hield vooral in dat geen van de partijen bij het contract verantwoordelijk zou moeten zijn voor de uitvoering ervan.

Als algemeen vertrekpunt vermoedde Szabo dat de beste oplossing te vinden was in het domein van gedistribueerd berekening, waar deelnemende computers strikte protocollen moesten volgen om met elkaar overeen te stemmen. Hoewel het Byzantijnse Generaalsprobleem (het coördinatieprobleem dat Adam Back op de universiteit leerde kennen) inderdaad nog niet volledig was opgelost (er bleven enkele risico's als er te veel onbetrouwbare deelnemers waren) geloofde hij dat er robuuste protocollen waren ontworpen voor de meeste scenario's.

'De modaliteiten van contractuele relaties kunnen vaak worden geformaliseerd en gestandaardiseerd, en vervolgens worden uitgevoerd via netwerkgebaseerde protocollen', legde Szabo uit op de Cypherpunk-mailinglijst. 'Deze protocollen,

202 Szabo, *Smart Contracts*, 51.

samen met economische prikkels, beschermen de uitvoering van het contract tegen zowel fraude door de hoofdpartijen als aanvallen van derden.' [203]

Dat gezegd zijnde, zouden de meeste slimme contracten vermoedelijk ook een vorm van geld nodig hebben: meestal moet minstens een van de partijen een betaling doen als onderdeel van de deal. Bovendien moest dit een soort valuta zijn die over het internet kon worden overgedragen, en die autonoom door een computerprogramma kon worden verstuurd… bij voorkeur anoniem. Voor slimme contracten is elektronisch geld noodzakelijk.

Vertrouwde derde partijen

Als digitale equivalenten van eigendomsrechten en contractrecht twee van de fundamentele bouwstenen waren die nodig zijn om een *Galt's Gulch in cyberspace* te realiseren, was een digitaal equivalent voor geld de derde.

Nick Szabo was één van de eersten onder Extropianen en Cypherpunks die deze inzichten herkende. Toen Hal Finney voor het eerst de voordelen van elektronisch geld begon te bepleiten in het *Extropy*-magazine, was Szabo de Extropiaan die naar Amsterdam verhuisde om voor David Chaum te werken. Rond dezelfde tijd dat de eerste webshops hun virtuele deuren openden, trad Szabo toe tot DigiCash als internetprogrammeur.

Tijdens de vroege jaren '90 werkte hij een tijdje op het kantoor van het bedrijf, en kreeg Szabo de kans om uit eerste hand te ervaren hoe het eraan toe ging bij de meest beloftevolle start-up voor elektronisch geld ter wereld. Hij kon zien hoe DigiCash het eerste Chaumiaanse digitale geldproduct op de markt bracht in de vorm van CyberBucks, het ongedekte prototype van eCash, waarvoor de start-up beloofde nooit meer dan een miljoen eenheden uit te geven. Hij was ook getuige hoe CyberBucks een beetje koopkracht verwierven, aangezien sommige Cypherpunks en andere geïnteresseerde technofielen bereid waren om kleine bedragen van het digitale geld te kopen met reguliere valuta, of het te accepteren in ruil voor goederen of diensten met een lage waarde.

Het systeem van CyberBucks was volledig afhankelijk van het bedrijf DigiCash:

---

203 Nick Szabo, *Re: Crypto + Economics + AI = Digital Money Economies*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 19 september 1995, online

Szabo realiseerde zich dat de start-up van Chaum simpelweg meer dan een miljoen eenheden van het elektronische geld kon uitgeven als ze van gedachten zouden veranderen, of als ze vanaf het begin gelogen hadden, of als een oneerlijke medewerker het systeem zou proberen te bedriegen, enzovoorts. Bovendien zou er geen enkele manier zijn om het te detecteren als ze het deden (om nog maar te zwijgen over het feit dat CyberBucks onmiddellijk waardeloos zou worden als de servers van DigiCash ooit uitvielen, wat uiteindelijk ook gebeurde).

Szabo beschouwde dit als aanzienlijke problemen.

'Een van de dingen die ik daar leerde, was hoe gemakkelijk het was om met mensen hun saldo's te knoeien in een centraal gereguleerde valuta', herinnerde de pionier van de digitale valuta zich later. 'Wie zou zijn rijkdom toevertrouwen aan een stel slordige Frank Zappa-fans in het verre Amsterdam?'[204] (ze hielden ervan om platen van Frank Zappa op het kantoor van DigiCash te draaien).

Net als Scott Stornetta en Stuart Haber een aantal jaar eerder, wakkerde dit bij Szabo de neiging aan om dieper na te denken over de rol van vertrouwde entiteiten in het groeiende online ecosysteem. Hoewel cryptografie privacy en beveiliging kon bieden op een niveau dat gelijk of zelfs beter was dan wat mogelijk is in de fysieke wereld, merkte Szabo op dat protocolontwikkelaars doorgaans een bepaald type risico leken te negeren. Het was het risico dat inherent was verbonden aan de afhankelijkheid van een *vertrouwde derde partij* (TTP).

Het typische voorbeeld is een certificaatautoriteit die een register bijhoudt van de werkelijke identiteiten gekoppeld aan hun publieke sleutels. Hoewel dit een handige manier is om iemands publieke sleutel te vinden, zijn deze publieke sleutels eigenlijk maar zo veilig te gebruiken als de certificaatautoriteit zelf. Als een publieke sleutel die door een certificaatautoriteit wordt vermeld, eigenlijk toebehoort aan een aanvaller, zou Szabo benadrukken, kan deze aanvaller elk bericht ontcijferen dat bedoeld is voor wie dan ook die geassocieerd is met de publieke sleutel in het register.

In zijn essay over dit onderwerp, toepasselijk genaamd *Trusted Third Parties are Security Holes* [205], legde Szabo later uit dat vertrouwde derde partijen vaak niet werden opgenomen in de kosten van een ontwerp, en waarom hij geloofde dat

204 Nick Szabo, e-mail aan auteur, 10 juli 2018.

205 Nick Szabo, *Trusted Third Parties are Security Holes*, *Satoshi Nakamoto Institute* , online

dit een vergissing was. Vertrouwde derde partijen zijn veiligheidsgaten, beargumenteerde de Cypherpunk, *zelfs* als ze zelf daadwerkelijk eerlijk zijn: ze kunnen aantrekkelijke doelwitten worden voor kwaadwillige hackers, of misschien zelfs voor naties en hun regelgevende instanties tijdens periodes van politieke instabiliteit of onderdrukking.

Een gecompromitteerde vertrouwde derde partij kan dus enorm duur blijken. Szabo beargumenteerde dat de kosten van een mogelijke inbreuk moeten worden meegenomen bij het ontwerpen van protocollen, wat volgens hem zou leiden tot het feit dat veel protocollen opnieuw ontworpen moeten worden om de vertrouwde derde partijen volledig te elimineren.

Szabo stelde nogmaals dat mogelijke oplossingen misschien wel te vinden zijn in de wereld van gedistribueerde berekening.

'De beste *TTP* van allemaal is er een die niet bestaat, maar waarvan de noodzaak [ertoe] is geëlimineerd door het protocolontwerp, of die geautomatiseerd en verdeeld is over de deelnemers van een protocol', concludeert hij in zijn paper.

Vrij bankieren

Net als Chaum waren de meeste Cypherpunks vooral geïnteresseerd in elektronisch geld vanwege de mogelijkheden tot privacy die het kon bieden. Maar Szabo, May, en enkele andere Cypherpunks die zich bij de beweging hadden aangesloten vanuit de *Extropian*-community, waren ook gedreven door monetaire hervorming. Ze waren voornamelijk geïnteresseerd in de ideeën van Hayek over vrij bankieren, zoals ook beschreven door Max More in de digitale geldeditie van *Extropy*.

Bovendien had Szabo het werk van George Selgin bestudeerd, wiens boek *The Theory of Free Banking* in datzelfde tijdschrift was besproken, en dat van Selgins collega Lawrence H. White, die zelf een artikel aan het tijdschrift had bijgedragen. Aangezien Hayek net voor de oprichting van de Cypherpunkbeweging overleed, dacht Szabo dat de medeoprichters van de door Hayek geïnspireerde moderne school voor vrij bankieren wellicht konden helpen bij het ontwerp van een elektronisch geldsysteem.

Ergens midden jaren '90 besloot hij een nieuwe, meer themagerichte mailinglijst te maken: de Libtech-lijst. Hier zouden vrije bankiers als Selgin en White,

evenals geïnteresseerde Extropianen en Cypherpunks, gerichte discussies voeren over bankieren, monetaire economie en het allerbelangrijkste: de ontwerpen voor digitale valuta.[206]

Toen twee zeer verschillende werelden elkaar ontmoetten op de Libtech lijst, keek Szabo met een frisse blik naar de inzichten uit de Oostenrijkse economie, door zijn eigen ervaring als computerwetenschapper. Dit stelde hem in staat nog duidelijker dan voorheen de gebreken van fiatgeld te zien. Waar Hayek uitvoerig had gewaarschuwd voor de mankementen van centrale banken, zag Szabo in dat dit uiteindelijk te wijten was aan een fundamentele ontwerpfout van het huidige monetaire systeem.

Centrale banken waren vertrouwde derde partijen.

'Het probleem, kort gezegd, is dat ons geld voor zijn waarde momenteel afhankelijk is van het vertrouwen in een derde partij', betoogde Szabo later. 'Zoals vele inflatoire en hyperinflatoire episodes in de 20e eeuw hebben aangetoond, is dit geen ideale situatie.'[207]

Door deze fundamentele zwakte centraal te stellen, bevestigde Szabo op een bepaalde manier Hayeks analyse, althans voor zichzelf.

Maar tegelijkertijd betwistte hij enigszins het monetaire ecosysteem dat Selgin voorspelde dat zou ontstaan in een vrije bankomgeving. Als het probleem van het moderne monetaire systeem was dat iedereen een centrale bank moest vertrouwen, dan zou vrij bankieren gewoon particuliere banken tot de nieuwe vertrouwde derde partijen maken. Zelfs als concurrentie hen eerlijk kon houden, vertegenwoordigden deze TTP's (Trusted Third Parties) een bredere reeks veiligheidsrisico's, variërend van losgeslagen werknemers tot draconische overheden, die marktdynamieken niet noodzakelijkerwijs volledig zouden oplossen.

Als en wanneer deze nieuwe vertrouwde derde partijen – de banken – het vertrouwen van hun klanten zouden schenden, zouden mensen niet simpelweg overstappen naar hun concurrenten, zo voorspelde Szabo. In plaats daarvan zouden mensen opnieuw aandringen op waarborgen van de centrale bank. Zo was het moderne monetaire systeem immers in de eerste plaats ontstaan.

Voordat vrij bankieren een haalbaar alternatief kon zijn, concludeerde Szabo,

206 Nick Szabo, *Nick Szabo on Cypherpunks, Money and Bitcoin*, interview door Peter McCormack, *What Bitcoin Did*, 1 november 2019, online

207 Nick Szabo, *Bit Gold*, *Unenumerated*, 27 december 2008, online

moest er volledig nieuwe vorm van elektronisch geld worden ontworpen dat het vertrouwen minimaliseerde. Net zoals eigendomsrechten en contractrecht voor cyberspace vanaf nul opnieuw moesten worden uitgevonden, zou ook een digitale munteenheid moeten worden gecreëerd door te starten vanuit basisprincipes.

De oorsprong van geld

Om geld te kunnen creëren, moest Szabo het eerst begrijpen. De Cypherpunk was natuurlijk niet de eerste die de natuur van geld bestudeerde, en hij dacht ook niet dat hij dat was. Hij was goed op de hoogte van de theorieën van Carl Menger en Ludwig von Mises over de oorsprong van geld, en deelde grotendeels hun inschatting dat geld voortkwam uit ruilhandel. Maar waar Menger en Mises hun stelling hadden ontwikkeld door logica en redeneren, ging Szabo op zoek naar daadwerkelijke historische documenten, en zelfs archeologische resten.

In zijn zoektocht onderzocht Szabo de prehistorie van de mensheid en bestudeerde hij pre-industriële samenlevingen, zoals die van de Native Americans. Hij ontdekte dat geld zelfs ouder was dan tekst; vroege vormen van geld werden al gebruikt door jager-verzamelaarstammen. Dit leidde tot zijn hypothese dat geld letterlijk zo oud kan zijn als de mensheid zelf. Zoals eerder gesuggereerd door evolutiebioloog Richard Dawkins in zijn baanbrekende werk *The Selfish Gene*[208], kan het vermogen om geld te gebruiken diep geworteld zijn in ons DNA en kan het de overleving van de soort bevorderd hebben.

In zijn latere essay *Shelling Out: The Origins of Money* legt Szabo dit verder uit.[209]

Een van de grote voordelen van de mensheid in de meedogenloze overlevingsstrijd is, ontdekte Szabo, dat de meeste mensen bereid en in staat zijn om samen te werken. Ze bundelen hun krachten, verdelen arbeid en specialiseren zich, waarna ze de opbrengst delen. Dit fenomeen heeft waarschijnlijk altijd bestaan: prehistorische jagers die een wild zwijn doodden, deelden het vlees met hun stamleden. Op hun beurt zouden deze leden de gunst later teruggeven, bijvoorbeeld door blauwe bessen of eetbare paddenstoelen te delen die ze de volgende dag verzamelden.

---

208 Richard Dawkins, *The Selfish Gene*, 244.

209 Nick Szabo, *Shelling Out: The Origins of Money*, *Satoshi Nakamoto Institute*, online

Dit altruïstische gedrag profiteerde iedereen, zolang alle stamleden elkaar kenden en wisten wat ieders bijdragen waren. Iedereen had een publieke reputatie. Profiteurs, degenen die nooit iets bijdroegen, konden uiteindelijk worden uitgesloten van de deelrondes of zelfs uit de stam worden verbannen. Dit zorgde ervoor dat iedereen sterk gemotiveerd was om bij te dragen.

Echter, dit model werd onhoudbaar als een stam (of vaak een groep stammen) te groot werd. Menselijke hersenen kunnen maar een beperkt aantal sociale relaties onderhouden, bekend als *Dunbars nummer*, dat rond de 150 ligt.[210] Wanneer er meer mensen zijn dan dit aantal, wordt het moeilijk om ieders reputatie bij te houden. Als niemand zich kan herinneren wie met wie heeft gedeeld, brokkelt het publieke reputatiesysteem af, waardoor profiteurs vrij spel krijgen ten koste van anderen.

Om misbruik te voorkomen, kan het zelfs rationeel worden voor elk individu om te stoppen met delen en zelf een profiteur te worden, ondanks dat iedereen beter af zou zijn als iedereen deelde. Dit leidt tot een groot gevangenendilemma.[211]

Maar Szabo legde uit dat genen strategieën kunnen coderen om oplossingen te vinden voor uitdagingen in de speltheroie van de echte wereld. Gedurende lange perioden en via natuurlijke selectie zouden de beste eigenschappen, die de overleving van een soort bevorderen, dominant worden.

Het gebruik van geld werd door de Cypherpunk als zo'n eigenschap beschouwd. Voor het grootste deel van de menselijke geschiedenis was dit echter een heel ander soort geld dan wat moderne samenlevingen gebruiken. Doorheen de eeuwen en over verschillende culturen heen, droegen mensen juwelen, zoals kettingen, iets wat geen enkel ander dier doet. De oppervlakkige uitleg hiervoor is dat mensen simpelweg plezier beleven aan het dragen van dergelijke sieraden. Maar Szabo begreep dat er een fundamenteelere vraag schuilging achter deze simpele verklaring, het soort vraag dat een evolutionair bioloog zou stellen. *Waarom* hebben mensen zich zo ontwikkeld dat ze plezier beleven aan het dragen

210 Het is echter belangrijk op te merken dat dit getal—vernoemd naar primatoloog Robin Dunbar—bekritiseerd is en tegenwoordig in de wetenschappelijke gemeenschap niet met de specifieke nauwkeurigheid wordt gehanteerd die het suggereert. Hoewel er een limiet is aan het aantal stabiele sociale relaties dat mensen kunnen onderhouden, is het werkelijke aantal niet per se 150 voor iedereen. Zie bijvoorbeeld Patrick Lindenfors, Andreas Wartel, and Johan Lind, *Dunbar's Number Deconstructed*, Biology Letters, 5 mei 2021: online

211 Strikt genomen is een *public goods game* de meer precieze speltheoretische analogie.

van sieraden?

Net als Dawkins vermoedde Szabo dat mensen in de loop van de eeuwen een voorliefde voor ornamenten hadden ontwikkeld omdat dit een evolutionair voordeel bood: het stelde hen in staat om te coöpereren en middelen te *delen* op een grotere schaal dan alleen binnen hun eigen stam.

Szabo ontdekte bijvoorbeeld dat halskettingen en andere verzamelobjecten verhandeld werden tussen stammen in ruil voor voedsel, wapens of bruiden. De ornamenten konden later teruggeruild worden of met een andere stam geruild worden voor andere hulpbronnen. In plaats van te onthouden wie wat gedeeld had, dienden de sieraden als een soort proto-geld en bevorderden ze wat evolutionaire psychologen *wederzijds altruïsme* noemen.

Het stelde stammen in staat een mate van samenwerking en specialisatie tussen hen te bevorderen. Verschillende stammen jaagden bijvoorbeeld op verschillende soorten dieren in verschillende delen van het jaar, wat hen uiteindelijk allemaal ten goede kwam.

Proto-geld

Niet zomaar elk sieraad voldeed echter. Toen hij de resten van pre-civiele samenlevingen analyseerde, ontdekte Szabo dat mensen uit alle culturen de neiging hadden om zich te richten op verzamelobjecten met enkele zeer specifieke eigenschappen. Hoewel archeologen voorbeelden van proto-geld hadden gevonden die zo uiteenlopend waren als schelpen van een zeldzaam type slak, tot struisvogeleischerven, tot mammoet-tanden, deelden ze allemaal drie algemene kenmerken.

Allereerst waren de verzamelobjecten relatief makkelijk te beschermen tegen onopzettelijk verlies en diefstal. Kettingen zijn waarschijnlijk het beste voorbeeld in dit opzicht: ze zijn bijna onmogelijk te verliezen als ze om de nek worden gedragen. Alternatief gezien, waren ornamenten die niet op iemands lichaam gedragen konden worden, doorgaans minstens makkelijk te verbergen.

Ten tweede, de verzamelobjecten vertegenwoordigden een niet-te-vervalsen schaarste. Dat wil zeggen, ze zouden kostenlijk zijn om te maken of moeilijk te vinden: een mammoettand was schaars omdat een mammoet doden niet gemakkelijk is, terwijl struisvogel eieren moeilijk te bemachtigen zijn.

'Op het eerste gezicht lijkt de productie van een goed uitsluitend omdat het duur is, volledig verspillend', werkte Szabo later uit in *Shelling Out*. 'De onvervalsbaar dure grondstof voegt echter voortdurend waarde toe door welvarende overdrachten mogelijk te maken. Steeds meer van de kosten worden terugverdiend bij elke transactie die mogelijk wordt gemaakt of goedkoper wordt gemaakt. De kosten, aanvankelijk volledig verspild, worden omgeslagen over vele transacties.'

En ten derde, het was doorgaans vrij eenvoudig om vast te stellen dat het proto-geld inderdaad onvervalsbaar zeldzaam was, door simpelweg observaties of metingen te doen. De zeldzame slakkenhuisjes bijvoorbeeld, zou iedereen in deze stammen eenvoudig herkend hebben, terwijl het namaken ervan onmogelijk zou zijn geweest met de gereedschappen die ze ter beschikking hadden.

Szabo ontdekte dat de oudste vormen van geld meestal makkelijk te beveiligen waren en aantoonbaar moeilijk te verkrijgen.

Moderne fiatvaluta bezaten volgens velen in wezen geen van de drie kwaliteiten van proto-geld. Ze waren niet bijzonder gemakkelijk te beschermen tegen diefstal, en de meeste mensen deden zelfs geen poging om hun eigen geld te beveiligen, in plaats daarvan vertrouwden ze op derde partijen (banken) voor veilige bewaring. Maar wellicht nog belangrijker: fiatvaluta was niet fundamenteel schaars; regeringen en centrale banken konden naar believen meer geld drukken, of digitaal extra geld aanmaken via een druk op de knop.

Szabo benadrukte dat het zwevende fiatvalutasysteem dat al tientallen jaren de wereldstandaard was, een grote historische uitzondering was. Rekening houdend met de weinige soortgelijke voorbeelden waarvan hij wist (sommige in het dynastieke China, twee in het Frankrijk van de achttiende eeuw en de Confederatiedollar tijdens de Amerikaanse burgeroorlog) verwachtte hij niet dat het nieuwe monetaire experiment zou blijven duren. Hij was ervan overtuigd dat fiatvaluta uiteindelijk ten onder zou gaan.

Veel Oostenrijkse economen waren uiteraard tot vergelijkbare conclusies gekomen als Szabo. Degenen die een terugkeer naar de goudstandaard voorstaan, geloven specifiek dat het edelmetaal de beste vorm van geld is, grotendeels vanwege de onvervalsbare schaarste ervan.

Szabo was echter niet overtuigd dat goud de beste vervanging was: hoewel het edelmetaal inderdaad moeilijk te verkrijgen was, was het ook moeilijk te

beveiligen. Hij schreef:

> *'Dure metalen en verzamelobjecten hebben een onvervalsbare schaarste vanwege de hoge creatiekosten. Dit gaf geld ooit een waarde die grotendeels onafhankelijk was van een vertrouwde derde partij. Edelmetalen hebben echter problemen. Het is te kostbaar om metalen steeds opnieuw te testen voor gewone transacties. Daarom werd een vertrouwde derde partij (meestal geassocieerd met een belastingontvanger die de munten accepteerde als betaling) gevraagd om een standaard hoeveelheid van het metaal in een munt te stempelen. Het vervoeren van grote hoeveelheden waardevol metaal kan zeer onzeker zijn, zoals de Britten ontdekten toen ze tijdens de Eerste Wereldoorlog goud naar Canada vervoerden over een door U-boten geïnfecteerde Atlantische Oceaan om hun goudstandaard te ondersteunen.'*

Hij daar voegde hij aan toe:

'Erger nog, je kunt online niet betalen met metaal.'[212]

De Cypherpunk wilde de wenselijke monetaire eigenschappen van goud reproduceren in een elektronisch geldsysteem — een digitale valuta met onvervalsbare kostbaarheid.

Toen Adam Back in 1997 hashcash aankondigde, leek dit eindelijk mogelijk te zijn.

Bit Gold

Minder dan een jaar later, in 1998, had Szabo zijn eigen voorstel voor een digitale munteenheid ontworpen: *Bit Gold*. Hoewel hij Bit Gold nog niet in code had geïmplementeerd (het was tot dan toe slechts een idee) deelde hij een beschrijving ervan op de Libtech lijst.

Net als Hashcash, was Bit Gold ontworpen rondom het *proof-of-work* concept. De vereiste rekenkracht om deze *proof-of-work* te genereren koppelde de creatie van de valuta aan de kosten voor energie, met iets wat lijkt op digitale schaarste als gevolg. Vanuit Szabo's visie vertegenwoordigde de *proof-of-work* een onvervalsbare kostbaarheid.

212 Szabo, *Bit Gold.*

Het proof-of-work systeem van Bit Gold zou beginnen met een *kandidaat-reeks*, wat in feite een willekeurig getal is. De gedachte hierachter was dat iedereen deze reeks kon pakken en samenvoegen met hun eigen nonce om zo iets te creëren dat op een hash lijkt. Gezien de kenmerken van hashen, zou de daaruit voortkomende hash een nieuwe, op het eerste gezicht willekeurige, reeks cijfers zijn.[213]

Het trucje, dat ook door hashcash wordt gebruikt, was dat niet alle hashes volgens het Bit Gold protocol als geldig werden beschouwd. In plaats daarvan moest een geldige hash beginnen met een vooraf bepaald aantal nullen. Door de onvoorspelbare aard van hashing, was de enige manier om zo'n hash te vinden door middel van *trial and error*, waarbij bij elke poging een nieuwe nonce werd gebruikt.

Wanneer iemand een geldige hash vond, zou deze hash de nieuwe kandidaat-reeks worden. De volgende geldige hash zou dan gegenereerd moeten worden vanuit deze nieuwe kandidaat-reeks en een ander nonce. Zodra een tweede geldige hash gevonden werd, zou deze op zijn beurt de nieuwe kandidaat-reeks worden, en zo verder.

Het systeem van Bit Gold zou na verloop van tijd een lange reeks hashes genereren, waarbij de meest recente hash altijd fungeert als nieuwe kandidaat-reeks.

Het geldgedeelte leek in grote lijnen op dat van de eerdere voorstel tot het bezit van cijfers van Hadon Nash aan de Cypherpunk-mailinglijst. Wie een geldige hash produceerde zou letterlijk dit hash *bezitten*. Eigendom van hashes zou worden vastgelegd in een digitaal eigendomsregister, waar alle hashes zouden worden toegewezen aan de publieke sleutels van hun eigenaren.[214] Aangezien het register alleen publieke sleutels zou gebruiken, geen namen, kon Bit Gold vrij anoniem worden gebruikt.

Om een hash *uit te geven*, zou de eigenaar een bericht moeten ondertekenen waarin wordt aangegeven wie de nieuwe eigenaar is (opnieuw, door naar deze persoon te verwijzen alleen door hun publieke sleutel). Als de digitale handte-

213 In Szabo's oorspronkelijke voorstel zou Bit Gold eigenlijk gebruikmaken van een *secure benchmark function*, wat iets anders is dan een hashfunctie, maar vergelijkbaar genoeg dat het product een *hash* noemen en het proces *hashen* noemen voldoende nauwkeurig is om de werking van Bit Gold te begrijpen.

214 Nick Szabo, *Secure Property Titles with Owner Authority*, *Satoshi Nakamoto Institute*, online

kening overeenkomt met de publieke sleutel die in het eigendomsregister staat vermeld, zou de overdracht geldig zijn en zou het register worden bijgewerkt om de nieuwe eigenaar van de hash te reflecteren. Zonder een geldige handtekening, zou de overdracht afgewezen moeten worden en zou de hash in het bezit blijven van de huidige eigenaar.

Het proof-of-work zou ervoor zorgen dat Szabo's elektronische geld aantoonbaar moeilijk te verkrijgen is, terwijl publieke-sleutelcryptografie het veilig zou maken.

Dat is natuurlijk onder voorwaarde dat het register zelf veilig is.

Het register

Dus wie zou het register onderhouden?

Szabo begreep dat elke enkele entiteit die het register zou bijhouden, een vertrouwde derde partij zou zijn. Hoewel zelfs deze derde partij niet in staat zou zijn om bewijzen te vervalsen, iedereen kon onmiddellijk herkennen dat de hashes ongeldig zijn, kon het potentieel nog steeds hashes dubbel uitgeven, of transacties censureren, of misschien zelfs hashes stelen van andere gebruikers.

In Szabo's voorstel zou het eigendomsregister dus onderhouden worden door een Bit Gold *eigendomsclub*. Deze club bestond uit *clubleden* (oftewel internetservers) die het eigendomsregister tussen hen zouden dupliceren en gezamenlijk bijhouden wie wat bezit. Als een van de clubleden zou proberen vals te spelen of te stelen, zouden de andere clubleden dit opmerken en de overdracht afwijzen, waardoor het vertrouwen tussen hen wordt verdeeld.

Szabo stelde voor om dit te implementeren met behulp van dezelfde soorten gedistribueerde computerprotocollen die hij voorzag voor slimme contracten. Zoals uitgelegd in zijn paper *Secure Property Titles with Owner Authority*, waren deze ontwerpen het best te begrijpen als geavanceerde stemmingen: zolang de meeste servers eerlijk bleven, zouden ze consensus bereiken over de toestand van het register. Als slechts een minderheid van de servers zou falen of uit de pas zou lopen, zou het systeem als geheel prima moeten blijven functioneren.

Dit was echter niet perfect: het zogeheten Byzantijnse Generaalsprobleem was niet volledig opgelost. Er konden vooral vervelende problemen ontstaan als het

register het doelwit zou worden van een Sybil-aanval. In dit soort computer aanval slaagt één kwaadwillig persoon erin zich voor te doen als meerdere verschillende deelnemers, waardoor de stemprocedures worden overrompeld. Szabo zou dit later omschrijven als het *sockpuppet-probleem*.[215]

Toch geloofde Szabo dat dit zichzelf zou kunnen oplossen. Hij opperde dat zelfs in een scenario waarin een meerderheid van de clubleden zou proberen vals te spelen, het register openbaar zou zijn. Dus cryptografische bewijzen zoals (het ontbreken van) geldige handtekeningen konden worden gebruikt om Bit Gold-gebruikers op de hoogte te stellen van dit wangedrag. De eerlijke minderheid van registerbeheerders kon dan afsplitsen om een concurrerend eigendomsregister te creëren. Wanneer ze de keuze hadden tussen een aantoonbaar oneerlijk meerderheidsregister of een eerlijk minderheidsregister, achtte Szabo het waarschijnlijk dat gebruikers de laatste zouden prefereren.

'Als de regels worden overtreden door de winnende stemmers, kunnen de correcte verliezers de groep verlaten en een nieuwe groep vormen, waarbij ze de oude titels erven', legde hij uit. 'Gebruikers van de titels (vertrouwende partijen) die correcte titels willen behouden, kunnen zelf veilig verifiëren welke afsplitsing de regels correct heeft gevolgd en overschakelen naar de juiste groep.'[216]

Szabo was zich ervan bewust dat het niet de meest elegante oplossing was en enkele belangrijke vragen bleven nog onbeantwoord: in het geval van een dubbele uitgave-aanval, hoe zouden offline gebruikers weten welke transactie eerst kwam? En in het verlengde daarvan, als deze dubbele uitgave zou resulteren in het creëren van een concurrerend register omdat verschillende leden van de eigendomsclub verschillende transacties eerst zagen, hoe zouden deze gebruikers dan weten welke *correct* is?

Desondanks zag Szabo dit in zijn ogen als een betere oplossing dan vertrouwen op een derde partij.

Het beheersen van inflatie

Het laatste probleem dat Szabo moest oplossen was inflatie.

---

215 Nick Szabo, 'Nick Szabo — The Quiet Master of Cryptocurrency … Gehost door Naval Ravikant' interview door Tim Ferriss, *The Tim Ferriss Show*, YouTube, 12 augustus 2017, online

216 Szabo, *Secure Property Titles*.

Naast de onmogelijkheid om eigendom van het proof-of-work over te dragen, had het *hashcash*-systeem van Adam Back nog een groot probleem. Het genereren van geldige hashes zou na verloop van tijd eenvoudiger worden, aangezien computers elk jaar krachtiger werden. Daarom konden de hashes niet goed functioneren als geld: hyperinflatie (of zelfs alleen al de vooruitzichten van hyperinflatie) zou waarschijnlijk betekenen dat zo'n munteenheid niet van de grond zou komen.

Szabo bedacht ook hiervoor een oplossing.

Omdat alle geldige Bit Gold hashes dienst deden als kandidaat-reeksen voor de volgende hash, werden ze noodzakelijkerwijs van een tijdstempel voorzien, in die zin dat de volgorde ervan niet kon worden veranderd. Bovendien konden nieuwe hashes mogelijk afzonderlijk worden vastgelegd op daadwerkelijke tijdstempelservers om een registratie bij te houden van wanneer ze werden gegenereerd.

Szabo legde uit dat deze tijdstempels een goed idee zouden geven van hoe moeilijk het moet geweest zijn om een Bit Gold-hash te produceren: een oudere hash was moeilijker te produceren dan een recentere hash.

Dit verschil moet dan volgens Szabo meegenomen worden in de waarde van een hash:

> *'De kosten van de reeks zijn evenredig met de onwaarschijnlijkheid van de reeks. We hebben empirisch bewijs dat aantoonbaar onwaarschijnlijke documenten, zeldzame drukfouten op postzegels bijvoorbeeld, behoorlijk waardevol worden: hoe zeldzamer en hoe verifieerbaarder, hoe waardevoller.'*[217]

Met andere woorden, een geldige *1998 hash* zou meer waard moeten zijn dan een geldige *2008 hash*.

Om de waarde van de hashes vast te stellen, wilde Szabo gebruikmaken van een beproefde en oude oplossing: de markt. Hij wilde een speciale marktplaats creëren waar Bit Gold hashes tegen elkaar verhandeld konden worden. Kopers en verkopers kunnen op die manier een eerlijke relatieve prijs voor elk van hen vinden. Misschien zou één hash uit 1998 zo'n tien hashes uit 2008 waard zijn,

217 Nick Szabo, *Bit Gold: Towards Trust-Independent Digital Money*, online

waarbij de exacte wisselkoers vermoedelijk zou worden bepaald door de gedaalde kosten van rekenkracht gedurende dat decennium.

Maar dit zou nog een ander probleem creëren, wist Szabo: 'de bits (de puzzeloplossingen) van de ene periode […] zijn niet inwisselbaar met die van de volgende periode.'[218]

De Cypherpunk begreep dat fungibiliteit, waarbij elke eenheid van een valuta gelijk is in waarde aan elke andere eenheid van dezelfde denominatie, een cruciale eigenschap is van geld. Een winkelier moet een betaling kunnen accepteren zonder te hoeven nadenken over de exacte waarde van het ene bankbiljet ten opzichte van het andere; elk dollarbiljet zou moeten volstaan. Als hashes verschillend gewaardeerd zouden worden, zou het de fungibiliteit van Bit Gold in de weg staan.

Nick Szabo, de bedenker van *Bit Gold*, had ook hiervoor een oplossing bedacht: hij zag een op vrij bankieren geïnspireerde *tweede laag* bovenop de *basisslaag* van Bit Gold voor zich.[219] Deze tweede laag zou bestaan uit een speciaal soort banken, die veilig controleerbaar zouden moeten zijn vanwege het openbare karakter van het Bit Gold-register. Deze banken zouden verschillende hashes uit verschillende tijdperioden verzamelen en, op basis van hun relatieve marktwaarde, deze bundelen tot pakketten met een standaardwaarde. Een pakket van bijvoorbeeld *1998* zou slechts één hash kunnen bevatten, terwijl een pakket van *2008* er tien zou bevatten.

Deze pakketten zouden uiteindelijk opgesplitst worden in een specifiek aantal eenheden, wellicht uniek per bank. Alice Bank kon bijvoorbeeld 10,000 Alicebucks per bundel uitgeven, of deze bundel nu een 1998 pakket of een 2008 pakket was. Het zijn deze eenheden die uiteindelijk als het onderling inwisselbare geld gebruikt zouden worden door reguliere gebruikers voor dagelijkse uitgaven, idealiter in de vorm van privé, Chaumiaanse eCash. Tegelijkertijd zouden gebruikers van Alice Bank altijd in staat moeten zijn om hun Alicebucks in te wisselen voor de daadwerkelijke hashes die deze onderbouwen.

'Samengevat', concludeerde Szabo zijn voorstel, 'is al het geld dat de mensheid ooit heeft gebruikt op de een of andere manier onzeker geweest. Deze onzekerheid

218 Nick Szabo, *Bit Gold Markets*, *Unenumerated*, 27 december 2008, online
219 Szabo, *Bit Gold Markets*.

heeft zich op vele manieren gemanifesteerd, van vervalsing tot diefstal, maar de meest schadelijke is waarschijnlijk inflatie geweest. Bit Gold kan ons misschien een vorm van geld geven met een tot nog toe ongeziene veiligheid tegen deze gevaren.'[220]

Nick Szabo had gelijk, tenminste in theorie. Waar hashcash het concept van digitale schaarste had geïntroduceerd, liet het voorstel van Bit Gold zien hoe dit kan worden omgezet in overdraagbaar elektronisch geld.

220 Szabo, *Bit Gold*.

Hoofdstuk 12

B-money (en BitTorrent)

Niet lang nadat Bit Gold had laten zien hoe proof-of-work in overdraagbaar elektronisch geld kon worden omgezet, werd er een enigszins vergelijkbaar voorstel voor digitale valuta ingediend bij de Cypherpunk-mailinglijst. De auteur, Wei Dai, was een bekende naam binnen de Cypherpunk gemeenschap, maar dan alleen bij naam.

Inderdaad, privacy was het oprichtingsbeginsel van de Cypherpunks, maar het lukte weinigen om deze principes zo effectief uit te voeren als Wei Dai. Hoewel zijn betrokkenheid bij de Extropians het vermoeden wekte dat hij in de Bay Area woonde, verscheen Dai nooit bij de persoonlijke bijeenkomsten van de Cypherpunks. Gedurende enige tijd waren de leden van de mailinglijst niet eens zeker of ze correspondentie voerden met een man of een vrouw. Hun onzekerheid ging zo ver dat de Cypherpunks zich zelfs afvroegen of Dai wel echt bestond, speculerend dat de naam wellicht een pseudoniem was; sommigen vermoedden dat het eigenlijk een alter-ego van Nick Szabo was.

In werkelijkheid was Wei Dai, een hij, een jonge informaticus die toevallig enkele jaren jonger was dan Szabo aan de Universiteit van Washington, hoewel de twee elkaar nooit op de campus hebben ontmoet. Als liefhebber van cyberpunk boeken, had Dai als student een interesse ontwikkeld in cryptografie omdat hij geloofde dat het de mensheid kon helpen beschermen tegen toekomstige entiteiten zoals de Blight, een kunstmatige super-intelligentie die diende als de

voornaamste antagonist in Vernor Vinge's roman *A Fire Upon the Deep*.[221]

Zijn interesse in cryptografie leidde Dai uiteindelijk naar de Cypherpunk-mailinglijst, waar hij kennis maakte met de talrijke bijdragen van Tim May. Terwijl hij zich verdiepte in Mays visie op de toekomst van de samenleving, raakte de jonge informaticus nog meer gefascineerd door het transformatieve potentieel van cryptografie, nu met een sterke nadruk op privacy en vrijheid van overheidsinmenging.

Dai, wiens naam aangeeft dat hij van Chinese afkomst is, begon zich uiteindelijk te mengen in de gesprekken op de mailinglijst. In het midden van de jaren '90 betrok Dai zichzelf bij discussies over allerlei onderwerpen, variërend van de economie van digitale reputatiesystemen tot de toepassing van speltheorie op het gebied van cryptografie, voorstellen om traceerbare betalingssystemen om te zetten in anonieme, en nog veel meer.

Gedurende die tijd nam Dai de filosofie en missie van de Cypherpunks als zijn eigen aan.

'Er heeft nooit een regering bestaan die niet vroeg of laat probeerde de vrijheid van haar onderdanen te verminderen en meer controle over hen te verkrijgen, en waarschijnlijk zal er nooit een dergelijke regering zijn' vat Dai op een bepaald moment samen wat hij beschouwt als de bindende ethos van de beweging. 'Daarom zullen we, in plaats van te proberen onze huidige regering te overtuigen om het niet te proberen, de technologie (bijvoorbeeld, remailers en elektronisch geld) ontwikkelen die het voor de regering onmogelijk zal maken om te slagen.'[222]

Cypherpunks schrijven code.

Ook Wei Dai ontwikkelde een aantal tools om de Cypherpunk-zaak te bevorderen. Dit bevatte een versleuteld tunneling-protocol (dat de overdracht van data van het ene netwerk naar het andere mogelijk maakte), een veilig systeem om bestanden te delen en de Crypto++ softwarebibliotheek (die vrij beschikbare cryptografische algoritmen bevat geschreven in de programmeertaal C++). Door zijn werk in versleuteling en zijn doorgaans intelligente en inzichtelijke e-mails, verdiende Dai's bijdragen hem een reputatie als een van de meest productieve en

221 Wei Dai, *Work on Security Instead of Friendliness? GreaterWrong*, 21 juli 2012, online

222 Wei Dai, *Law vs Technology*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 10 februari 1995, online

waardevolle deelnemers aan de mailinglijst van de Cypherpunks, ondanks zijn meer ongrijpbare persoonlijkheid.

Hoewel het op het eerste gezicht vreemd kan lijken, is het niet zo ongelooflijk dat sommigen vermoeden dat Nick Szabo en Wei Dai eigenlijk dezelfde persoon zijn: de twee hadden veel gemeen. Naast het volgen van dezelfde universitaire studies en dat ze beiden deel uitmaakten van zowel de Cypherpunk als de Extropian gemeenschappen, hadden Szabo en Dai een bijzondere interesse in elektronisch geld, en om vele van dezelfde redenen. Ze wilden helpen om Tim Mays *Galt's Gulch in cyberspace* te realiseren, en beiden begrepen het belang van digitale contracten in deze context.

In november 1998, net na zijn afstuderen aan de universiteit, kondigde Wei Dai informeel zijn eigen elektronisch geld aan. Dit voorstel werd bijna terloops aangekondigd in een mail waarin hij ook een geüpdatete versie van zijn anoniem communicatieprotocol, bekend als PipeNet, bekendmaakte.[223] Het gebeurde slechts weken nadat Szabo voor het eerst zijn digitale munteenheid besprak op de Libtech mailinglijst. Dai, die ook actief was op deze lijst, had b-money gecreëerd.

'Ik ben gefascineerd door Tim Mays crypto-anarchie', legde Dai zijn motivatie uit in het voorstel. 'In tegenstelling tot de gemeenschappen die traditioneel geassocieerd worden met het woord *anarchie*, wordt in een crypto-anarchie de regering niet tijdelijk vernietigd, maar permanent verboden en overbodig. Het is een gemeenschap waar de dreiging van geweld machteloos is omdat geweld onmogelijk is, en geweld onmogelijk is omdat de deelnemers niet in verband kunnen worden gebracht met hun daadwerkelijke namen of fysieke locaties.'

Hij concludeerde:

> *'Het protocol dat in dit artikel wordt voorgesteld, maakt het voor ontraceerbare pseudonieme entiteiten mogelijk om efficiënter samen te werken, door hen te voorzien van een ruilmiddel en een manier om contracten af te dwingen. [...] Ik hoop dat dit een stap is in de richting van het praktisch mogelijk maken van crypto-anarchie, naast de theoretische mogelijkheid.'*[224]

223 Wei Dai, *PipeNet 1.1 and b-money*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 26 november 1998, online

224 Wei Dai, untitled b-money description, 1998, online

B-money

B-money leek in belangrijke opzichten op Bit Gold, hoewel het op andere punten verschilde.

Net als Bit Gold, zou b-money in principe bestaan op een grootboek (wat Szabo een *register* noemde). Dit grootboek zou publieke sleutels vermelden, en het aantal toegeschreven munteenheden aan elke publieke sleutel aangeven. Om het elektronische contant geld te verplaatsen, ondertekenden gebruikers cryptografisch een bericht dat aangeeft hoeveel munteenheden er worden uitgegeven van de bijbehorende publieke sleutel, en naar welke publieke sleutel ze werden uitgegeven. Als de transactie geldig was (de publieke sleutel had voldoende geld en de handtekening klopte), zou het grootboek dienovereenkomstig worden bijgewerkt.

Net zoals Szabo, legde Dai een sterke nadruk op het belang van contracten. B-money was ontworpen om de uitvoering van contracten te vergemakkelijken, en een significant deel van het voorstel was gewijd aan het uitleggen van de taken van bemiddelaars in geschillenoplossing (hoewel het niet helemaal de autonome slimme contracten waren die Szabo oorspronkelijk in gedachten had, waren er enige cryptografische veiligheidsmaatregelen opgesteld om bepaalde vormen van fraude te voorkomen).

Szabo was er ook in geslaagd om Wei Dai ervan te overtuigen dat het minimaliseren van vertrouwen essentieel was. *Vertrouwde derde partijen zijn beveiligingsrisico's*, gaf Dai toe, en hij kwam tot de conclusie dat een elektronisch geldsysteem niet mocht staan of vallen met één enkele entiteit om de saldo's van gebruikers bij te houden, transacties mogelijk te maken of dubbele uitgaven te voorkomen.

In plaats daarvan bedacht Dai twee alternatieve oplossingen. De eerste variant van b-money was met name zeer ambitieus. In deze variant was er geen centrale instantie, maar onderhield *elke* gebruiker van het systeem zijn eigen exemplaar van het grootboek. Bij elke nieuwe b-moneytransactie zou iedere gebruiker afzonderlijk de geldigheid ervan controleren en hun eigen versie van het grootboek bijwerken als de transactie in orde bleek. Zolang iedereen actueel bleef, zouden de grootboeken gesynchroniseerd blijven onder alle gebruikers.

In theorie is het grote voordeel van zo'n gedistribueerd systeem dat corruptie onmogelijk zou zijn. Als iemand bijvoorbeeld te veel geld toeschrijft aan zijn

eigen publieke sleutels, zou dit geen enkel effect hebben op iemand anders: alle andere grootboeken zouden onveranderd blijven. Als de bedrieger probeerde zijn vervalste geld uit te geven, zou niemand anders die transactie als geldig zien. Net zoals bij de tijdstempeloplossing van Scott Stornetta en Stuart Haber zou iedereen ervoor zorgen dat alle anderen eerlijk zou blijven.

Het leek een ideale oplossing om het grootboek over alle gebruikers te verspreiden — in theorie.

Helaas wist Wei Dai dat het in de praktijk niet haalbaar zou zijn. Om dubbele uitgaven te voorkomen, vereiste het systeem een *synchroon en onverstoorbaar anoniem uitzendkanaal*.[225] Alleen als alle gebruikers zeker konden zijn dat zij allemaal dezelfde transacties in precies dezelfde volgorde ontvingen, kon iedereen er vertrouwen in hebben dat hun grootboeken gesynchroniseerd waren en dat een betaling die zij zouden ontvangen ook door alle anderen zou worden geregistreerd. Dit leek onwerkbaar: dubbele uitgavetransacties konden tegelijkertijd naar verschillende delen van het netwerk worden gestuurd, terwijl onbetrouwbare deelnemers eenvoudigweg konden liegen over de volgorde van de transacties die ze hadden ontvangen.

Of in technische termen: Wei Dai's eerste oplossing negeerde het Byzantijnse Generaalsprobleem. Dit is waarom Dai in hetzelfde voorstel met een tweede oplossing kwam.

In deze tweede versie van het b-money systeem, zou niet iedereen een versie van het hoofdregister bijhouden, maar zou het systeem bestaan uit twee soorten deelnemers: reguliere gebruikers en *servers*. Net zoals de *eigendomsclub* in Szabo's Bit Gold voorstel, zouden alleen deze servers de b-money hoofdregisters bijhouden. Om er zeker van te zijn dat een transactie werd voltooid, moesten reguliere gebruikers checken bij een willekeurige subset van servers, en een betaling pas als finaal beschouwen als die servers de transactie erkenden.

Dit introduceerde natuurlijk wel weer wat vertrouwde partijen in het systeem. De servers konden samenwerken om overdrachten te blokkeren, transacties dubbel uit te geven, mogelijk fondsen te stelen of zelfs regelrecht geld voor zichzelf te creëren.

Wei Dai stelde daarom een manier voor om de servers eerlijk te houden.

225 Dai, untitled b-money description.

'Hij stelde voor dat elke server verplicht is om een bepaald bedrag op een speciale rekening te storten, die zou worden gebruikt als potentiële boetes of beloningen voor bewijzen van wangedrag', stelde hij voor. 'Ook moet elke server periodiek zijn huidige database van geldcreatie en geldbezit publiceren en zich daaraan binden. Elke deelnemer moet controleren of zijn eigen rekeningsaldi kloppen en dat de som van de rekeningsaldi niet groter is dan het totale bedrag aan gecreëerd geld.'

Echter, het b-money voorstel ging niet in detail in op een van deze oplossingen. Wellicht het meest problematisch was dat Dai niet uitlegde wie zou bepalen of er wangedrag plaatsvond, als dit niet werd bepaald door de (samenzwerende) servers zelf, of hoe de boetes konden worden afgedwongen. Net zoals Bit Gold geen oplossing had geboden om conflicten tussen servers te beslechten, had b-money dat ook niet gedaan.

Monetaire beleid van b-money

Net als Bit Gold zou b-money een zuiver digitale munteenheid zijn. Er zou geen bank of bedrijf zijn die de digitale eenheden dekte met dollars of goud, en geen garantie dat iemand de munteenheid zou accepteren voor betaling. Maar net zoals Szabo, dacht Dai niet dat dit een probleem zou zijn.

'Denk er op deze manier over na', betoogde hij op de mailinglijst van de Cypherpunks. 'In het geval van goederengeld, wordt de waarde deels bepaald door de industriële/esthetische waarde van het goed en deels door het nut van het goederengeld als ruilmiddel. In het geval van fiatgeld en b-money, komt alle waarde voort uit zijn nut als ruilmiddel.'[226]

In tegenstelling tot Szabo, wilde Dai zijn valuta echter voorzien van een gericht monetair beleid. Waar de koopkracht van Bit Gold overgelaten werd aan de markt, met geldige proof-of-work hashes die vrij verhandeld worden voor wat kopers en verkopers bereid zijn te accepteren, was b-money specifiek ontworpen om een voorspelbare koopkracht te bieden.

Net als Irving Fisher en de Vereniging voor Stabiel Geld ongeveer 80 jaar eerder,

226 Wei Dai, *Re: alternative b-money creation*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 11 december 1998, online

stelde Dai voor om de koopkracht van zijn munteenheid te koppelen aan een consumentenprijsindex. Hij wilde dat dezelfde hoeveelheid b-money-eenheden op elk moment een gelijk aandeel van deze index kon kopen. Met andere woorden, de gemiddelde prijs van goederen en diensten, uitgedrukt in b-money, moest stabiel blijven.

Als we het breder bekijken, zou het creëren van valuta in b-money vergelijkbaar werken met Bit Gold: iedereen zou nieuwe valuta-eenheden kunnen genereren door middel van een proof-of-work door een geldige hash te produceren, vermoedelijk ook gebaseerd op een bepaalde kandidaat-reeks. Wie de hash creëerde, mocht deze houden (of misschien zouden ze een equivalent in b-money-eenheden krijgen; een geldig proof-of-work zou heel goed op de grootboek kunnen worden weerspiegeld als 100 digitale *munten*).

Het belangrijkste verschil met Bit Gold, was echter dat de moeilijkheidsgraad om een geldig proof-of-work te genereren, kon veranderen.

Alle gebruikers van het systeem (b-money versie 1) of de servers (b-money versie 2) zouden voortdurend moeten bepalen hoeveel een mandje goederen zou kosten in verhouding tot de productie van een geldige hash. Dat wil zeggen, als het creëren van een hash goedkoper wordt (door verbeteringen in computerhardware) in verhouding tot de prijsindex, dan zou de moeilijkheidsgraad om een geldige hash te produceren naar boven moeten worden bijgesteld: de hash zou met meer nullen moeten beginnen. Een nieuwe hash zou dan alleen aan het grootboek worden toegevoegd als aan de meest recente drempelwaarde was voldaan.

Wei Dai vermeldde in de bijlage van zijn voorstel ook een alternatieve benadering om een vergelijkbaar resultaat te bereiken. Het aanmaken van geld kon gebeuren via een veiling. In dit geval zouden alle gebruikers (b-money versie 1) of de servers (b-money versie 2) eerst de optimale uitbreiding van de geldvoorraad bepalen, waarna deze nieuwe eenheden b-money geveild zouden worden aan degene die bereid en in staat was om het met het meeste proof-of-work te betalen.

Een grote voordeel van deze benaderingen was dat alle b-money hashes, ongeacht wanneer ze werden gecreëerd, dezelfde waarde moesten hebben: ze zouden fungibel zijn. Dit elimineerde de noodzaak om een hele andere bankenlaag te ontwerpen bovenop de basislaag van de valuta, zoals Szabo had voorgesteld voor Bit Gold.

Het was een innovatieve aanpak, maar opnieuw bleef er veel ongespecificeerd. Zowel voor de aanpassingsmethode van de moeilijkheidsgraad als het veilingmodel, bleef het in het voorstel van b-money onduidelijk hoe gebruikers (of servers) zouden beslissen over de volgende moeilijkheidsgraad voor proof-of-work, of de optimale toename van de geldvoorraad… en hoe geschillen in dit deel van het proces zouden kunnen worden opgelost (het Byzantijnse Generaalsprobleem bleef de kop opsteken).

'B-money was nog geen volledig ontwerp om in de praktijk te brengen', erkende Dai later.[227] Het voorstel bood een ruwe schets van hoe een elektronisch geldsysteem eruit kon zien, maar er waren nog meerdere problemen die moesten worden opgelost voordat het als een daadwerkelijke digitale valuta zou kunnen functioneren. Dai zelf besloot echter dat hij niet degene zou zijn die deze problemen zou oplossen.

Ontgoocheling

In zijn voorstel voor b-money leek Wei Dai nog altijd optimistisch over de mogelijkheden en het potentieel van Tim Mays crypto-anarchistische visie. Maar in werkelijkheid was de ongrijpbare informaticus de droom van de Cypherpunks aan het opgeven.

'Ik ben niet verder gegaan met het ontwerpen omdat ik, tegen de tijd dat ik klaar was met het opschrijven van b-money, eigenlijk al wat gedesillusioneerd was geraakt door crypto-anarchie', herinnerde Dai zich later. 'Ik had niet voorzien dat zo'n systeem, eenmaal geïmplementeerd, zoveel aandacht en gebruik zou aantrekken buiten een kleine groep van *hardcore* Cypherpunks.'[228]

Dai's ontgoocheling weerspiegelde een groeiend sentiment binnen de Cypherpunk-gemeenschap tegen het einde van de jaren 90. Het internet was inmiddels echt mainstream geworden, maar de Cypherpunks ontdekten dat het grote publiek nogal onverschillig was over online privacy. Het leek erop dat de meeste mensen er geen probleem mee hadden om betalingsverwerkers volledig inzicht te geven in hun uitgavenpatroon, en ze leken er ook geen probleem mee

227 Wei Dai, comment in the discussion thread *AALWA: Ask any LessWronger anything*, *LessWrong*, 2014, online

228 Dai, comment.

te hebben om een spoor van hun andere online activiteiten achter te laten. De gemiddelde internetgebruiker dacht zelfs niet eens aan het versleutelen van hun e-mails.

Sinds de Cypherpunks voor het eerst bijeen kwamen in het ongemeubileerde appartement van Eric Hughes, hadden ze bijna tien jaar besteed aan het transformeren van revolutionaire cryptoprotocollen in werkende software. Tot hun grote teleurstelling bleek dat bijna niemand hierin geïnteresseerd was. Het doorzettingsvermogen in hun activisme voor privacy had hen weliswaar geholpen de crypto-oorlogen te winnen, maar dit leek nu een tamelijk nutteloze inspanning te zijn geweest. De meeste internetgebruikers bleken namelijk perfect op hun gemak met het opgeven van zowat al hun persoonlijke informatie in ruil voor iets meer gemak.

Hughes had zich inmiddels vrijwel volledig teruggetrokken uit de gemeenschap en de mailinglijst. Maar niet voordat hij zijn nuchtere herbeoordeling van de *Cypherpunks schrijven code*-filosofie had aangeboden, kenmerkend voor de recente desillusie van Wei Dai, hemzelf en andere Cypherpunks.

'Misschien het belangrijkste wat ik van de Cypherpunks heb geleerd is dat alleen code niet voldoende is. Niet alleen code, niet wijdverspreide code, zelfs niet veelgebruikte code', schreef Hughes zich richtend tot de Cypherpunk-mailinglijst. 'Voor langdurig succes is een zekere mate van tolerantie in de samenleving nodig voor activiteiten die in privé worden ondernomen. Niet alleen gemakkelijk of makkelijker, maar noodzakelijk.'[229]

Hughes was tot het inzicht gekomen dat het essentieel was dat het grote publiek zou begrijpen waarom privacy belangrijk was. Code was uiteraard ook nog steeds nodig — code maakte privacy in eerste instantie mogelijk. Maar hij geloofde nu dat code uiteindelijk alleen maar nuttig was als er een brede publieke consensus bestond dat mensen daadwerkelijk het recht zouden moeten hebben om hun privacy te beschermen. Zonder zo'n publieke consensus zou het gebruik van cryptografie kunnen worden gemarginaliseerd en wellicht zelfs verboden, met als risico dat de overblijvende gebruikers mogelijk zouden worden geviseerd en vervolgd.

229 Eric Hughes, *Kid Gloves or Megaphones*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 14 maart 1996, online

'Hetzelfde geldt voor anonieme transacties', schreef Hughes. 'Tenzij er een soortgelijke consensus bestaat, zullen we weer te maken krijgen met een marginale activiteit. Ik beschouw dit als een verlies.'[230]

Het optimisme en de assertiviteit die de beweging in de begindagen kenmerkten, werden steeds meer overschaduwd door een gevoel van somberheid en verlatenheid.

In plaats daarvan kwamen sommige van de meer hoopvolle impulsen voor de Cypherpunk-missie in de late jaren '90 van relatieve buitenstaanders van de gemeenschap.

Zero-Knowledge Systems

De Canadese broers Austin en Hamnett Hill waren nog maar halverwege de twintig toen ze TotalNet, de internetprovider die ze hadden opgericht en die de derde grootste van hun land werd, verkochten. Met wat geld in hun zak en de tijd om het uit te geven, zochten de twee naar hun volgende project toen ze op de Cypherpunk-mailinglijst stuitten. Ze raakten volledig in de ban van het technolibertarische ethos van de beweging.

In 1997 besloten de twee broers, samen met hun vader Hammie Hill, om hun middelen, connecties, en zakelijke talenten in te zetten, en richtten ze *Zero-Knowledge Systems* op. Het nieuwe bedrijf nam zich voor om de visie van de Cypherpunks werkelijkheid te laten worden, en om er tegelijkertijd ook wat geld mee te verdienen.

De kernactiviteit van de start-up was een privacy-netwerk dat ze *Freedom* noemden. Freedom was gebaseerd op Wei Dai's PipeNet, het anonieme communicatieprotocol waarvan een bijgewerkte versie zou worden aangekondigd in dezelfde Cypherpunks-mailinglijstpost die b-money introduceerde. Net als PipeNet, werden in Freedoms verhullingstechnieken een geavanceerdere variant van David Chaums originele remailer-protocol ingebed, maar waar remailers alleen e-mails anonimiseerden, paste Freedom de mix-technologie toe om alle soorten internetgegevens te verhullen: e-mails, surfen, tekst-chat en meer.

Gebruikers van Freedom konden in wezen op het internet *inloggen* onder ver-

230 Hughes, *Kid Gloves*.

schillende identiteiten: misschien een reguliere identiteit voor professioneel werk, een pseudonieme identiteit voor politieke betrokkenheid, en nog een pseudoniem voor seksueel getinte webactiviteiten. Niemand, zelfs Zero-Knowledge Systems niet, zou in staat zijn de pseudonieme online identiteiten te koppelen aan een echte identiteit, of aan andere pseudoniemen.

De start-up wekte behoorlijk wat interesse op binnen de Cypherpunk-gemeenschap en, belangrijker nog, de oprichters van Zero-Knowledge Systems wisten de durfkapitalisten uit te leggen waarom ze de kans niet mochten missen om te investeren in *de toekomst van privacy*. Binnen een paar jaar slaagde de start-up erin om tientallen miljoenen dollars op te halen.

Waarschijnlijk konden de Hills beter verkopen dan de meeste Cypherpunks. Ze wisten ook op een goede manier de ambitieuze doelen van Zero-Knowledge Systems aan het grote publiek te presenteren. Er verschenen aantrekkelijke print-advertenties in bekende tijdschriften zoals *Wired, Forbes en Fortune*, met teksten als 'Ik ben geen stuk van je inventaris', 'Ik ben een individu en je zult mijn privacy respecteren' en 'Op het net heb ik de controle'. Bijzonder scherpe lezers konden ook een verborgen boodschap ontrafelen uit een binaire code op de pagina's, die zich vertaalde naar 'Wie is John Galt?' — een beroemde zin uit Ayn Rands *Atlas Shrugged*.

En wellicht nog het belangrijkst van alles, Zero-Knowledge Systems wist het beste talent in de privacy-sector aan te trekken. Enkele van de bekendste cryptografen en computerwetenschappers op de Cypherpunk-mailinglijst besloten zich bij de start-up te voegen, waaronder Ian Goldberg – die tijdens de crypto-oorlogen het SSL crypto-protocol van Netscape had gebroken en het bedrijf als 'Hoofdwetenschapper en Hoofd Cypherpunk' zou dienen – en Adam Back. Stefan Brands, de uitvinder van Brands Cash, werd ook aangenomen en zijn patenten op elektronisch geld werden eveneens door de start-up gekocht.

De Hills waren zeker niet kort van ambitie. Freedom was het hoofdproject van het bedrijf, maar Zero-Knowledge Systems wilde uiteindelijk de idealen van Cypherpunks breed realiseren. Het onderzoeks- en ontwikkelingsteam van de start-up, ook wel de 'Kwaadaardige Genieën' genoemd, kreeg de taak om aanvullende producten te ontwerpen. Dit omvatte onder andere een elektronisch geldsysteem gebaseerd op het ontwerp van Brands, met de codenaam Zorkmid (een verwijzing naar de munteenheid van een vroeg online spel).

Ondanks alles, leek één probleem echter aan te houden. De meeste internetgebruikers gaven gewoon niet veel om privacy.

Zero Knowledge Systems had het plan om tegen 2000 zo'n 2,5 miljoen gebruikers van Freedom aan te kunnen. Maar hoewel de 250 medewerkers zich flink hebben ingezet om dit mogelijk te maken, waren er rond de eeuwwisseling slechts iets meer dan twaalfduizend actieve gebruikers op het netwerk, of minder dan een procent van het oorspronkelijke doel.

Deels kwam dit doordat veel mensen moeite hadden met het installeren van de software, maar zelfs degenen die erin slaagden Freedom operationeel te krijgen, ontdekten dat hun internetsnelheid aanzienlijk afnam bij het gebruik van de service. Buiten een relatief technisch onderlegde kern van gebruikers (voornamelijk mannen tussen de 25 en 35 jaar) waren weinig mensen bereid dit voor lief te nemen, en daarnaast nog de jaarlijkse vergoeding van $ 50 aan Zero-Knowledge Systems te betalen. Aan het einde van de rit zagen mensen gewoonweg geen reden om Freedom te gebruiken: de voordelen voor de privacy waren voor hen onzichtbaar.

Of in de woorden van Austin Hill, een paar jaar later: 'Iedereen beweert te geven om privacy, maar men zou zo een DNA-staal afstaan voor een *gratis* Big Mac.'[231]

Om het bedrijf te redden, heeft Zero Knowledge Systems uiteindelijk haar strategie veranderd. In plaats van op de algemene internetgebruiker te focussen, zou de start-up vanaf 2001 haar inspanningen richten op gevestigde bedrijven, zoals financiële instellingen en telecombedrijven. Ze boden hen beveiligde database- en communicatiesystemen aan. Tot grote ontsteltenis van zijn kleine, maar toegewijde gebruikersbasis werd Freedom stopgezet.

Hiermee liet de start-up het Cypherpunk-ethos grotendeels achter zich, en personen zoals Back en Brands vertrokken kort daarna. Toen het bedrijf uiteindelijk zijn naam veranderde in Radialpoint, was Zero Knowledge Systems in alle opzichten vervangen door een totaal ander IT-bedrijf.

Ondanks een hoopvol begin, was dit een nieuwe tegenslag voor het doel van de Cypherpunks.

231 Austin Hill, ontwerpdocument van 2005 gedeeld met de auteur, 30 maart 2022.

Mojo Nation

Een andere positieve impuls kwam van twee tot dusver onbekende tieners die een compleet ander deel van de cyberspace ontregelden: Met de lancering van Napster in 1999 gooiden Shawn Fanning en Sean Parker, respectievelijk achttien en negentien jaar oud, de digitale variant van een handgranaat recht in het hart van de muziekindustrie.

Napster was een krachtig idee om één specifieke, technische reden. In tegenstelling tot de meeste internetdiensten tot dat moment, die vertrouwden op een centrale server om gebruikers te voorzien van wat ze nodig hadden, was Napster ontworpen als een *peer-to-peer* (P2P) netwerk. De peers (Napster-gebruikers) op het Napster-netwerk fungeerden als gelijken, ze hielpen elkaar waar nodig: specifieker, ze deelden hun eigen muziekbestanden met elkaar. Omdat Napster zelf geen muziekbestanden verspreidde, dachten Fanning en Parker dat ze claims wegens inbreuk op auteursrechten konden omzeilen, terwijl gebruikers nog steeds gratis nummers konden downloaden.

Maar toen de populariteit van Napster ontplofte, lanceerde de muziekindustrie een succesvolle tegenaanval. Fanning en Parker deelden misschien zelf geen muziek, maar artiesten en platenmaatschappijen beweerden dat de service desondanks actief inbreuk maakte op het auteursrecht: Napster bood gebruikers een platform, het beheerde en bewaarde de indexen om alle muziekbestanden te vinden, en de service koppelde peers dienovereenkomstig. Al snel bezweken Fanning en Parker onder de enorme juridische druk, en in juli 2001 haalden ze Napster offline.

Uiteindelijk was Napster een kortstondig project. Maar in een paar jaar tijd populariseerden ze de P2P-technologie, die een hele nieuwe klasse van vernieuwers inspireerden. Alternatieve diensten om bestanden te delen zoals Kazaa en eDonkey doken al snel op, elk van hen ontworpen om nog decentraler te zijn dan de creatie van Fanning en Parker. Gedurende de volgende paar jaar waren de makers van deze nieuwe protocollen betrokken bij een hoogtechnologisch kat-en-muis-spel met de platenlabels die probeerden hun projecten lam te leggen.[232]

De eenendertigjarige Cypherpunk, Jim McCoy, besloot dat hij ook wilde

232 Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, 22–27.

meespelen. Begin 2000 nam hij ontslag bij Yahoo – 'Ik werd het zat om niets revolutionairs te doen'[233] – en samen met verschillende andere Cypherpunks, waaronder DigiCash-alumnus Bryce *Zooko* Wilcox, richtte McCoy Autonomous Zone Industries op.

De naam van het bedrijf was geïnspireerd op *tijdelijke autonome zones*, een term die voor het eerst werd gebruikt in 1991 door anarchist Hakim Bey om niet-permanente, lokale samenlevingen te beschrijven die vrij zijn van de overheid. De start-up zou een ambitieus open-source softwareproject genaamd Mojo Nation ontwikkelen. Net als Napster was Mojo Nation in essentie een P2P *file sharing system*. Maar McCoy, als ervaren Cypherpunk, had een paar extra tools in zijn crypto-gereedschapskist om het ontwerp van Fanning en Parker te verbeteren.

Een van Mojo Nations meest interessante innovaties was dat alle bestanden op het netwerk in kleine stukjes werden opgedeeld, gecodeerd en strategisch gekopieerd en verspreid over het netwerk. Als iemand een bestand ging downloaden, downloadden ze in feite al deze kleine gecodeerde stukjes van verschillende gebruikers over het netwerk, om uiteindelijk deze puzzelstukjes bij elkaar te brengen en in één keer het volledige bestand te decoderen. Omdat alle uploaders slechts een beetje bandbreedte nodig hadden om hun stukje te delen, kon de downloadsnelheid worden verhoogd. Dit stelde Mojo Nation-gebruikers in staat om grotere bestanden te delen dan de typische MP3's. Bovendien bood het meer privacy: gebruikers die de gecodeerde stukjes deelden, wisten vaak niet wat voor soort inhoud ze deelden (of deze inhoud al dan niet auteursrechtelijk beschermd was).

Daarnaast werden sommige taken die Napster nog steeds als een centrale coördinator uitvoerde, in Mojo Nation overgedragen aan de gebruikers. Gebruikers die als archivaris fungeerden zouden bijvoorbeeld de indexen van bestanden die op het netwerk werden gehost bijhouden, terwijl andere gebruikers, die als zoekagenten fungeerde, zoekopdrachten via deze indexen zouden aanbieden. Door dergelijke verantwoordelijkheden in de handen van gebruikers te leggen, geloofde McCoy dat Mojo Nation niet vatbaar zou zijn voor het soort rechtszaken waarmee Napster te maken had gehad. In plaats daarvan zouden de gebruikers zelf verantwoordelijk zijn als ze wetten van hun jurisdictie overtraden — maar al deze

233 Damien Cave, *The Mojo solution*, *Salon*, 9 oktober 2000, online

individuele mensen waren natuurlijk veel moeilijker te vinden dan Fanning en Parker.

Wat dit alles liet draaien was wellicht het meest interessante element van Mojo Nation: een digitale valuta genaamd *Mojo*.

Mojo

Mojo is ontworpen als een ongedekte digitale valuta die eigenlijk alleen nuttig was binnen de context van het bestandsuitwisselingsnetwerk.

Specifiek had Mojo de taak om een markt voor bestandsdeling en andere taken mogelijk te maken. Waar Napster-gebruikers hun eigen bestanden gratis deelden, konden Mojo Nation-gebruikers elkaar betalen voor de service, en de prijzen zouden worden bepaald door vraag en aanbod. Iemand zou bijvoorbeeld kunnen aanbieden om 1.000 Mojo te betalen voor elk gecodeerd deel van een bestand dat weer in elkaar gezet kan worden als een DVD-rip van *The Matrix*: wie een of meerdere van deze gecodeerde delen had, kon het aanbod accepteren als ze dachten dat het hun tijd, moeite en bandbreedte waard zou zijn om ze te uploaden. De verdiende Mojo's konden vervolgens worden gebruikt om andere diensten op het netwerk te kopen, of misschien in te ruilen voor dollars op een speciale Mojo-handelsbeurs.[234]

'De mensen die betaald krijgen, zijn degenen die de diensten uitvoeren. Dus die agenten die je hebben geholpen om dat blok [bestand] te vinden, worden betaald', legde McCoy uit. 'De verspreide zoekagenten krijgen betaald. Alle verschillende blokservers waar je blokken van hebt gekocht krijgen betaald, en als de gebruiker via een *relay-server* werkte, hetzij omdat ze achter een firewall zaten of omdat ze hun privacy wilden beschermen, zou de persoon die berichten doorgaf ook een deel van de betaling ontvangen.'[235]

McCoy's visie was dat heel Mojo Nation zou worden gestuurd door marktprocessen, waarbij de ene gebruikers probleem de volgende gebruikers gelegenheid was om wat geld te verdienen door het op te lossen. Dit zou het Mojo Nation-

234 Als een interessant detail werden de meeste Mojo-transacties aanvankelijk alleen tussen twee peers geregistreerd, waarbij elke peer krediet of schuld opbouwde bij de ander. De schuld werd pas vereffend met een daadwerkelijke Mojo-token wanneer een bepaalde drempel werd bereikt.

235 Cave, *The Mojo solution*.

netwerk quasi-autonoom laten functioneren, hoopte de Cypherpunk, met zeer weinig dagelijkse betrokkenheid van Autonomous Zone Industries.

Een opvallende uitzondering op deze regel bestond echter wel. De munteenheid van Mojo Nation werd beheerd door Autonomous Zone Industries *zelf*, via een speciale tokenserver die de rekeningsaldi bijhield en dubbele uitgaven voorkwam. Bovendien functioneerde de server als een gecentraliseerde muntfabriek: het kon nieuwe Mojo uitgeven wanneer McCoy en zijn collega's geloofden dat dit nodig was, zonder technische beperking op hoeveel ervan gecreëerd kon worden.

Het resulteerde uiteindelijk in de vernietiging van de munteenheid. Toen sommige gebruikers slimmigheidjes ontdekten om anderen te bedriegen om hun munten naar hen te sturen, besloot het team van Mojo Nation de slachtoffers te compenseren met nieuw geld. Dit leidde uiteindelijk tot de uitgifte van zoveel Mojo dat het uiteindelijk resulteerde in hyperinflatie. Mojo was afhankelijk geweest van een vertrouwde derde partij – de muntfabriek – en dat vertrouwen was geschonden.

Om iets als Mojo Nation echt te laten werken, had het waarschijnlijk een onafhankelijke digitale munteenheid nodig.

'[…] we bestudeerden MojoNation kritisch, omdat ons hoofddoel een werkende gemeenschapsmunt voor p2p-diensten was, en tot op zekere hoogte nog steeds is', schreef informaticus Daniel A. Nagy kort na het einde van Mojo Nation aan Jim McCoy. 'Als reden voor het falen, wezen we hyperinflatie aan. MN had geen inflatiebeperkende maatregelen en op den duur leidde dit ertoe dat de Mojo geheel werd geïnflateerd.' Hij voegde eraan toe dat 'Ik geloof in de visie dat de wereld dringend behoefte heeft aan een p2p-cashsysteem. Zonder zo'n systeem zal e-commerce een grote PITA blijven.' [236]

Dat gezegd zijnde, was het vertrouwen op een gecentraliseerd digitaal valutasysteem niet het enige probleem waarmee Mojo Nation te kampen had. Hoewel de software door meer dan 100.000 mensen werd gedownload en gebruikt,[237] bleken meerdere onderdelen van het systeem erg moeilijk om draaiende te krijgen (en te houden). Met problemen variërend van netwerkinstabiliteit tot ontbrekende

236 Daniel A. Nagy, opmerkingen als antwoord op *The Mojo Nation Story — Part 2*, *Financial Cryptography*, 12 oktober 2005, online

237 Bryce Wilcox-O'Hearn, *Experiences Deploying A Large-Scale Emergent Network*, Peer-to-Peer Systems: 104–110.

bestandsfracties en een gebrek aan vertrouwen tussen gebruikers,[238] was de dienst waarschijnlijk te ambitieus voor het bescheiden budget van Autonomous Zone Industries: het bedrijf zat binnen een paar jaar door zijn geld heen en de negatieve publiciteit rond Napster maakte het moeilijk om meer financiering te verkrijgen.

In 2002 zag McCoy zich gedwongen om de meeste werknemers te ontslaan.

BitTorrent

Hoewel Mojo Nation ten onder ging, waren er enkele ontwikkelaars bij de start-up die hun vooruitstrevende technologieën niet wilden laten vergaan. Zo besloot Wilcox bijvoorbeeld de code van Mojo Nation te kopiëren (forken) om een versie van het protocol genaamd Mnet uit te brengen. Daarnaast bracht ook een andere medewerker van Autonomous Zone Industries, de 28-jarige software-ontwikkelaar en Cypherpunk Bram Cohen, zijn eigen op Mojo Nation geïnspireerde bestands-uitwisselingsnetwerk uit.

Hij noemde het: BitTorrent.

Cohen had Mojo Nation in feite tot op de bot gestript. BitTorrent nam sommige van McCoy's ideeën over, zoals het opdelen van bestanden in kleinere fracties. Maar verder was het protocol vrij eenvoudig: er waren geen ingebouwde archivaris (indexen, torrent-bestanden genoemd, werden buiten het protocol onderhouden en verspreid), er waren geen zoekagenten (gewone websites, opnieuw buiten het protocol, konden gebruikers helpen specifieke torrent-bestanden te vinden), en er was geen eigen valuta.

BitTorrent had geen eigen munteenheid nodig, omdat niemand hoefde te betalen voor bestanden. In plaats daarvan uploaden gebruikers, die de verschillende delen van een bestand downloaden, deze delen gelijktijdig naar andere downloaders. Dit betekende dat bestanden technisch gezien altruïstisch gedeeld werden, maar op zo'n manier dat de last op hulpbronnen voornamelijk werd gedragen door degenen die ook profiteerden van de bestandsoverdrachten.

En zo had Cohen een echt peer-to-peer en volledig gedistribueerd bestands-overdrachtprotocol ontworpen. Waar Napsters P2P-netwerk effectief kon worden uitgeschakeld door juridische druk uit te oefenen op het bedrijf erachter en

238 Wilcox-O'Hearn, *Large-Scale Emergent Network*.

zelfs het veel ambitieuzere Mojo Nation niet kon functioneren zonder dat de Autonomous Zone Industries een valutasysteem voor het netwerk onderhield, was BitTorrent niet van enige betrouwbare derde partij afhankelijk.

Vanuit een juridisch oogpunt waren gebruikers nu voor het eerst volledig verantwoordelijk voor hun eigen file sharing activiteiten. Net als e-mail (SMTP) of zelfs het internet zelf (IP), was BitTorrent in wezen slechts een internetprotocol. Bram Cohen was op geen enkele wijze aansprakelijk voor hoe mensen het protocol gebruikten, zelfs al werd er op grootschalige wijze illegaal auteursrechtelijk beschermde bestanden uitgewisseld via BitTorrent.

Bovendien, als Cohen om welke reden dan ook legale druk zou ondervinden, zouden noch hijzelf, noch het later door hem opgerichte BitTorrent-bedrijf op technisch niveau controle over het BitTorrent-netwerk kunnen uitoefenen. Hoewel Cohen de software initieel creëerde, werd deze bediend door mensen over de hele wereld. Het netwerk werd al snel bijna onmogelijk om te censureren en zo goed als onstopbaar — zelfs de maker kon dit niet veranderen.

BitTorrent zou zich in de volgende jaren vestigen als de standaard voor bestandsoverdrachten. Ongeveer een decennium na Cohens eerste software-release, in het begin van de jaren 2010, had het protocol op elk moment van de dag minstens vijftien miljoen gelijktijdige gebruikers,[239] en in een typische maand waren er wereldwijd zo'n 150 miljoen mensen verbonden met het netwerk.[240] Alles bij elkaar opgeteld, werd geschat dat BitTorrent-gebruikers verantwoordelijk waren voor zo'n 25 tot 30 procent van al het internetverkeer in de wereld, wat meer was dan enig ander protocol in die tijd.[241]

Zonder een centrale entiteit die ze nog konden aanklagen, hadden muziekartiesten en platenmaatschappijen weinig andere keuze dan zich ook aanpassen aan de nieuwe realiteit. In plaats van te proberen hun muziek van het internet te verwijderen, verschoven ze uiteindelijk hun inspanningen om te concurreren met diensten om bestanden te delen door hun nummers gemakkelijk beschikbaar te maken via handige softwaretoepassingen (zoals Apple's iTunes) en later, streamingdiensten. Slechts een paar jaar na de introductie van BitTorrent zou het

239 Liang Wang, *BitTorrent Mainline DHT Measurement*, *MLDHT*, 2013, online

240 BitTorrent, *BitTorrent and µTorrent Software Surpass 150 Million User Milestone; Announce New Consumer Electronics Partnerships*, BitTorrent.com, 9 januari 2012, online

241 Hendrik Schulze and Klaus Mochalski, *Internet Study 2008/2009*, ipoque.

kopen van een fysieke cd (of zelfs het bezit van muziek in het algemeen) ouderwets lijken.

Misschien had deze kennis de doorgewinterde Cypherpunks aan het einde van de jaren 1990 enige hoop kunnen bieden. Een van *hun* technologieën zou niet alleen de wereld veroveren, maar, nog relevanter: Cohens code revolutioneerde hoe mensen het internet gebruikten en ernaar keken. Dit dwong uiteindelijk een volledige transformatie van de entertainmentindustrie af.

Waar Wei Dai, Eric Hughes, en andere Cypherpunks dachten dat elektronisch geld en andere crypto-tools alleen succesvol zouden zijn als het publieke bewustzijn over het belang van online privacy toenam, zou BitTorrent jaren later aantonen dat het ook andersom kon werken: een krachtige genoeg technologie kon, op zichzelf, helpen de heersende cultuur te veranderen.

Hoofdstuk 13

RPOW

In het begin van de jaren 2000 had de Cypherpunk-beweging het grootste deel van zijn momentum verloren.

Terwijl sommige van de oorspronkelijke Cypherpunks gedesillusioneerd raakten en stopten met deelnemen aan de Cypherpunk-mailinglijst, ging de algehele kwaliteit van dit discussieplatform achteruit, met veel nieuwe berichten die weinig meer waren dan gescheld en schreeuwpartijen, of zelfs regelrechte spam. John Gilmore, de oorspronkelijke host van de lijst, had eind jaren 1990 geprobeerd om een moderatiebeleid te introduceren, maar dit werd streng afgewezen door mensen zoals Tim May, die zich in reactie daarop uitschreef (May keerde terug toen het beleid werd aangepast om boze berichten en andere inhoud van lage kwaliteit om te leiden in plaats van te censureren, hoewel hij nog steeds niet blij was met de veranderingen).[242]

Gilmore besloot uiteindelijk te stoppen met het hosten van de mailinglijst, waarna enkele van de overgebleven abonnees nieuwe groepen creëerden en overstapten naar Usenet, die op een meer verspreide manier konden worden gehost door meerdere mensen tegelijk.[243] Desalniettemin, zou het verval van de beweging alleen maar versnellen. Na de terroristische aanslagen van 11 september 2001, maakte een scherpe toename van digitale surveillance mensen huiverig om discussies over radicale privacytools te faciliteren, en toen de enige resterende

242 Tim May, *My Departure, Moderation, and Ownership of the List*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 2 februari 1997, online

243 Mark Frauenfelder, *Homeless Cypherpunks Turn to Usenet*, *Wired*, 17 februari 1997, online

Cypherpunk-server werd gehost vanaf het webadres al-qaeda.net, besloot zelfs Tim May dat het tijd was om te vertrekken. Dit keer, voorgoed.

Dat betekende niet dat de Cypherpunk-ethos verloren of volledig vergeten was. Velen van de Cypherpunks behielden hun interesse in bestaande privacytools zoals PGP, evenals in nieuwe technologieën zoals Tor (The Onion Router): het privacy-netwerk dat in 2002 werd gelanceerd leek op Zero-Knowledge Systems' Freedom, maar vereiste geen betaald abonnement. Tor stelde iedereen in staat om anoniem het internet te gebruiken.

Veel van de Cypherpunks bleven ook in contact via andere middelen. Online migreerden nogal wat van hen uiteindelijk naar de strikter gemodereerde Cryptografie mailinglijst, die soms werd beschouwd als de feitelijke opvolger van de Cypherpunk-lijst. Offline liepen enkele van de Cypherpunks elkaar regelmatig tegen het lijf op cryptografieconferenties of hackerevenementen.

Ondertussen ontstonden vele andere initiatieven voor elektronisch geld. Rond de overgang van het millennium werkten honderden start-ups aan online betalingssystemen, en veel van deze bedrijven omschreven hun oplossingen als een vorm van digitaal geld. Hoewel dat vaak gewoon betekende dat de betaalsystemen snel, goedkoop en gemakkelijk te gebruiken waren, waren ze niet per se privé. CyberCash, bijvoorbeeld, trok veel media-aandacht voor zijn digitaal geldsysteem, genaamd CyberCoin, dat zich specialiseerde in kleine betalingen in plaats van anonimiteit. Hetzelfde gold voor het systeem van elektronisch geld van Compaq, dat veel aandacht trok, genaamd Millicent.

Andere initiatieven die enig potentieel toonden, zoals n-Count (medeontworpen door een voormalige werknemer van DigiCash), Proton (een project van samenwerkende Europese banken), of Mondex (een initiatief van de Britse bank NatWest dat later werd verkocht aan Mastercard), waren vooral gebaseerd op het concept van fysieke smartcards. Net zoals de smartcard die in ontwikkeling was bij de start-up van David Chaum, moesten deze stukken hardware (gelijkend aan een kredietkaart) vooraf geladen worden met een waarde die fiatvaluta vertegenwoordigde, om vervolgens te worden gebruikt voor persoonlijke transacties. Hoewel de meeste van deze privacyfuncties aanboden, waren ze vooral ontworpen om fysiek geld te vervangen in plaats van te dienen als anonieme valuta voor cyberspace.

Misschien nog dichter bij de visie van de Cypherpunks, richtte Robert Hettinga, die sinds 1996 de jaarlijkse Financial Cryptography conferenties had georgani-

seerd, in 1999 de Internet Bearer Underwriting Corporation op. Na het falen van DigiCash, wilde deze Cypherpunk financiering veiligstellen om een nieuw soort eCash-systeem te ontwikkelen, maar deze keer geoptimaliseerd voor goedkope transacties. Hij was van mening dat sterke privacygaranties niet alleen individuen beschermen tegen Big Brother, maar dat ze ook de wrijving kunnen verminderen en dus economische voordelen kunnen opleveren.

Maar geen van deze projecten heeft haar beloftes kunnen waarmaken. Hoewel sommige technologieën banenbrekend waren in specifieke sectoren, zoals het openbaar vervoer of voor betaalkaarten voor telefooncellen, slaagde digitaal geld er niet in om veel aantrekkingskracht te winnen bij het algemene publiek. Door het gebrek aan interesse begon de financiering ook te verminderen.

'Eerlijk gezegd is het dot-com geld verdwenen', concludeerde Hettinga in 2001, nadat hij er niet in geslaagd was genoeg geld op te halen om het elektronische geldsysteem van zijn bedrijf te ontwikkelen. 'We gaan ook over terrein waar CyberCash, DigiCash en veel andere mensen hun vingers aan verbrand hebben.'[244]

In plaats van het investeren in nieuwe crypto-initiatieven, richtten traditionele banken en financiële dienstverleners zich op het verbeteren van bestaande cashloze betalingsystemen, zoals transacties via creditcards en betaalpassen. Intussen wonnen flamboyante nieuwe web-gebaseerde betalingsverwerkers zoals PayPal snel aan marktaandeel en het leek erop dat privacy (laat staan monetaire hervorming) geen grote zorg was voor de meesten van hen. De dystopische toekomst waar Chaum en veel van de Cypherpunks voor gewaarschuwd hadden (een toekomst waarin alle financiële transacties konden worden gemonitord, geregistreerd en mogelijk gecensureerd) werd snel realiteit.

Toch was niet iedereen bereid de hoop op te geven…

Hal Finney

Geboren in het voorjaar van 1956 in het kleine Californische dorpje Coalinga, toonde Hal Finney al vroeg, nog als een jong kind, een interesse in codes: op de basisschool, vond hij het leuk om codes met letters en cijfers te maken voor willekeurige teksten die hij tegenkwam.

244 Declan McCullagh, *Digging Those Digicash Blues*, *Wired*, 14 juni 2001, online

Iets later, in zijn tienerjaren, ontwikkelde Hal een fascinatie voor computers. Gelukkig was de middelbare school die hij bezocht zijn tijd ver vooruit: de schooladministratie maakte al gebruik van een computer voor het beheer en de opslag van leerlinggegevens jaren voordat dit gebruikelijk werd. Jonge Hal, enthousiast om met de machine te werken, bood vrijwillig zijn hulp aan het schoolpersoneel aan, waardoor hij tussen de lessen door een soort bijbaantje kreeg.

Finney behaalde in 1974 zijn middelbareschooldiploma als beste student van zijn klas en werd toegelaten tot het California Institute of Technology (Caltech), één van de meest prestigieuze en selectieve universiteiten ter wereld. Omdat Caltech toen nog geen bacheloropleiding in informatica aanbood, besloot hij een opleiding in techniek te volgen, terwijl hij tegelijkertijd zoveel mogelijk programmeercursussen volgde.

Rond dezelfde tijd ontwikkelde Finney een sterke waardering voor logica en omarmde hij de libertaire filosofie. Hij ging graag filosofische discussies aan met zijn medestudenten aan de universiteit, waar een combinatie van prikkelende ideeën, stevige argumentaties en een bedachtzame benadering van gesprekken hem veel aandacht opleverde van zijn leeftijdsgenoten. Onder hen was Fran, het meisje met wie hij later zou trouwen en de rest van zijn leven zou doorbrengen.

Kort na zijn afstuderen aan Caltech in 1978, vond Finney zijn eerste serieuze baan als programmeur bij een kleine ingenieursfirma APh Technological Consulting. APh was zojuist een samenwerking gestart met speelgoedfabrikant Mattel om het besturingssysteem voor hun Intellivision-spelcomputer te ontwikkelen, naast een aantal vroege spellen. In de daaropvolgende jaren zette Finney zijn werk voort in het ontwikkelen van baanbrekende videogames zoals *Space Battle* en *Star Strike* voor de Intellivision, alsook *Adventures of Tron*, *Astroblast!* en *Space Attack* voor het Atari Video Computersysteem.

Als algemeen optimistisch mens, was Finney ervan overtuigd dat de wereld van morgen beter zou zijn dan die van vandaag, en stond hij open voor verandering. Dus toen de Extropiaanse-gemeenschap eind jaren '80 begon te vormen, paste hij er ook goed in. Het vooruitzicht van technologische vernieuwingen zoals nanotechnologie, kunstmatige intelligentie en *mind uploading* maakte hem enthousiast. En als een overtuigd atheïst die niet in het hiernamaals geloofde, was Finney al erg geïnteresseerd in het potentieel van cryonics sinds hij over het concept las

tijdens zijn eerste jaar op de universiteit.

Zoals Fran het later zei: 'Hij geloofde niet in God. Hij geloofde in de toekomst.'[245]

Cypherpunkrealisme

Toen het internet begin jaren '90 voor het eerst publiek toegankelijk werd, was Finney een van de allereerste gebruikers die zich een verbinding wist te bemachtigen.

Terwijl hij de verschillende, op dat moment enkel op tekst gebaseerde, hoeken van de gloednieuwe informatiesnelweg verkende, herkende Finney al snel het revolutionaire potentieel van het ontluikende digitale domein. Voor het eerst zou de mensheid over de hele wereld verbonden zijn, ongeacht geografische afstanden, willekeurige grenzen of culturele verschillen. Hij geloofde dat de gevolgen hiervan de wereld zouden veranderen.

Maar al snel besefte hij dat er ook een nadeel was aan de digitalisering van communicatie. Als kenner van de technische architectuur van het internet, wist Finney dat zonder beschermende maatregelen, cyberspace rampzalige inbreuken op individuele privacy kon faciliteren: alles dat iemand online doet, kon potentieel bespioneerd worden. Hij voorzag dat het internet eigenlijk een bedreiging voor de menselijke vrijheid kon worden. Dit was het geval voor gewone communicatie, en Finney dacht dat dit net zo goed opging voor financiële transacties.

'Er kunnen dossiers worden gemaakt die de uitgavenpatronen van ons allemaal volgen', waarschuwde Finney. 'Als ik nu iets bestel via de telefoon of elektronisch met mijn Visa kaart, wordt er een registratie bijgehouden van hoeveel ik precies heb uitgegeven en waar ik het heb besteed. Naarmate de tijd vordert, kunnen er meer transacties op deze manier plaatsvinden en het uiteindelijke resultaat kan een groot verlies aan privacy zijn.'[246]

Het internet had behoefte aan een ontraceerbare vorm van geld, concludeerde Finney — digitaal contant geld. En hij was opgetogen te ontdekken dat zo'n

245 Nicole Weinstock, *Member Profile: Hal Finney*, *Cryonics 40*, issue 2: 9.

246 Hal Finney, *Re: Physical to digital cash, and back again*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, August 19, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00581.html]

systeem al in ontwikkeling was.

'Het leek me zo duidelijk', herinnerde Finney zich later. 'We worden geconfronteerd met problemen zoals het verlies van privacy, oprukkende computarisering, enorme databases en meer centralisatie, en Chaum biedt een volledig andere weg om in te slaan, eentje die macht in handen van individuen legt in plaats van regeringen en bedrijven. De computer kan eerder als instrument gebruikt worden om mensen te bevrijden en te beschermen, in plaats van hen te controleren.'[247]

Finney had daarom een uitnodiging aanvaard van mede-Extropiaan Tim May, die een ontmoeting organiseerde met een groep lokale hackers en cryptografen uit de Bay Area, die zichzelf spoedig de Cypherpunks zouden noemen.

Kort daarna bevond Finney zich in de positie waar hij Chaums eCash-project aan het promoten was onder zijn mede-Extropianen, en op een bepaald moment daarover een zeven pagina's tellende uitleg voor het *Extropy* magazine schreef. Finney schreef aan de techno-libertarische menigte dat cryptografie individuen kon beschermen tegen overheidsmacht, inmenging, en controle, en legde uit hoe elektronisch geld de Extropiaanse zaak kon bevorderen.

En, als een echte Cypherpunk, schreef Finney code. De game-ontwikkelaar was verantwoordelijk voor een vroeg Cypherpunk-succes toen hij Eric Hughes hielp de allereerste Chaumian remailer te ontwikkelen. Het was ook Finney's idee om de uitdaging te organiseren om de (verzwakte) export-grade encryptiestandaard van Netscape te kraken, een uitdaging die voltooid werd door mede-Cypherpunk Ian Goldberg. Dit bleek een grote overwinning tijdens de crypto-oorlogen.

Maar Finney's meest opmerkelijke bijdragen vielen ten goede aan PGP: nadat Phil Zimmermann voor het eerst de encryptietool had uitgebracht, werd Finney een belangrijke bijdrager aan het project. De tweede versie van de software, een grote verbetering ten opzichte van versie 1, werd grotendeels door hem ontwikkeld, hoewel dit een beetje stil werd gehouden om Finney te behoeden voor mogelijke juridische problemen zoals Zimmermann die ondervond. Een paar jaar later zou Finney de eerste werknemer worden van Zimmermanns PGP-bedrijf.

Finney stond echter niet achter de visie van Tim May om met behulp van Cypherpunk-hulpmiddelen een crypto-anarchistische samenleving te stichten.

---

247 Hal Finney, *Why remailers...*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 15 november 1992, online

Dit was niet omdat hij het idee om de staat uit economische interacties te verwijderen niet leuk vond, of omdat de ideeën van May op dat vlak te radicaal voor zijn smaak waren. Als een Extropiaan en libertariër vond Finney in feite dat Mays visie in principe geweldig klonk. Hij geloofde echter niet dat Mays idee om een anarchistische samenleving te bereiken door middel van cryptografie erg realistisch was.

'[…] er bestaat niet zoiets als cyberspace', schreef Finney op een gegeven moment aan de mailinglijst van de Cypherpunks in reactie op een van de betogen van May. 'Ik ben nu niet in cyberspace, ik ben in Californië. Ik val onder de wetten van Californië en de Verenigde Staten, ook al communiceer ik met een andere persoon, of het nu per post of elektronisch is, via telefoon of TCP/IP-verbinding. Wat betekent het om te spreken over een regering in cyberspace? Het is de regering in de fysieke ruimte die ik vrees. Haar agenten dragen fysieke wapens die echte kogels afvuren. Totdat ik in mijn computer kan leven en elektronen kan eten, zie ik de relevantie van cyberspace niet in.' [248]

Hoewel individuen Cypherpunk hulpmiddelen konden gebruiken om hun privacy te beschermen, geloofde Finney niet dat de meeste mensen hun hele leven zich in cyberspace zouden kunnen *verbergen*. Zelfs als Cypherpunk-hulpmiddelen een kleine groep technisch onderlegde elite zouden kunnen helpen om bepaalde wetten te omzeilen, verwierp hij de gedachte dat dit de beschaving ingrijpend zou veranderen, omdat hij uiteindelijk niet geloofde dat een libertaire samenleving gerealiseerd kon worden zonder wijdverspreide steun van de bevolking.

In plaats van een anarchistisch utopia om naar te migreren, zag Finney het internet eerder als een plek voor intellectuele uitwisseling: in plaats van een Galt's Gulch, zag hij cyberspace als een plek om ideeën vrijelijk uit te wisselen en te bediscussiëren. En dit, zo geloofde Finney, was de echte sleutel tot het bereiken van ware vrijheid. De beste en enige manier om een vrije samenleving te creëren was om de massa ervan te overtuigen dat een vrije samenleving een goed idee is.

'In de kern geloof ik dat we de soort samenleving zullen hebben die de meeste mensen wensen. Als we vrijheid en privacy willen, moeten we anderen overtuigen dat deze waardevol zijn. Er zijn geen snelkoppelingen. Terugtrekken in technologie is

248 Hal Finney, *Re: Voluntary Governments?* oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 4 augustus 1994, online

als het over je hoofd trekken van je dekens. Het voelt even goed, totdat de realiteit je inhaalt.'[249]

Elektronisch geld

Ondanks zijn nuchtere en misschien wel meer realistische kijk op de mogelijkheden van cryptografie, was Finney altijd gedreven om elektronisch geld te realiseren. Hij voerde uitvoerig gesprekken over de mogelijkheden hiervan met zowel de Extropianen als de Cypherpunks op hun respectievelijke mailinglijsten, en ook op de Libtech mailinglijst van Nick Szabo.

Op de Cypherpunk-mailinglijst was hij bij gesprekken over digitale valuta altijd één van de meest actieve deelnemers en nam hij soms zelfs een soort ondersteunende rol aan. Hoewel sommige Cypherpunks hevig konden twisten over de beste benadering van elektronisch geld, stond Finney meer open voor verschillende ideeën. In plaats van vast te houden aan één oplossing, gaf hij liever een overzicht van de verschillende compromissen die elk van hen met zich meebracht.

Finney leek bijvoorbeeld grotendeels onbeslist, of misschien beter gezegd, open-minded over het onderwerp van dekking. Hij merkte op dat het dekken van elektronisch geld met fiatvaluta werkte, maar speculeerde soms ook over digitale valuta gedekt door een mandje van goederen, of door een synthetisch gemiddelde van meerdere nationale valuta, of helemaal niet gedekt.

Elke keer wanneer een nieuw voorstel voor elektronisch geld opdook op de mailinglijst, was Finney altijd enthousiast om het te beoordelen, met een speciale nadruk op hun privacyfuncties. Na het bestuderen van het ontwerp, koppelde hij vaak terug op de mailinglijst om in zijn eigen woorden uit te leggen hoe het werkte, hoe het zich verhield tot eerdere voorstellen, en wat hij van het idee vond. Naast (meestal constructieve) feedback voor de indiener, bood Finney aan andere Cypherpunks in wezen een openbare dienst door hen te helpen de mogelijkheden en beperkingen van verschillende benaderingen te begrijpen.

Finney had ook een speciale interesse in de wettelijkheid van elektronisch

249 Hal Finney, *POLI: Politics vs Technology*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 2 januari 1994, online

geld, een onderwerp dat hem in de begindagen van de Cypherpunk-gemeenschap naar de geschiedenis van het geld leidde. Hier kwam hij voor het eerst het werk van George Selgin over vrij bankieren tegen. Terwijl hij wetten over wettig betaalmiddel, belastingregels, bankregulering en meer bestudeerde, deelde Finney zijn bevindingen op de mailinglijst van de Cypherpunks en begon hij de mogelijkheden en risico's in kaart te brengen (het was bijvoorbeeld Finney die ontdekte dat niet-commerciële experimenten voor systemen zoals eCash getolereerd zouden moeten worden, zelfs als ze gebruik maakten van Chaums gepatenteerde blinde handtekeningenschema).

Tegelijkertijd stelde Finney zich terughoudend op tegenover enkele uitspraken, geïnspireerd door crypto-anarchie, over de beloften van elektronisch geld. Ook hier was hij sceptisch over enkele van de meer radicale voorspellingen met betrekking tot massale belastingontduiking en hoe elektronisch geld dit zou mogelijk maken.

'We zijn verblind door het beeld van monetaire stromen die over de hele wereld flitsen. Wat ik echter nooit precies kan plaatsen is, wat precies verhindert dat zoiets vandaag de dag wordt gedaan?' vroeg Finney aan de mailinglijst. 'Als je in goud wilt investeren, kun je toch naar de goudhandelaar gaan en wat kopen? Of je kunt je geld in een beleggingsfonds in goud stoppen en het als een betaalrekening gebruiken. Als je yen of marken wilt, kun je daarin investeren. Als het punt is om dit in het geheim te doen, waarom zou het dan gemakkelijker zijn om je salaris per post naar de digicash-bank in de Bahamas te sturen dan naar een bestaande bank daar?'[250]

Ook hier was het niet zo dat Finney de meer radicale beloftes van Tim May onaantrekkelijk vond. Hij beschouwde ze gewoon als niet erg realistisch. Afgezien van het feit dat de meeste mensen hun belastingen toch al rechtstreeks van hun salaris betaalden, moest iedereen uiteindelijk in de fysieke wereld leven, waar belastingontduiking nog steeds illegaal zou zijn. Het was voor Finney verre van duidelijk dat het verbergen van rijkdom in cyberspace de meeste mensen in het echte leven ten goede zou komen.

'Het lijkt mij dat de zwakte in deze plannen om de overheid te omzeilen met

250 Hal Finney, *Re: Re: re: re: digital cash*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 16 maart 1994, online

digitaal geld zit in de omzetting van fysiek geld naar digitaal geld. Dat lijkt het knelpunt te zijn waar de overheid nog steeds controle kan houden', concludeert Finney.[251]

Herbruikbare proofs-of-work

In de jaren 2000, ongeveer tien jaar nadat Finney bij Extropianen begon te pleiten voor elektronisch geld, was er nog steeds geen succesvol elektronisch geldsysteem. Hoewel een reeks ideeën besproken was op de mailinglijst van de Cypherpunks, en Finney veel van de voorstellen persoonlijk had beoordeeld, was geen van hen van de grond gekomen. In sommige gevallen, zoals bij de start-ups van Chaum of Hettinga, was dit omdat het product uiteindelijk commercieel niet haalbaar bleek te zijn, of althans zo leek het. Maar in andere gevallen, zoals bij het Bit Gold van Nick Szabo of de b-money voorstellen van Wei Dai, waren de systemen in de eerste plaats nooit geïmplementeerd.

Wellicht was het omdat zijn verwachtingen voor het potentieel van elektronisch geld meer ingetogen waren dan die van Tim May en andere crypto-anarchisten in de eerste plaats, of misschien was het gewoon vanwege zijn over het algemeen optimistische karakter, maar waar vele andere Cypherpunks tegen deze tijd ontgoocheld waren geraakt, wilde Finney het idee nog een kans geven. Hij besloot uiteindelijk om een op proof-of-work gebaseerd elektronisch geldsysteem te ontwikkelen, zelfs als het in een vereenvoudigde vorm moest.

In 2004 lanceerde hij *Reusable Proofs of Work*, of kortweg *RPOW* (uitgesproken als *arpow*). Hij nodigde mensen uit om het systeem te testen, adverteerde het elektronische geld op een eenvoudige blauw-groene webpagina met een RPOW-logo in stripboekstijl (denk aan de 'POW' letters die de plek markeren waar Batmans uppercut de kaak van een ongelukkige handlanger raakt).

'Beveiligingsonderzoeker Nick Szabo heeft de term bit gold bedacht om een soortgelijk concept van tokens, dat inherent een bepaald niveau van inspanning vertegenwoordigt, te omschrijven', schreef Finney op de website van het project. 'Het concept van Nick is complexer dan het eenvoudige RPOW-systeem, maar zijn inzicht is van toepassing: op sommige manieren kun je een RPOW-token zien als

251 Finney, *Re: Re: re: re: digital cash*

het hebben van de eigenschappen van een zeldzame grondstof zoals goud. Het kost moeite en uitgaven om goud te delven en munten te slaan, waardoor ze inherent zeldzaam zijn.'[252]

Waar Bit Gold was ontworpen rondom een *eigendomsclub*, zou ook RPOW beheerd worden door specifieke servers. Voor het prototype had Finney zelf een RPOW-server opgezet. Deze voerde de basisbewerkingen uit die nodig zijn voor het elektronische geldsysteem: het gaf nieuwe RPOW-tokens uit (de munteenheden), en controleerde of tokens niet twee keer werden uitgegeven.

Het is belangrijk te vermelden dat de RPOW-server alleen nieuwe tokens uitgaf als aan één van de twee voorwaarden was voldaan: er moest een geldige hash worden ingediend, of een oudere token moest worden ingeleverd als ruil.

De eerste optie was een eenvoudige proof-of-work functie. Als gebruiker Alice een RPOW-token wilde, moest ze verbinding maken met Finney's server (mogelijk via Tor voor optimale privacy), een aantal gegevens die uniek zijn voor de server en voor haarzelf nemen, en beginnen met hashen tot ze een geldige hash (beginnend met genoeg nullen) vond. Vervolgens stuurt ze de hash naar de server, die deze op geldigheid controleert, en (indien geldig) een unieke RPOW-token terugstuurt, in feite gewoon een unieke gegevensreeks. De server bewaarde ook een kopie van de token in een lokale database.

Wanneer Alice een RPOW-token wilde uitgeven, bijvoorbeeld om een MP3-bestand te kopen, zou ze het simpelweg naar de beoogde ontvanger, Bob, sturen. Technisch gezien maakte het voor het RPOW-systeem niet uit hoe ze het verzond, zolang ze er maar zeker van was dat het bij Bob terechtkwam zonder dat iemand het onderschepte (een bericht aan Bob versleuteld met zijn publieke sleutel zou de klus klaren).

Wanneer Bob de RPOW-token ontving, zou hij deze moeten valideren en controleren dat deze niet dubbel was uitgegeven. Hij zou daarom de token direct doorsturen naar de RPOW-server, die naging of de token in de interne database stond en of deze niet dubbel was uitgegeven. Als de token geldig was, zou de server dit aan Bob bevestigen. Hierdoor kon Bob het MP3-bestand naar Alice sturen. De server zou ook de RPOW-token als uitgegeven bestempelen, waardoor deze in de toekomst niet meer gebruikt kon worden.

252 Hal Finney, *Reusable Proofs of Work*, RPOW website index pagina, online

Ten slotte zou de server Bob een nieuw RPOW-token geven, en die nieuwe token opnemen in zijn interne database. Op deze manier kon Bob de nieuwe token later uitgeven.

Stel je voor dat Bob zijn nieuwe RPOW-token wil gebruiken om toegang te krijgen tot Carols website. Als Carol de RPOW-token van Bob krijgt, stuurt ze hem weer door naar de RPOW-server van Finney. De server bevestigt dan dat de token echt is, markeert deze als besteed in zijn interne database en geeft vervolgens een nieuwe RPOW-token uit aan Carol. Deze wordt ook toegevoegd aan de interne database van de server.

Op deze manier kon het proof-of-work, vertegenwoordigd door een enkele geldige hash (gemaakt door Alice), effectief oneindig blijven circuleren. Het was inderdaad *herbruikbaar* proof-of-work.

Betrouwbaar rekenen

Het systeem zoals tot dusver beschreven zou vrij goed werken, behalve dat het vertrouwen vereist in de beheerder van de RPOW-server om geen dubbele uitgaven te doen of RPOW-tokens voor zichzelf te maken zonder een proof-of-work te leveren. Finney wilde echter niet dat de gebruikers de beheerder van de RPOW-server moesten vertrouwen, zelfs als die beheerder hijzelf was. Daarom voegde Finney nog een speciale eigenschap toe aan het ontwerp.

Ten eerste zou de RPOW-server gebruik maken van gratis en open source software. Iedereen kon online de broncode van RPOW vinden en controleren hoe het functioneerde.

En, als hoofdinnovatie van het systeem, was de RPOW-server gehost op een veilige hardwarecomponent, de IBM 4758. Dit maakte *betrouwbaar rekenen* mogelijk.

Kortom, de sabotagebestendige hardware bevatte een geheime sleutel, ingebed door IBM, die niemand, zelfs niet de eigenaar van de veilige hardwarecomponent, kon manipuleren of eruit kon halen. Met behulp van een techniek die *remote attestation* wordt genoemd, kon de geheime sleutel vervolgens de gratis en open source software die op de veilige hardwarecomponent was geïnstalleerd, cryptografisch ondertekenen. Met deze handtekening en de bijbehorende publieke

sleutel van IBM kon iedereen verifiëren dat de veilige hardwarecomponent daadwerkelijk de RPOW-broncode uitvoerde die Finney had gepubliceerd, zonder achterdeuren of aanpassingen.

Zolang men IBM vertrouwde om niet mee te werken met Finney om een valse handtekening te fabriceren (en aannemende dat de centrale server niet volledig offline ging), konden RPOW-gebruikers er zeker van zijn dat het elektronische geldsysteem functioneerde zoals het moest.

'[…] Het RPOW-systeem is ontworpen met één overkoepelend doel: het onmogelijk maken dat iemand, zelfs de eigenaar van de RPOW-server of zelfs de ontwikkelaar van de RPOW-software, in staat zou zijn om de regels van het systeem te overtreden en RPOW-tokens te vervalsen', legde Finney uit op de RPOW-website. 'Zonder zo'n garantie tegen vervalsbaarheid, zouden RPOW-tokens het werk dat is gedaan om ze te creëren niet geloofwaardig kunnen vertegenwoordigen. Vervalsbare tokens zouden meer lijken op papiergeld dan op bit-goud.'[253]

Het lot van RPOW

De eerste RPOW-release was weliswaar nog erg ruw, maar Hal Finney had het voornemen het project in de loop van de tijd te verbeteren. Wellicht het belangrijkst, hij plande om het systeem te upgraden zodat het op meerdere, onafhankelijk van elkaar opererende, servers zou draaien. Zo zou het volledige RPOW-systeem niet onderuit gaan als zijn server om welke reden dan ook offline ging.

Ondertussen vond de Cypherpunk het ook leuk om te experimenteren en te sleutelen aan de RPOW-software. Zo heeft hij bijvoorbeeld een BitTorrent-client aangepast om samen te werken met zijn elektronische geldsysteem. Dit leek op het Mojo Nation concept en stelde gebruikers in staat om andere gebruikers te betalen als ze hun download wilden versnellen. In een even creatieve toepassing van de RPOW-technologie werkte hij aan een peer-to-peer pokerapplicatie. Hier konden gebruikers tegen elkaar spelen, waarbij de RPOW-tokens automatisch naar de digitale portemonnee van de winnaar werden overgemaakt.

Finney kreeg al snel hulp van een jongere ontwikkelaar genaamd Gregory

253 Hal Finney, *RPOW Theory*, RPOW website theorie pagina, online

Maxwell, die een actieve interesse toonde in het elektronische geldsysteem. Maxwell droeg bij aan het project met code, en overwoog om geavanceerde bestedingsvoorwaarden zoals escrow-betalingen te implementeren. Hij besprak met Finney ook mogelijke oplossingen voor sommige van de meer subtiele technische uitdagingen, zoals het instellen van vervaltermijnen voor tokens, of de relatief zwakke versleuteling die de veilige hardwarecomponent beveiligde.

Helaas voor Finney bleek Maxwell echter een zeldzame uitzondering. Omdat bijna niemand anders interesse toonde in het elektronische geldsysteem, lukte het RPOW niet om door te breken.

Dit was waarschijnlijk ten minste gedeeltelijk te wijten aan het feit dat RPOW geen heel goede vorm van geld was. Geconfronteerd met hetzelfde probleem als Adam Backs hashcash, een probleem dat Szabo en Dai geprobeerd hadden op een omslachtige manier op te lossen, zouden computationele verbeteringen het na verloop van tijd goedkoper maken om geldige hashes te genereren, wat suggereert dat de markt uiteindelijk zou worden overspoeld met RPOW-tokens. De verwachting van hoge inflatie werkte ontmoedigend om de RPOW-valuta-eenheden te bezitten.

'Het klopt dat als de Wet van Moore blijft gelden, de kosten voor het vervaardigen van een *proof-of-work*-token exponentieel zullen blijven dalen', gaf Finney toe op de website van het project. 'Maar onthou dat dit geen geld is en niet bedoeld is als een stabiel middel om waarde op te slaan. Het is eerder bedoeld als een gemakkelijk te ruilen representatie van computerrekenkracht.'[254]

Inderdaad, het elektronische geldsysteem van Finney fungeerde niet zozeer als een breed geaccepteerde waardeopslag of rekeneenheid. Het werd vooral nuttig geacht als ruilmiddel op plaatsen waar hashcash zinvol kon zijn, bijvoorbeeld om te dienen als *postzegels* voor het beperken van spam.

Maar waarschijnlijk slaagde het elektronische geldsysteem er ook niet in om van de grond te komen omdat het de opstartuitdaging niet kon overwinnen. Geld is enkel nuttig als anderen het accepteren als betaalmiddel, maar zonder een economische stimulans om RPOW-tokens bij te houden, hadden de meeste mensen daar geen reden toe. En zonder dat er iemand was die de tokens als betaling accepteerde, was er ook niemand die ze wilde uitgegeven, wat betekende

254 Hal Finney, *RPOW FAQs*, RPOW website FAQ pagina, online

dat er nog minder reden was voor iemand om ze in eerste instantie te accepteren als betaling…

'Het had het probleem dat er min of meer niets was om het voor te gebruiken', concludeerde Maxwell ook, die jaren later terugkeek op het RPOW-project, 'wat het moeilijk maakte om de aandacht erop gericht te houden.'[255]

Net als eCash en hashcash voorheen, leed ook RPOW aan een kip-en-ei-probleem.

E-gold

Ondanks de beste bedoelingen van Hal Finney is RPOW halverwege de jaren 2000 geëindigd als nog een mislukte poging om elektronisch geld te creëren.

Het was op dit moment dat sommige techno-libertariërs wat nieuw perspectief vonden in een alternatieve vorm van internetgeld, die met een zeer verschillend ontwerp, succesvoller leek te zijn: e-gold.

Het project van Douglas Jackson, een digitale valuta gedekt door goud, groeide rond het midden van de jaren 2000 snel. Het voldeed aan verschillende van de eisen die de Cypherpunks hadden gesteld aan elektronisch geld: transacties konden met enige mate van anonimiteit worden uitgevoerd, het systeem ondersteunde microtransacties tot op één tienduizendste van een gram goud en, natuurlijk, goud zelf vertegenwoordigde onvervalsbare kostbaarheid. Naarmate de technologie van e-gold verbeterde, konden ontwikkelaars zelfs computerprogramma's in het systeem integreren via een Application Programming Interface (API), waardoor oplossingen die op slimme contracten leken mogelijk werden.

Er was natuurlijk één vereiste waaraan e-gold niet kon voldoen. De ervaring met DigiCash's Cyberbucks had de Cypherpunks geleerd wat er kon gebeuren met een digitale munteenheid als het afhankelijk was van één enkel bedrijf, en de klanten van Douglas Jackson zouden deze les binnenkort ook leren. Met de arrestatie van de CEO en federale agenten die het kantoor van het bedrijf in 2006 binnenvielen, was er weer een internetvalutaproject mislukt. Szabo's stelling klonk nogmaals luid en duidelijk: *vertrouwde derde partijen zijn veiligheidslekken*.

Na meer dan twintig jaar van niet-gerealiseerde voorstellen, verlaten projecten

255 Gregory Maxwell, IRC message to author, 13 augustus 2020.

en mislukte start-ups, bestond er nog steeds geen elektronisch geld.

Intussen werd de noodzaak om een alternatief voor fiatgeld te vinden steeds groter…

Deel III

Bitcoin

Hoofdstuk 14

Fiat in de 21ste eeuw

Voor het grootste deel van zijn leven voelde Friedrich Hayek dat zijn ideeën waren gemarginaliseerd. Spontane orde van onderaf moest het onderspit delven voor de economische staatsinterventie van John Maynard Keynes, die van bovenaf functioneert. In plaats van rentetarieven die bepaald werden door de markt, hadden centrale banken het goud vaarwel gezegd om het manipuleren van de rente nog gemakkelijker te maken. En geld, verre van gedenationaliseerd, was een strategisch instrument geworden op het globale geopolitieke schaakbord.

Weinig schaakspelers waren zo sluw als de Amerikaanse president Richard Nixon.

Door in 1971 effectief het Bretton Woodssysteem te ontbinden, had Nixon een liquiditeitscrisis weten te voorkomen toen landen hun dollarreserves opnieuw naar goud begonnen om te zetten. Maar dat zou natuurlijk uit zichzelf de problemen die veroorzaakt werden door het begrotingstekort van Amerika niet oplossen. Het vertrouwen in de dollar begon te dalen nu die niet langer werd gedekt door edelmetaal, en het begon erop te lijken dat de Verenigde Staten hun dominante positie in het internationale financiële systeem mogelijks zouden verliezen.

Nixon zou een oplossing vinden tijdens een wereldwijde oliecrisis.

In 1973 riepen olieproducerende Arabische landen, verenigd in de *Organization of the Petroleum Exporting Countries* (OPEC), bestaande uit meerdere overheden, een olie-embargo uit over landen die Israël steunden tijdens de Oktoberoorlog

tussen de joodse staat en Egypte. De landen voor wie de handel verboden werd, waren Amerika, het Verenigd Koninkrijk en vele andere westerse landen. Het veroorzaakte een scherpe stijging in de olieprijs, met verstrekkende negatieve gevolgen voor de gehele wereldeconomie.

Als reactie hierop werd in 1973 de nieuwbenoemde Amerikaanse minister van Financiën, William Simon, naar Saudi-Arabië gestuurd, een lidstaat van de OPEC. Zijn taak was om olie als economisch wapen te neutraliseren, het vestigen van een stevige greep van de Sovjet-Unie in de regio te voorkomen en bovendien een oplossing voor de dollarcrisis te vinden; al met al geen gemakkelijke klus. Maar Simon ging de onderhandelingen in met een sterk drukkingsmiddel: het Amerikaanse leger.

De overeenkomst die Simon wist te sluiten met de Saoedische koninklijke familie zou het geopolitieke landschap voor de komende decennia vormgeven. Kort samengevat, zouden Saudi-Arabië en andere OPEC-landen hun olie exclusief voor Amerikaanse dollars verkopen, ongeacht welk land petroleum wilde kopen. Landen die olie exporteren zouden alleen de Amerikaanse valuta accepteren als betaling. Deze dollars zouden op hun beurt grotendeels gebruikt worden om Amerikaanse staatsobligaties te kopen en zo de Amerikaanse uitgaven te financieren. In ruil hiervoor zou het Amerikaanse leger hulp en uitrustingen verstrekken om de Saoedische olievelden te beschermen en de veiligheid van de koninklijke familie te waarborgen.[256]

Deze deal bezorgde de Verenigde Staten een aanhoudende vraag naar hun dollars: iedereen die olie wilde kopen van OPEC-landen, die samen meer dan twee derde van de wereldreserves controleerden,[257] moest eerst Amerikaanse dollars verkrijgen. Gezien het centrale belang van olie in de wereldeconomie, garandeerde dit dat de dollar in feite de wereldreservevaluta bleef. Deze onofficiële overeenkomst zou bekend komen te staan als het petrodollarsysteem (kort nadat deze regeling was ingevoerd, op 30 december 1974, werd het privébezit van goud opnieuw gelegaliseerd in de Verenigde Staten).

Het petrodollarsysteem was een geweldige overeenkomst voor de Amerikanen

256 Andrea Wong, *The Untold Story Behind Saudi Arabia's 41-Year U.S. Debt Secret*, *Bloomberg*, 31 mei 2016, online

257 Energy Exploration & Exploitation, *World Oil Reserves 1948–2001: Annual Statistics and Analysis*, *Energy Exploration & Exploitation*, vol. 19, no. 2 & 3, online

- maar niet zo geweldig voor het merendeel van de rest van de wereld. Om dollars te verkrijgen om olie te kunnen kopen, moesten de meeste landen goederen of diensten naar de VS exporteren, of dollars kopen op de buitenlandse valutamarkten … terwijl de VS simpelweg dollars konden drukken, zonder zich zorgen te maken over een gouddekkingverhouding. Als en wanneer ze dat deden, betaalden andere landen echt de prijs, omdat de waarde van hun dollarreserves daalde.

Het petrodollarsysteem implementeerde in feite het Cantillon-effect op wereldwijde schaal, met de Amerikaanse regering en Amerikaanse financiële instellingen in het hart van dit monetaire paradigma.[258]

De Hayekiaanse heropleving

Intussen had stagflatie de economische wereld tot wanorde gebracht, aangezien de Keynesiaanse assumptie dat inflatie werkloosheid zou tegengaan, onjuist bleek. Als het gebruik van inflatie om de economie te stimuleren verslavend was, zoals Hayek had betoogd, waren de positieve effecten van deze drug nu uitgewerkt en ondervond de samenleving de pijnlijke ontwenningsverschijnselen. Na een bestuur van veertig jaar bevond het Keynesianisme zich in een existentiële crisis.

Het was in deze context dat Hayeks ideeën werden herontdekt om de basis te vormen voor een heropleving van klassieke economische ideeën.

Deze *neoliberale* herleving begon in het Verenigd Koninkrijk, waar Margaret Thatcher in 1975 de leiding nam over de Conservatieve Partij. Nadat ze als student *The Road to Serfdom* had gelezen, werd ze een aanhanger van het werk van Hayek en een sterke voorstander van vrije markten en een kleine overheid. Thatcher verwierp de gewoonte van de Conservatieve Partij om een compromis te sluiten over deze idealen om de centristische stem te winnen, en koos in plaats daarvan voor de harde aanpak. Op een gegeven moment, tijdens een vergadering met de onderzoeksafdeling van haar partij, haalde ze op beroemde wijze zelfs Hayeks boek *The Constitution of Liberty* uit haar tas en sloeg het neer op tafel. 'Dit is waar we in geloven!' verklaarde ze.[259]

---

258 Alex Gladstein, *Uncovering The Hidden Costs of the Petrodollar*, *Bitcoin Magazine*, 28 april 2021, online

259 Wapshott, Keynes Hayek, 258–59.

Het plan had succes. De Iron Lady, zoals Thatcher vaak werd genoemd, werd in 1979 verkozen tot de eerste vrouwelijke premier van het Verenigd Koninkrijk. Eenmaal in functie voerde ze haar plannen uit om de omvang van de overheid te beperken en de vrije markt meer ruimte te geven. Ze deed dit door belastingen te verlagen, regulerende obstakels weg te nemen en een nationale golf van privatisering door staatsbedrijven te verkopen. Dit beleid leverde haar in de daaropvolgende jaren meerdere herverkiezingen op. Uiteindelijk werd Thatcher hierdoor de langstzittende Britse premier van de twintigste eeuw.

Het succes van Thatcher in het VK diende als inspiratie voor een geestverwant in de Verenigde Staten. De Republikeinse kandidaat voor de presidentsverkiezingen van 1980, Ronald Reagan, beloofde eveneens een vermindering van de overheidsuitgaven. Zijn campagneslogan, 'We kunnen de overheid van onze ruggen halen, uit onze zakken', sloeg aan bij de Amerikaanse kiezers. De voormalige filmster versloeg de zittende president Jimmy Carter met een grandioze overwinning.

Als president verlaagde Reagan inderdaad de belastingen en zette hij de sociale programma's stop. Om zijn economische beleid verder te ontwikkelen, dat later bekend kwam te staan als *Reaganomics*, creëerde de president een nieuwe adviesraad voor economisch beleid. Hierin benoemde hij economen die een sterke voorkeur hadden voor de vrije markt, waaronder opmerkelijk Milton Friedman, een vroege bewonderaar van Hayek.[260]

Decennia eerder, in 1947, nodigde Hayek Friedman, die net was begonnen als economieprofessor aan de Universiteit van Chicago, uit voor een tiendaagse conferentie in Zwitserland. Ongeveer 60 toonaangevende voorstanders van de vrije markt, bekende libertaire denkers en andere invloedrijke vrijdenkende personen, hadden hier tien dagen besteed aan het bespreken hoe een vrije samenleving kan worden behouden en hoe te voorkomen dat het Westen zou terugvallen naar fascisme of afglijden naar socialisme. Voor Hayek vertegenwoordigde de topbijeenkomst (die een jaarlijks terugkerend evenement zou worden) 'de wedergeboorte van een liberale beweging in Europa'.[261]

Friedman had zich in de decennia na die reis naar Zwitserland weten te

260 Wapshott, Keynes Hayek, 261.

261 Wapshott, Keynes Hayek, 211–214.

vestigen als een van de meest invloedrijke economen van de twintigste eeuw. Net als Hayek verwierp Friedman de destijds dominante Keynesiaanse doctrine van staatsinterventie en overheidsuitgaven. Naarmate hij beroemder werd, werd hij in veel opzichten een meer effectief voorvechter van Hayeks ideeën over markten en het prijssysteem dan Hayek zelf ooit was geweest.

Echter, op bepaalde punten zouden Friedmans gedachten ook afwijken van de inzichten van Hayek. Zijn bijdragen op het gebied van economie hielpen bij het vormgeven van een aparte denkrichting die bekend staat als de *Chicago School of Economics*.

De Chicago School verschilt op een aantal belangrijke punten van de Oostenrijkse School.

Een fundamenteel verschil was de methodologie van de Chicago School. Waar Carl Menger de basis had gelegd voor de Oostenrijkse school van economie in praxeologie, de methode gebaseerd op logica, redenering en basisprincipes, koos de Chicago School voor een meer traditioneel empirisme, waarin hypotheses worden geformuleerd en getoetst aan de hand van reële wereldgegevens en statistieken.

Het tweede grote verschil was bijna net zo fundamenteel als het eerste: de Chicago School was het niet eens met de Oostenrijkers over het onderwerp geld.

Monetarisme

Hoewel Friedman een grote voorvechter was van Hayeks ideeën over markt en prijzen, omvatte dit niet Hayeks perspectief op de stadia van productie, of hoe rentetarieven en het intertemporele prijssysteem de toewijzing van middelen door de tijd heen konden sturen. Friedman was zeker geen voorstander van Hayeks voorstel om geld te denationaliseren. In plaats daarvan pleitte Friedman voor strikte overheidsregulatie van geld.

Friedman heeft, samen met econome Anna Schwartz, een onderzoek uitgevoerd naar economische hoogte- en dieptepunten in de Verenigde Staten.[262] Hun studie bestreek de periode vanaf het midden van de negentiende eeuw tot het midden van de twintigste eeuw, met extra aandacht voor de Grote Depressie

262 Milton Friedman and Anna Schwartz, A Monetary History of the United States.

van de jaren 1930. Friedman en Schwartz kwamen tot de conclusie dat elke economische recessie voorafging aan een afname van de geldvoorraad, of op z'n minst een vertraging in haar groei.

Volgens economen, inclusief Hayek, kan de geldvoorraad het duidelijkst stijgen en dalen door het wijdverspreide gebruik van fractioneel bankieren. Telkens wanneer iemand bij een fractionele reservebank een lening afsluit, brengt de bank nieuw geld in omloop (als krediet), wat de geldvoorraad vergroot. En vice versa: elke keer dat iemand een lening terugbetaalt bij een fractionele reservebank, wordt er geld uit de omloop genomen, waardoor de geldvoorraad afneemt.

Friedman en Schwartz legden uit dat toen de Federal Reserve de rentetarieven in 1928 had verhoogd, de bereidheid van mensen om leningen af te sluiten vanzelfsprekend verminderde. Maar naarmate oude leningen werden afbetaald en geld daardoor uit de omloop werd gehaald, terwijl er niet zoveel nieuwe leningen werden uitgegeven om dit te compenseren, nam de totale geldvoorraad af. Dit zette, zoals Hayek ook had uitgelegd, een deflatoire schuldenspiraal in gang.

Maar Friedman nam Hayeks uitleg van hoe rentemanipulatie deze deflatoire schuldenspiraal had ingeleid niet over, en hij was vooral het niet eens met Hayeks voorstel om deze schuldenspiraal zijn gang te laten gaan. In plaats daarvan stelde hij een oplossing voor die veel meer leek op wat Irving Fisher en de stabilisatoren in de jaren 1920 hadden voorgesteld (maar waarvan hij geloofde dat het niet goed was uitgevoerd in de jaren 1930).

De econoom van de Chicago School redeneerde dat de geldvoorraad op een gestage en voorspelbare manier zou moeten groeien, zodat de economie meegroeit en het geaggregeerde prijsniveau stabiel kan blijven of misschien heel langzaam kan stijgen. Zolang de prijzen stabiel werden gehouden, kon de markt voor de rest zorgen. *Monetarisme*, zoals deze monetaire doctrine werd genoemd, werd een fundamenteel onderdeel van de Chicago School van Economie.

De voorgestelde hulpmiddelen om de geldvoorraad te beheren waren dezelfde als die van Fischer: de consumentenprijsindex zou fungeren als de maatstaf voor stabiliteit en rentetarieven konden worden gereguleerd om de geldvoorraad te verhogen of te verlagen. Als de prijzen zouden dalen, wilden monetaristen dat centrale banken de rentetarieven zouden verlagen om zo de kredietverlening aan te wakkeren, uitgaven te stimuleren, en opwaartse druk op de prijzen te zetten. Als de prijzen te snel zouden stijgen, wilden monetaristen dat centrale banken de

rentetarieven zouden verhogen. Als de prijzen stabiel bleven, zou de hoeveelheid geld in de economie gestaag groeien samen met de economie zelf, en was de rente precies goed ingesteld.

Monetaristen waren het grotendeels oneens met Keynesianen over de rol van de overheid. Zij waren niet van mening dat regeringen lage rentetarieven zouden moeten gebruiken om de uitgaven te verhogen, maar in plaats daarvan geloofden zij dat overheidsuitgaven uitsluitend gefinancierd zouden moeten worden door middel van fiscaal beleid, met andere woorden, belastingen. Hoewel monetaristen het erover eens waren dat geaggregeerde uitgaven essentieel waren om een economische neergang te vermijden, beweerden zij dat de particuliere sector de uitgaven even goed kon doen, en in feite de uitgaven zou doen als mensen goedkoop genoeg geld konden lenen. Op een bepaalde manier combineerden monetaristen ideeën van zowel Oostenrijkers als Keynesianen in een nieuwe benadering.

De theorie overtuigde Hayek echter niet, om veel van dezelfde redenen dat de stabilisatoren hem voorheen nooit overtuigd hadden: hij geloofde dat het manipuleren van rentetarieven de spontane orde door de tijd heen verstoorde, en geloofde niet in het monetaristische idee van stabiliteit (eerder in zijn carrière had hij aangehaald dat stabiele prijzen eigenlijk niet stabiel zijn, aangezien deflatie juist de natuurlijke staat is van een gezonde economie, terwijl hij later in zijn carrière toevoegde dat de vrije markt, en niet een centraal geleid overheidscomité, zou moeten bepalen wat stabiel is).

Hoewel Hayeks ideeën over markten en het prijssysteem in de jaren tachtig een heropleving genoten, bleven zijn ideeën over geld grotendeels onopgemerkt. Geld bleef onder staatscontrole en zelfs de nieuwe stroom vrijemarkteconomen in Chicago geloofde niet dat hier verandering in moest komen.

Spaargeld en leningen

In 1987 benoemde president Reagan een ander lid van zijn Economische Beleidsadviesraad tot de nieuwe voorzitter van de Federal Reserve, met name Alan Greenspan. Net zoals Friedman was ook Greenspan een fervent monetarist. Toen de Amerikaanse Senaat kort daarna de nominatie bevestigde, stond de monetaire

theorie van de Chicago School op het punt om voor het eerst in de praktijk te worden gebracht.

Nauwelijks in zijn nieuwe functie benoemd, werd Greenspan vrijwel meteen geconfronteerd met de ergste bankencrisis sinds 1929. In een economie met zowel hoge inflatie als hoge rentetarieven om de inflatie te dempen, hadden de spaarbanken het moeilijk. Veel van deze samenwerkende bankachtige financiële instellingen, die langlopende leningen zoals hypotheken verstrekten met een vaste rente, hadden nu moeite om voldoende geld aan te trekken om aan alle opnameverzoeken van spaarders te voldoen. Uiteindelijk dwong dit veel spaar- en leenverenigingen om in gebreke te blijven en faillissement aan te vragen.

Toen de bezorgdheid bij economen en beleidsmakers toenam dat deze faillissementen een domino-effect op de Amerikaanse economie konden hebben, verlaagde Greenspan in 1989 de rentetarieven. Hierdoor werd het goedkoper voor de spaar- en leenverenigingen om geld te verkrijgen, terwijl tegelijkertijd de eerste tekenen van een economische neergang werden tegengegaan en beheerst.

Desondanks moest de *Federal Savings and Loan Insurance Corporation* (FSLIC) uiteindelijk ingrijpen om de mislopende sector te redden, waarbij spaarders in totaal 125 miljard dollar werd terugbetaald. De FSLIC, alsook de *Federal Deposit Insurance Corporation* (FDIC), waren tijdens de crisis van de jaren 1930 (Great Depression) in het leven geroepen om het vertrouwen van het volk in de banken te herstellen: deze overheidsinstellingen garandeerden dat bankklanten hun deposito's (tot een zekere limiet) terugbetaald kregen in geval van een bankfaillissement. Aangezien de Federal Reserve in haar rol als kredietverstrekker in uiterste nood tijdens de economische crisis van de jaren 1930 had gefaald, gaf het deposanten een tweede reden om zich geen zorgen te maken over fractioneel reservebankieren.

Het klopt dat de reddingsacties de omvang van de spaar- en leencrisis beperkten en veel persoonlijke drama's voorkwamen. Maar dit ging gepaard met aanzienlijke kosten: de 125 miljard dollar moest worden betaald door de overheid, dus in werkelijkheid door de Amerikaanse belastingbetaler. Zelfs de Amerikanen die zorgvuldig en voorzichtig waren met hun spaargeld, moesten indirect een deel van de last dragen, terwijl de spaar- en leningverenigingen en hun klanten er relatief makkelijk vanaf kwamen.

Aan het begin van zijn carrière had Hayek al zijn zorgen uitgesproken over het morele risico dat centrale banken in de economie introduceerden. Dit werd met

de FDIC en FSLIC alleen maar explicieter. Tijdens de spaar- en leencrisis werd het duidelijk dat financiële instellingen grote risico's konden nemen; de Amerikaanse overheid zou de rekening betalen als het fout liep.

Dot-Com

Ongeveer tien jaar na de crisis van de spaar- en leenverenigingen, tegen het einde van de jaren 1990, deden de aandeelmarkten het enorm goed.

Dit kwam deels door een algemeen gevoel van optimisme in de westerse wereld: eerder in dat decennium was de Sovjet-Unie eindelijk ingestort. Hoewel Ludwig von Mises al in 1973 overleden was, leek zijn economische rekenprobleem eindelijk bevestigd te zijn. Nu de dwaasheid van centrale planning eindelijk bevestigd leek, omarmden voormalige Sovjetlanden de vrijemarkteconomie.

Bovenop dit alles werden de Verenigde Staten overmand door een enorme tech-euforie, wat het duidelijkst weerspiegeld werd op de Nasdaq -aandelenbeurs. Door bedrijven uit Silicon Valley, zoals Netscape, die openbaar werden met waarderingen van meerdere miljarden dollars, schoten technologieaandelen over de hele linie omhoog. Zelfs internetstart-ups, die vaak niet meer dan een domeinnaam hadden, werden in sommige gevallen gewaardeerd op tientallen, of zelfs honderden, miljoenen dollars. Het internet was de toekomst en iedereen wilde er een stuk van hebben.

Maar studenten van Hayeks werk hadden reden om te denken dat er ook iets anders aan de hand was. De Federal Reserve onder Greenspan had namelijk in de nasleep van de spaar- en leencrisis de rentetarieven verlaagd naar de laagste niveaus sinds de jaren 1960. Net zoals in de jaren 1920, was geld goedkoop en mensen waren maar al te blij om te lenen en te investeren in de aandelenmarkt. Kunstmatig lage rentetarieven waren de drijvende kracht achter de economische boom.

En, deze leerlingen van Hayek zouden weten dat de economische realiteit vroeg of laat een inhaalslag ging maken. En dat deed ze uiteindelijk. Net voor de eeuwwisseling, besloot Greenspan om de rentetarieven te verhogen, en plofte de dot-com-bubbel, en de Nasdaq stortte naar beneden. De razernij was voorbij.

Als Hayek nog in leven was geweest, dan had hij waarschijnlijk betoogd dat

de beste weg voorwaarts zou zijn om op de tanden te bijten en de markt te laten normaliseren. De economie zou door een pijnlijke recessie moeten gaan naarmate onrendabele bedrijven zouden sneuvelen, en middelen langzaam maar zeker herverdeeld konden worden naar meer duurzame inspanningen.

Maar Greenspan had een ander idee. De monetarist was vastbesloten een deflatoire schuldenspiraal te voorkomen, dus besloot hij opnieuw de rente te verlagen. Deze keer liet hij ze ver onder het niveau van de jaren 1990 zakken, waardoor krediet in de vroege jaren 2000 zelfs goedkoper was dan het tijdens de opmars van de dot-com-bubbel was.

Op het eerste zicht leek het te werken. In de daaropvolgende jaren begon de aandelenmarkt langzaam te herstellen. Voor veel economische commentatoren diende dit als een bevestiging dat het monetarisme naar behoren had gewerkt. Greenspan had de Amerikaanse economie met minimale schade door de dot-com-crash geloodst, wat hem zelfs een nieuwe bijnaam opleverde: *de Maestro*.

Eén sector in het bijzonder beleefde in het midden van de jaren 2000 niets minder dan een volledige economische opleving: de huizenmarkt.

Te groot om te falen

Deze bloei in de huizenmarkt baarde Greenspan, met het oog op monetaire stabiliteit, nauwelijks zorgen. Hoewel sommige afgeleide prijzen, zoals de kosten van woninghuur en onderhoud, in acht werden genomen, waren de werkelijke huizenprijzen zelf niet opgenomen in de CPI (Consumentenprijsindex); ze waren in 1983 uit de index gehaald. Vastgoed wordt sindsdien grotendeels beschouwd als een vorm van investering, hetgeen bijzonder handig was omdat politici in die tijd de inflatiecijfers wilden verlagen.[263]

Desalniettemin kon de bloei in grote mate worden toegeschreven aan het beleid van Greenspan. Lage rentetarieven hadden in het begin van de jaren 2000 de hypotheekrente naar ongekende dieptepunten gestuurd, en de Amerikaanse woningmarkt floreerde als direct gevolg hiervan. De prijs van een nieuw huis steeg jaar na jaar, aangezien iedereen leek te willen profiteren van de kans om

263 The Economist, *Why don't rising house prices count towards inflation? The Economist*, 29 juli 2021, online

goedkoop in te stappen.

En er was nog een andere, verborgen reden voor deze bloei. Financiële instellingen hadden, voornamelijk sinds de late jaren 1980, complexe soorten van hypotheekgedekte effecten gebruikt, namelijk gedekte schuldobligaties. Dit stelde hen in staat om hypotheekschulden in stukken te hakken en door te verkopen; in plaats van de bank die het uitgaf, waren de hypotheekschulden steeds meer eigendom van investeerders, waardoor ook andere financiële instellingen zoals banken, verzekeringsmaatschappijen en pensioenfondsen betrokken raakten.

Het probleem was echter dat elke hypotheekschuld kon worden voorgesteld als een praktisch risicovrij activum. Daarom waren sommige financiële instellingen die hypotheken verstrekten maar al te graag bereid nieuwe hypotheken te verstrekken aan vrijwel iedereen die er een aanvroeg. Controles op inkomen, baanzekerheid of kredietwaardigheid werden grotendeels over het hoofd gezien. De risico's die inherent waren aan deze hypotheken werden verhuld om ze opnieuw te kunnen verkopen.

Maar de risico's konden niet eeuwig verborgen blijven. Midden jaren 2000 begon Alan Greenspan, de toenmalige voorzitter van de Federal Reserve, de rente weer te verhogen, en zijn opvolger in 2006, Ben Bernanke, volgde zijn voorbeeld. Nogmaals voor degenen die het werk van Hayek hadden bestudeerd: wat er vervolgens gebeurde kwam niet als een verrassing.

Toen het duurder werd om te lenen, begon de huizenmarkt op te drogen, terwijl tegelijkertijd steeds meer Amerikanen in gebreke bleven bij de hypotheken die hen zo vrij waren verstrekt. Toen de huizenprijzen in de Verenigde Staten begonnen te dalen, ontdekten degenen die hadden geïnvesteerd in hypotheekgebonden effecten dat ze lang niet zo veilig waren als geadverteerd, waardoor sommigen van hen in geldnood kwamen om hun eigen schulden af te betalen.

Toen wanbetalingen (leningen die niet kunnen worden terugbetaald) zich als een epidemie doorheen de Amerikaanse financiële sector begonnen te verspreiden, en steeds grotere bedrijven beïnvloedden, werd de omvang van de crisis steeds duidelijker. Toen de financiële reus Lehman Brothers in september 2008 het grootste bedrijf werd dat ooit faillissement indiende in de geschiedenis van de Verenigde Staten, wisten financiële professionals, beleidsmakers en iedereen die oplette dat verdere escalatie tot een volledige economische neerval kon leiden.

Toen het erop leek dat de grote verzekeringsmaatschappij AIG wellicht de

volgende zou zijn om te bezwijken, heeft de Federal Reserve, ondersteund door een nieuwe noodwet, een werkelijk opmerkelijke stap genomen. De centrale bank verklaarde de verzekeraar *te groot om te falen*, en samen met de Amerikaanse schatkist redde ze AIG door middel van een injectie van $ 68 miljard (plus nog eens $ 112 miljard aan garanties).

Dit luidde een nieuw beleidstijdperk in, zowel in de VS als daarbuiten, omdat de crisis internationaal om zich heen greep. In de daaropvolgende weken coördineerde de Federal Reserve nogmaals met het Amerikaanse Ministerie van Financiën om voor $ 405 miljard aan noodlijdende activa te laten kopen, terwijl aan de andere kant van de Atlantische Oceaan de Britse minister van Financiën, Alistair Darling, ook een noodmaatregel uitrolde in de vorm van een bankreddingsplan ter waarde van £ 137 miljard ($ 230 miljard). Vergelijkbare maatregelen werden in andere Europese landen genomen.[264]

Een onmiddellijke financiële instorting werd afgewend, maar alleen omdat grote delen van de financiële sector werden gered door openbare instellingen en de creatie van enorme hoeveelheden nieuw geld uit het niets; het morele risico stond nu volop in de schijnwerpers.

Een nieuwe wereld

De overheidsinterventies zouden zich niet alleen tot reddingsoperaties beperken. Midden in een crisis had de Federal Reserve opnieuw de rente verlaagd met als doel deflatie te vermijden en de economie weer op de rails te krijgen, deze keer tot bijna nul procent: geld lenen werd bijna gratis. Maar het leek weinig effect te hebben.

In november 2008 kondigde de Federal Reserve daarom een grootschalig programma aan ter aankoop van activa, genaamd *Quantitative Easing* (kwantitatieve versoepeling). De Fed zou nog eens voor $ 600 miljard aan hypotheekgedekte effecten opkopen met vers gecreëerde dollars, en breidde dit kort daarna uit naar het opkopen van bank- en overheidsschuld. De centrale bank kreeg al snel voor meer dan $ 2000 miljard van deze drie activa in handen, waardoor de totale

264 US Department of the Treasury, *Troubled Asset Relief Program*, online; Federico Mor, *Bank Rescues of 2007-09: Outcomes and Cost, House of Commons Research Briefing*, 8 oktober 2018, online

waarde van haar balans bijna verdrievoudigde.

Quantitative Easing (QE) stelt centrale banken in staat risicovolle activa van de markt te halen, maar het hoofddoel van deze programma's is om het geldaanbod te vergroten en deflatie tegen te gaan wanneer traditionele instrumenten de klus niet klaren. Met andere woorden, QE kan helpen om inflatie te stimuleren wanneer de rentetarieven tot nul (of bijna nul) zijn gedaald, door wanhopig duizenden miljarden rechtstreeks in de economie te pompen; een voorbeeld dat al snel door andere centrale banken over de hele wereld werd gevolgd.

En het *was* wanhopig. Volgens de toonaangevende theorie van Bernanke over geld en rente, zou QE zelfs helemaal geen inflatie moeten stimuleren als een rentetarief van nul procent dat al niet deed. Toch bleek het enigszins te werken. Zoals de voorzitter van de Fed grappend zei: 'Het probleem met QE is dat het in de praktijk goed werkt, maar niet in theorie.'[265]

Toch betraden de centrale banken met de invoering van QE bijna volledig onbekend terrein. Niemand die leidinggaf aan deze opkoopprogramma's wist precies wat de effecten zouden zijn, of hoe lang het zou duren voordat dergelijke effecten zichtbaar werden. Sterker nog, de financiële crisis van 2008 en de nasleep daarvan markeerden het begin van een nieuwe en onzekere wereld van geld en financiën.

Oorspronkelijk opgericht als een kredietverstrekker in uiterste nood, ongeveer een eeuw geleden, was de Federal Reserve al bijna even lang de rentevoeten aan het manipuleren. Nu begon het ook winnaars en verliezers in de markt te kiezen met reddingspakketten en begon het zelfs middelen toe te wijzen via de vermogensmarkten door middel van QE. Het mandaat van de centrale bank was na verloop van tijd uitgebreid om taken te omvatten die even goed de verantwoordelijkheden zouden kunnen beschrijven die doorgaans aan centrale planners van de Sovjet-Unie werden toegeschreven.

Ondertussen bood de crisis — net als de crisis van de jaren 1930 — een klimaat waarin Keynesiaanse ideeën een heropleving konden maken: een groep econo-

265 Rupal Patel and Jack Meaning, *Can't We Just Print More Money? Economics in Ten Simple Questions*, The Bank of England, 238.

men, bekend als de *Neo-Keynesianen*[266], drongen er bij overheden wereldwijd op aan om het begrotingstekort te verhogen om zo nationale economieën te stimuleren. Toen IMF-directeur Dominique Strauss-Kahn in 2008 deze 'Keynesiaanse heropleving' aanbeveelde, stemden wereldleiders, onder wie de Amerikaanse president George W. Bush en de Britse premier Gordon Brown, in met het steunen van de plannen. Financiële stimuleringspakketten werden al snel over de hele wereld uitgerold.

Het grootste deel van Hayeks leven waren zijn ideeën gemarginaliseerd. Hayek had al in de jaren 1920 kritiek geuit op de rol van centrale banken, en sinds de jaren 1930 waarschuwde hij dat Keynesiaanse maatregelen weinig deden buiten het verlengen van onhoudbare economische oplevingen. Toch leken de zaken in de loop van de tijd alleen maar erger te worden. Geld was geëvolueerd tot een geopolitiek schaakstuk voor nationalisten, een machtsmiddel voor economische planners van centrale banken en vooral, een bron van economische onrust — dat op zijn beurt de heropleving van de Keynesiaanse doctrine bevorderde.

Het monetaire systeem was in de vroege eenentwintigste eeuw zo ver verwijderd van Hayeks ideaal als maar mogelijk kon zijn, en er was geen oplossing in zicht.

Tenzij je toevallig geabonneerd was op een technologiemailinglijst in een bijna vergeten hoekje van het internet…

266 De Neo-Keynesianen integreerden meer van de neoklassieke ideeën over vrije markten, maar namen ook meer mogelijke marktfalen aan, met name door het onvermogen van sommige prijzen om zich snel aan te passen aan nieuwe omstandigheden, wat overheidsingrijpen rechtvaardigt. Dit geldt vooral voor de arbeidsprijs, vanwege psychologische factoren.

Hoofdstuk 15

Het ontwerp

De financiële markten waren al in rep en roer toen Adam Back in de zomer van 2008 een e-mail ontving van iemand die zichzelf *Satoshi Nakamoto* noemde. Nakamoto legde uit dat hij een digitaal geldsysteem had ontworpen dat gebaseerd was op het proof-of-work-systeem dat Back meer dan tien jaar eerder had geïntroduceerd via hashcash. De e-mail bevatte een link naar een conceptversie van een ontwerptekst (de zogenaamde *whitepaper*), getiteld 'Bitcoin: Een Peer-to-Peer Elektronisch Geldsysteem.' Nakamoto was geïnteresseerd in feedback.

Back had nog nooit van de naam Satoshi Nakamoto gehoord, en, als betrokken lid van de Cypherpunkbeweging sinds midden jaren 1990, had hij al te veel mislukte pogingen gezien om digitale valuta te creëren om hoge verwachtingen te hebben van het nieuwe voorstel in zijn inbox. Toch had Nakamoto genoeg interesse bij de Britse Cypherpunk gewekt om het document te lezen, en hij merkte enkele overeenkomsten met het b-money-voorstel van Wei Dai op. Back wees Nakamoto hierop in zijn antwoord, maar liet het daar bij.

Ook Wei Dai kreeg al snel bericht van Satoshi Nakamoto. 'Ik had veel interesse om jouw b-money pagina te lezen', stond er in de e-mail van Nakamoto. 'Ik sta op het punt om een paper te publiceren dat jouw ideeën uitbreidt tot een volledig functioneel systeem.'[267]

Nakamoto vroeg vervolgens wanneer het ontwerp van b-money voor het eerst

267 Satoshi Nakamoto and Wei Dai, *Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails*, *gwern.net*, laatste update op 14 september 2017, online

werd gepubliceerd: hij wilde naar Dais voorstel voor elektronisch geld verwijzen in de definitieve versie van zijn witboek. Deze e-mail bevatte ook weer een link naar het concept.

Dai— die net als Back, Satoshi Nakamoto niet kende — reageerde met links naar een webarchief met de originele b-money e-mail en de relevante discussies op de Cypherpunks-mailinglijst van tien jaar eerder. 'Bedankt dat je me over je paper hebt verteld', voegde Dai toe. 'Ik zal het eens bekijken en je laten weten of ik opmerkingen of vragen heb.'[268]

Dai gaf geen vervolg aan hun correspondentie. Tegen die tijd had hij de hoop opgegeven dat digitale geldsystemen, geïnspireerd door de Cypherpunkbeweging, genoeg gebruikers konden aantrekken om een zinvol verschil in de wereld te maken. Hij schonk nauwelijks aandacht aan Nakamoto zijn ontwerp. In plaats daarvan koos hij ervoor om zijn tijd te besteden aan beslissingstheorie en andere benaderingen van AI-veiligheid (de oorspronkelijke reden waarom hij geïnteresseerd raakte in cryptografie).

Ondertussen leek Nakamoto de informatie te hebben vergaard die hij nodig had. Terwijl de financiële crisis van 2008 in de daaropvolgende weken en maanden volledig tot uiting kwam, werd er niets meer gehoord van Nakamoto.

Tot en met 31 oktober. Alle abonnees van de Cryptography-mailinglijst ontvingen op dit moment een e-mail van Satoshi Nakamoto. Doordat deze lijst fungeerde als de feitelijke opvolger van de Cypherpunks-lijst, werden veel van de originele Cypherpunks nu voorgesteld aan het nieuwe voorstel voor een digitale valuta. 'Bitcoin P2P e-cash paper', luidde het onderwerp.[269]

Inderdaad, het elektronische geldproject van Nakamoto had nu een naam: *Bitcoin*.

'Ik heb mij toegelegd om een nieuw elektronisch geldsysteem te creëren dat volledig van persoon tot persoon functioneert en geen vertrouwde derde partij vereist', luidde Nakamotos e-mail, alvorens de hoofdeigenschappen samen te vatten:

- Dubbele uitgaven worden voorkomen met een peer-to-peer netwerk.

268 Nakamoto and Dai, *Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails.*

269 Satoshi Nakamoto, *Bitcoin P2P e-cash paper.* oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. 31 oktober 2008. online

- Geen mint of andere vertrouwde partijen.
- Deelnemers kunnen anoniem zijn.
- Nieuwe munten worden gemaakt op basis van proof-of-work in de stijl van Hashcash.
- Het proof-of-work voor het genereren van nieuwe munten geeft het netwerk ook de energie om dubbele uitgaven te voorkomen.

Bijgevoegd was een link naar de actuele versie van het witboek.[270] *Bitcoin: Een Peer-to-Peer Elektronisch Geldsysteem*, luidde nu de titel. In amper negen pagina's (inclusief een bladzijde voor externe referenties), schetste Nakamoto de kernmechanismen van zijn digitale valuta. Het maakte een compacte, maar zeer efficiënte beschrijving van — zoals de inleiding van het paper omschreef — 'een elektronisch betalingssysteem gebaseerd op cryptografisch bewijs in plaats van vertrouwen.'

Blockchain

Het systeem dat Satoshi Nakamoto in zijn ontwerptekst beschreef leek daadwerkelijk op b-money — dat nu als eerste van acht verwijzingen wordt genoemd — op meerdere manieren.

Net als in Wei Dais ontwerp voor elektronisch geld zouden de munteenheden van Bitcoin (ook wel *bitcoin* genoemd, maar meestal geschreven met een kleine letter b) niet worden gedekt, terwijl eigendom van bitcoin zou worden toegeschreven aan publieke sleutels. Transacties zouden in essentie cryptografisch ondertekende berichten zijn die aangeven dat de aan deze publieke sleutels toegeschreven munten overgedragen worden aan andere publieke sleutels. Het eigendom van Bitcoin zou dan cryptografisch gegarandeerd zijn; bitcoin zou alleen kunnen worden verplaatst met geldige handtekeningen.

Dit heeft als doel de privacy van de gebruikers te beschermen, hoewel Nakamoto in zijn witboek toegeeft dat dit niet helemaal perfect zou zijn.

'Sommige connecties zijn nog steeds onvermijdelijk met *multi-input* transacties, aangezien deze noodzakelijkerwijs onthullen dat de inputs toebehoorden

270 Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, online

aan dezelfde eigenaar', schreef hij. 'Het risico bestaat als de eigenaar van een sleutel wordt onthuld, dat connecties andere transacties kunnen onthullen die toebehoren aan dezelfde eigenaar.'

Maar misschien nog wel het interessantste is dat Nakamoto Bitcoin heeft ontworpen volgens de meest ambitieuze variant van b-money, waarbij alle gebruikers een grootboek bijhouden om het eigendom van de valuta binnen het systeem te volgen. Elke node (elke deelnemer op het netwerk) zou alle nieuwe transacties zien, hun geldigheid controleren en hun grootboeken dienovereenkomstig bijwerken — terwijl ongeldige transacties (waaronder dubbele uitgaven) zouden worden afgewezen.

Tien jaar eerder had Dai de conclusie getrokken dat zo'n gedistribueerde aanpak niet praktisch was. Zonder een synchrone en onverstoorbare anonimiteit van het uitzendkanaal, konden verschillende delen van het netwerk verschillende transacties als eerste waarnemen. Hierdoor zouden transacties die dubbel worden uitgegeven, in principe het netwerk opsplitsen, waar verschillende nodes conflicterende basisregisters bijhouden. Met potentieel oneerlijke deelnemers die uit zijn op het zaaien van verdeeldheid, en zonder een leider die beslist welke versie van het grootboek de daadwerkelijke toestand van het netwerk vertegenwoordigt, zag Dai geen manier om dergelijke splitsingen op te lossen. Het was in feite een perfect voorbeeld van het Byzantijnse Generaalsprobleem, en Satoshi Nakamoto geloofde dat hij dit probleem had opgelost.

Bij het ontwerpen van dit systeem, leek het erop dat Nakamoto inspiratie had geput uit het werk van Scott Stornetta en Stuart Haber: drie van de volgende vier referenties in het witboek wezen naar de vertrouwenloze tijdstempelpapers van Stornetta en Haber (inclusief degene die ze samen schreven met Dave Bayer), terwijl de vierde refereerde naar een voorstel voor tijdstempels door Belgische onderzoekers die sterk leunden op het werk van Stornetta en Haber. In een aparte referentie, gaf Nakamoto ook erkenning aan de fundamentele paper van Ralph Merkle die Merkle-bomen voor het eerst beschreef.

Het paste als gegoten. Wei Dais idee om het grootboek van eigendom over alle gebruikers te verdelen stond filosofisch zeer dicht bij het concept van Haber en Stornetta, waarin kopieën van het basisregister van een tijdstempelprotocol werden gedeeld. In beide gevallen zou elke deelnemer de belangrijke informatie zelf verifiëren, zodat ze zeker zouden weten dat niemand kon valsspelen. Elk

individu zou een ander eerlijk houden.

In het meest geavanceerde voorstel van Stornetta en Haber verwerkten gebruikers documenten samen in een grote Merkle-boom, zodat de Merkle-wortel opgenomen kon worden in de volgende Merkle-boom. Dit resulteerde in een wiskundig verifieerbare chronologische volgorde van Merkle-bomen en dus ook een chronologische volgorde van documenten opgenomen in de Merkle-bomen. Zolang de gebruikers van het systeem hun eigen basisregister bijhielden, konden ze altijd bewijzen dat een bepaald document was opgenomen vóór een ander document en op welk tijdstip.

Het elektronische geldsysteem van Nakamoto was op een zeer vergelijkbare manier ontworpen: de documenten van Haber en Stornettas tijdstempeloplossingen werden in Bitcoin in feite vervangen door transacties. Terwijl transacties via het peer-to-peer netwerk van Bitcoin werden verzonden, zouden gebruikers ze met enige regelmaat samenvoegen in een Merkle-boom. Een dergelijke bundel van transacties zou het grootste deel uitmaken van wat een *blok* werd genoemd. Als twee of meer conflicterende transacties in het netwerk circuleerden, kon slechts een van hen in een blok worden opgenomen, en alleen transacties die in een blok waren opgenomen zouden als bevestigd worden beschouwd.

En, net zoals in Haber en Stornettas basisregisters, zou elk nieuw Bitcoinblok ook de hash bevatten van het vorige blok, ook wel de *blok-hash* genoemd. Dit zou het onmogelijk maken om een ouder blok te wijzigen en het nog steeds wiskundig te laten passen in de ketting van alle blokken, aangezien dit noodzakelijkerwijs de hele ketting vanaf dat blok zou veranderen, iets wat alle gebruikers zouden opmerken.

Inderdaad, de inhoud van Bitcoinblokken, hun chronologische volgorde en daarmee de volgorde van alle transacties daarin, zouden in feite cryptografisch zijn verzegeld. Nakamoto noemde deze ketting van blokken in de mailinglijst: de *block chain*.

Minen

Omdat een Bitcoinblok alleen als geldig zou worden beschouwd als het geen conflicterende transacties bevat, bood de *blokketen* het begin van een oplossing

voor het probleem van dubbele uitgaven. Zelfs als verschillende gebruikers de transacties in een andere volgorde zouden zien, zouden hun eigendomsregisters nog steeds overeenkomen zolang ze alle blokken in dezelfde volgorde ontvingen. Bij een poging tot dubbele uitgave zou alleen de transactie die in een blok was opgenomen worden gebruikt om alle grootboeken bij te werken.

Toch loste dit het probleem van dubbele uitgaven niet volledig op. Als verschillende gebruikers namelijk verschillende blokken creëren (mogelijk met conflicterende transacties in deze verschillende blokken), en de verschillende blokken worden gelijktijdig naar verschillende delen van het netwerk gestuurd, zou exact hetzelfde probleem weer opduiken: het netwerk zou opsplitsen.

En aangezien elk volgend blok de hash van het voorgaande blok zou bevatten, zou dit zelfs betekenen dat verschillende delen van het netwerk uiteindelijk compleet verschillende, onverenigbare blokketens zouden creëren. Hierdoor zouden gebruikers op termijn hun eigendomsrechten op diverse manieren bijhouden en permanent buiten consensus vallen. Gebruikers van de verschillende delen van het netwerk zouden niet meer met elkaar kunnen handelen.

Nakamoto wist dat alle Bitcoingebruikers zich moesten verenigen rond dezelfde blokketen, ook al betekende dit dat sommige gebruikers af en toe de blokken moesten opgeven die ze als eerste hadden ontvangen in geval van een conflict. Maar met mogelijk onbetrouwbare deelnemers en niemand die de leiding heeft, was het bepalen op welke blokketen zich te vestigen alweer een uitstekend voorbeeld van het Byzantijnse Generaalsprobleem.

Hier komt het proof-of-work-systeem van Adam Back bij kijken, met zijn originele hashcashvoorstel dat de volgende referentie is in de Bitcoin-ontwerptekst. Proof-of-work vormde op dat moment al de basis voor verschillende digitale muntontwerpen van Cypherpunks, waaronder b-money, Bit Gold en RPOW. Maar waar deze ontwerpen gewoonlijk de proof-of-work-hashes *zelf* gebruikten als een vorm van geld, had Nakamoto, in wat een van zijn belangrijkste inzichten was, er een vernuftig nieuw gebruik voor bedacht.

Proof-of-work wordt in Bitcoin gebruikt als consensusmechanisme.

Naast een set van transacties en de hash van het voorgaande blok, zouden Bitcoinblokken een derde ingrediënt bevatten: een nonce. Dit willekeurige getal zou samen met de rest van de inhoud van een blok gehasht worden om de blokhash te genereren. De truc van het proof-of-work-systeem was dan ook dat niet

elk blok als geldig zou worden beschouwd. Alleen blokken met een blok-hash die begint met een vooraf bepaald aantal nullen zouden worden geaccepteerd door het netwerk van gebruikers.

Net zoals bij de productie van hashcash, zou de enige manier om een geldig blok te vinden, via vallen en opstaan zijn: een proces dat Satoshi Nakamoto later *mining* zou noemen. De mensen die aan het *minen* zijn (of *de miners*) zouden willekeurig veel verschillende nonces in een gewenst blok moeten proberen op te nemen, totdat één van hen een geldige blok-hash zou genereren. Een geldig blok — dat door niemand zou kunnen worden aangepast nadat het geproduceerd was, omdat dat de blok-hash ook zou veranderen — zou dan over het netwerk worden verzonden, waarbij elke gebruiker hun eigendomsregister zou bijwerken met de transacties in dit blok.

Miners zouden ondertussen hun inspanningen aanpassen om de nieuwe blok-hash op te nemen in een mogelijk volgend blok, dat op zijn beurt zijn eigen geldige blok-hash zou vereisen. Vergelijkbaar met hoe Bit Goldgebruikers (en vermoedelijk b-moneygebruikers) een cryptografische ketting van hashes zouden produceren om valuta te creëren, waarbij elke geldige hash diende als potentiële tekenreeks voor de volgende, zouden Bitcoinminers een cryptografische ketting van blok-hashes produceren.

En wat cruciaal is: de lengte van deze ketting zou als beslissende factor dienen in het geval van een conflict.

Als twee conflicterende blokken over het Bitcoinnetwerk zouden circuleren, zou elke gebruiker in eerste instantie het blok accepteren dat ze eerst ontvangen, en miners zouden de hash van dat blok opnemen in het volgende blok dat ze zouden proberen te vinden. In zekere zin zou het Bitcoinnetwerk inderdaad splitsen. Maar deze splitsing zou tijdelijk zijn. Zodra de ene kant van de splitsing sneller het volgende blok delft dan de andere kant van de splitsing, en hun versie van de blokketen langer wordt dan het alternatief, zouden Bitcoingebruikers en -miners van beide kanten van de splitsing deze langste ketting accepteren, waarbij ze de kortere ketting verlaten en daarmee de splitsing oplossen.

Om het Byzantijnse Generaalsprobleem te overwinnen, bedacht de sluwe Satoshi Nakamoto een nieuwe toepassing voor proof-of-work, door het in te zetten als een decentrale beslisser om consensus te bereiken. Omdat iedereen een proof-of-work kan uitoefenen, en omdat iedereen eenvoudig de geldigheid ervan kan

controleren zonder anderen te hoeven vertrouwen, paste dit perfect binnen het leiderloze ontwerp van Bitcoin.

'Het netwerk is robuust in zijn ongestructureerde eenvoud', concludeerde Nakamoto in zijn witboek. 'De nodes werken allemaal tegelijk met weinig coördinatie.'

Muntuitgifte

Als Bitcoingebruikers proof-of-work zouden produceren, en dus blokken minen, hadden ze een aansporing nodig. Miners zouden dus beloond worden met bitcoineenheden als ze een geldig blok vonden, legde Nakamoto uit in zijn witboek. Deze *blokbeloning* zou deels bestaan uit transactiekosten, betaald door andere gebruikers om hun transactie in een nieuw blok op te nemen. Maar het grootste deel van de blokbeloning zou aanvankelijk bestaan uit gloednieuwe munten.

Dit loste op een elegante manier twee problemen tegelijk op: ten eerste bood het een aansporing om te minen (waardoor het netwerk de staat van het grootboek kon overeenkomen), en ten tweede fungeerde het als methode om nieuwe valuta in omloop te brengen zonder een centrale uitgever. Bovendien deed het dit op een bijzonder slimme manier: hoewel proof-of-work kon worden gebruikt om nieuwe valuta te verdienen, was de hoeveelheid bitcoin die bij elk nieuw blok in omloop kwam in feite vastgelegd. Ongeacht hoeveel energie het had gekost om een geldig blok te produceren, het aantal nieuwe munten die per blok werd beloond, zou hetzelfde blijven.

Daarenboven — en dit kan wel eens een van Nakamoto's belangrijkste originele innovaties zijn, die niet gebaseerd zijn op eerdere digitale geldsystemen — zou een *aanpassingsalgoritme* voor de moeilijkheidsgraad ervoor zorgen dat nieuwe blokken op een zo gelijkmatig mogelijke snelheid zouden worden gevonden. Als er te veel blokken te snel geproduceerd zouden worden, zoals aangegeven door de tijdstempels in elk nieuw blok, zouden alle nodes op het netwerk automatisch gaan eisen dat nieuwe blokken meer proof-of-work zouden moeten bevatten (met als resultaat dat er meer rekenkracht nodig is om een geldige blok-hash te vinden, omdat nieuwe hashes meer nulwaarden aan het begin zouden vereisen). Ook als blokken te langzaam gevonden zouden worden, zouden alle nodes beginnen met

het accepteren van nieuwe blokken die minder proof-of-work bevatten (minder nulwaarden aan het begin).

Met blokken die tegen een redelijk gelijkmatig tempo worden gevonden, en elk blok een vastgesteld aantal nieuwe munten uitgeeft, zou de snelheid van muntaanmaak voorspelbaar zijn — ongeacht de hoeveelheid hashkracht die aan het netwerk wordt toegeschreven. Waar systemen zoals hashcash en RPOW te maken zouden hebben gehad met hyperinflatie, omdat de kosten om een geldige hash te produceren in de loop van de tijd bleven dalen door hardwareverbeteringen, was Bitcoin ontworpen om zich aan een vooraf geprogrammeerd uitgifteschema te houden.

Door de hoeveelheid proof-of-work te ontkoppelen van het tempo van valutacreatie, heeft Nakamoto het inflatieprobleem opgelost. Dit maakt dat de uitgifte van Bitcoin een grotere gelijkenis heeft met die van een edelmetaal.

'Het stabiel toevoegen van een vastgesteld aantal nieuwe munten is te vergelijken met gouddelvers die middelen verbruiken om goud in omloop te brengen', legt het Bitcoin- witboek uit. 'In ons geval gaat het om CPU-tijd en elektriciteit die verbruikt wordt.'

Positieve aansporing

Nakamoto was bovendien van mening dat het uitgiftemodel van Bitcoin potentiële aanvallers zou ontmoedigen. Het meest voor de hand liggende is dat oneerlijke deelnemers niet gemakkelijk dubbele uitgaven in transacties kunnen doen, aangezien slechts één van de conflicterende transacties in de blokketen kan worden opgenomen.

De enige manier om een dubbele uitgaveaanval uit te voeren, zou zijn als de aanvaller een van zijn transacties in een blok weet op te nemen en deze als betaling wordt geaccepteerd door de ontvanger, om vervolgens zelf een conflicterend blok te minen met de conflicterende transactie, en doorgaan met het minen van deze alternatieve blokketen totdat hij langer is dan de originele ketting. Als het hem inderdaad zou lukken om de langste ketting te maken (met de dubbele uitgavetransactie erin), zouden alle Bitcoingebruikers overschakelen naar deze alternatieve ketting, en iedereen zou hun grootboeken dienovereenkomstig

bijwerken. De originele transactie zou worden ingetrokken en de dubbele uitgave zou gelukt zijn.

Echter, zolang de aanvaller niet over meer rekenkracht beschikt dan de rest van het netwerk tezamen, zou de kans dat hij de eerlijke ketting inhaalt, exponentieel afnemen voor elk blok dat hij achterloopt, legt Nakamoto uit. De eerlijke ketting zou vrijwel zeker sneller groeien. Hij onderbouwde zijn uitleg met de achtste en laatste verwijzing in het witboek, en ook de oudste: het handboek *An Introduction to Probability Theory and Its Applications* uit 1957, geschreven door wiskundige William Feller.

Om een dubbele uitgave te voorkomen, zou de eenvoudigste oplossing zijn om te wachten tot er enkele blokken zijn ontgonnen boven op het blok dat een binnenkomende transactie bevat, voordat de betaling als definitief wordt beschouwd, schreef Nakamoto. Elk nieuw blok zou een extra bevestiging van de betreffende transactie vertegenwoordigen en met slechts een paar bevestigingen zou het in de meeste gevallen uiterst onwaarschijnlijk zijn dat een aanvaller deze ooit zou kunnen inhalen. En aangezien een aanvaller in middelen zou moeten investeren om rekenkracht te verkrijgen om het zelfs maar te proberen, zou een aanvalspoging meestal niet de moeite waard zijn.

Dit gezegd zijnde: het wachten op meer bevestigingen zou niet helpen als een aanvaller daadwerkelijk meer rekenkracht had dan de rest van het netwerk tezamen. In dat scenario zou de aanvaller uiteindelijk altijd kunnen inhalen en de langste ketting kunnen genereren, waarmee hij naar believen dubbel kon uitgeven.

Maar zelfs als dat het geval is, kan de aanvaller zijn aanval niet kosteloos uitvoeren; hij zou nog steeds het benodigde proof-of-work moeten leveren om geldige blokken te creëren.

Nakamoto veronderstelde dat de blokbeloningen die door het Bitcoinprotocol worden toegekend op zich al een mogelijke aanvaller zouden kunnen weerhouden om een dubbele uitgave te wagen:

> *'De stimulans kan wellicht nodes ertoe aanzetten om eerlijk te blijven. Als een hebzuchtige aanvaller erin slaagt meer CPU-vermogen te verzamelen dan alle eerlijke nodes, dan zou hij moeten kiezen tussen mensen te bedriegen door zijn betalingen terug te stelen, of om nieuwe munten te genereren. Het zou voor hem winstgevender*

zijn om volgens de regels te spelen, regels die hem verrijken met meer nieuwe munten dan de rest, in plaats van het systeem en de geldigheid van zijn eigen vermogen te ondermijnen.'

Zelfs in het ergste geval, zijn de stimuli van Bitcoin waarschijnlijk zodanig afgestemd dat iedereen eerlijk handelt.

Peer-To-Peer

Bitcoin was, zoals Nakamoto in zijn e-mailaankondiging had beloofd, ontworpen om een echt peer-to-peer-systeem te zijn.

Alle gebruikers zouden gelijk zijn binnen het netwerk, ze helpen elkaar het systeem draaiende te houden door het creëren en doorsturen van transacties en blokken, zonder enige speciale privileges of vertrouwde entiteiten. Er zou geen bedrijf zoals Digicash zijn om failliet te gaan, geen Bit Gold-eigendomsclub om te beslissen wie wat bezit, en ook geen vertrouwenloze RPOW-server om stop te zetten. Net als BitTorrent was Bitcoin in essentie ontworpen om een nieuw internetprotocol te zijn dat iedereen kon gebruiken, maar dat niemand zou beheersen.

Om dit klaar te spelen, moest Satoshi Nakamoto enkele van de meest hardnekkige problemen oplossen waar eerdere ontwerpen van gedecentraliseerde elektronische valuta mee worstelden: door dubbele uitgaven te voorkomen zonder een centrale partij, vond hij een oplossing voor het Byzantijnse Generaalsprobleem en ontdekte hoe inflatie in een proof-of-work-systeem beperkt kan worden ondanks voortdurende verbeteringen van de hardware. En, op het tijdstempelgebaseerde aanpassingsalgoritme van de moeilijkheid na, had hij dit gedaan zonder dat er baanbrekende technologieën nodig waren. Nakamoto gebruikte verschillende instrumenten uit de wereld van elektronisch geld en cryptografie die al minstens een decennium eerder waren ontwikkeld, en combineerde ze op een slimme manier.

Daarbovenop was zijn timing ook verbazingwekkend. Net toen centrale banken over de hele wereld ongekende maatregelen in het financiële systeem implementeerden in een wanhopige poging om een totale economische instorting te voorkomen, stelde Satoshi Nakamoto een nieuw soort geld voor. Dit geld kon

volledig zonder financiële instellingen functioneren — een digitaal valutasysteem dat geheel op wiskunde was gebaseerd.

Toch was de reactie op de publieke aankondiging van Bitcoin grotendeels zonder erkenning of waardering.

Schaalcapaciteit

De eerste reactie op Nakamotos aankondiging kwam ongeveer een dag later, van James A. Donald, een Cypherpunk die toevallig bijna klaar was met het ontwerpen van zijn eigen digitaal geldsysteem.

'Zo'n systeem hebben we zeer, zeer hard nodig, maar zoals ik jouw voorstel begrijp, lijkt het niet op te schalen naar de vereiste omvang', schreef Donald. 'Om tijdig dubbele uitgaven te detecteren en te verwerpen, moet men de meeste vorige transacties van de munten in de transactie hebben, wat, naïef geïmplementeerd, vereist dat elk persoon de meeste van eerdere transacties heeft, of de meeste transacties die recentelijk hebben plaatsgevonden. Als honderden miljoenen mensen transacties uitvoeren, is dat heel veel bandbreedte — iedereen moet alles weten, of een aanzienlijk deel daarvan.'[271]

Inderdaad, Nakamotos ontwerp vereiste dat gebruikers alle transacties op het Bitcoinnetwerk bijhielden, om zo hun lokale versies van het eigendomsgrootboek te kunnen bijwerken. Ze zouden precies moeten weten welke munten al waren uitgegeven en welke niet, om er zeker van te zijn dat een munt die ze als betaling ontvingen nog niet aan iemand anders was uitgegeven. Als het Bitcoinnetwerk groot genoeg zou worden, kon dit onuitvoerbaar worden voor de meeste standaardgebruikers.

Het was een probleem waarover Satoshi Nakamoto nagedacht had. In zijn witboek stelde hij een oplossing bestaande uit twee stappen voor, genaamd *Simplified Payment Verification* (SPV). Ten eerste, om de hoeveelheid benodigde schijfruimte voor het draaien van Bitcoin op de gemiddelde computer te minimaliseren, konden oudere blokken worden verwijderd van de computers, zodat ze alleen de blok-hashes hoefden op te slaan. En ten tweede, door gebruik te

271 James A. Donald, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 2 november 2008, online

maken van hashbewijzen, konden gebruikers controleren met behulp van deze blok-hashes dat transacties naar hen waren opgenomen in de blokketen — waarbij ze alle andere transacties grotendeels negeerden. Het draaien van een volledig validerende netwerknode 'zou meer en meer worden overgelaten aan specialisten met serverfarms van gespecialiseerde hardware', schreef Nakamoto als antwoord op Donald in de mailinglijst.[272]

Helaas loste deze oplossing het probleem niet volledig op, zoals Nakamoto zelf ook erkende in het witboek. Het introduceerde ook nieuwe problemen. SPV liet het beveiligingsmodel waarin iedereen elkaar in de gaten houdt varen, omdat in plaats daarvan alleen toegewijde miners zouden controleren of de regels van het systeem altijd worden nageleefd.

Donald reageerde op Nakamoto in de mailinglijst en waarschuwde dat als slechts een klein deel van de Bitcoingebruikers over voldoende middelen kon beschikken om een miner te zijn, deze een doelwit konden worden en een drukpunt voor regelgevende instanties.

In een lange en gedetailleerde repliek beschreef hij hoe overheden financiële netwerken stap voor stap zouden overnemen, uiteindelijk met als doel de gelduitgevende instantie te beheersen: 'Net zoals bijvoorbeeld de Federal Reservewet van 1913, is het doel altijd om het netwerk op te rollen in een enkele *te groot om te falen* entiteit, en zij zijn steeds groter, serieuzer en rampzaliger geworden.'

Bitcoin, voorspelde Donald, zou onderworpen worden aan hetzelfde type druk.

'Als een klein aantal instanties nieuwe munten uitgeeft, is dit beter bestand tegen staatsaanvallen dan bij een enkele uitgever, maar de overheid valt regelmatig financiële netwerken aan, met de financiële instorting die voortkomt uit de meest recente aanval die nog steeds aan de gang is terwijl ik dit schrijf', betoogde hij.

Om het systeem gedecentraliseerd te houden en ervoor te zorgen dat de meeste gebruikers alle transacties in het netwerk kunnen verwerken, stelde de Cypherpunk voor dat Bitcoin baat zou kunnen hebben bij een betalingslaag voor transacties van lage waarde. Alleen grote transacties zouden dan door alle gebruikers verwerkt en opgeslagen hoeven te worden in de blokketen.

'Ik denk dat we ons moeten bezighouden met het minimaliseren van de

272 Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 2 november 2008, online

gegevens en bandbreedte die gelduitgevers nodig hebben — voor kleine munten lijkt het protocol verspillend. Het zou mooi zijn om het volledige protocol voor grote munten te hebben, en een soort snelkoppeling voor kleine munten waarbij mensen accountgebaseerd geld vertrouwen voor kleine bedragen totdat ze worden omgezet in grote munten', schreef hij. 'Hoe kleiner de gegevensopslag en bandbreedte die gelduitgevers nodig hebben, hoe sterker het systeem bestand is tegen het soort overheidsaanvallen op financiële netwerken die we recentelijk hebben gezien.' [273]

Nakamoto heeft niet specifiek gereageerd op Donalds suggestie over de betalingslaag, maar hij heeft wel zeker de mogelijke aanvallen op staatsniveau aangepakt die Bitcoin uiteindelijk zou kunnen tegenkomen. Hoewel de mysterieuze auteur van het nieuwe witboek in zijn geschriften een tamelijk wetenschappelijke en zakelijke benadering van het onderwerp heeft uitgedragen, bevestigde Nakamoto nu onmiskenbaar de motivatie achter het gedecentraliseerde ontwerp van het systeem.

'Ja, maar we kunnen een grote slag winnen in de wapenwedloop en enkele jaren een nieuw territorium van vrijheid verwerven', schreef hij. 'Overheden zijn goed in het elimineren van de leiders van [...] centraal gecontroleerde netwerken zoals Napster, maar pure peer-to-peer netwerken zoals Gnutella en Tor lijken zich goed staande te houden.'[274]

Zorgen en verwarring

De eerste reactie die Nakamoto kreeg — de bezorgdheid van James A. Donald over schaalbaarheid — was zeker niet onterecht; het opschalen van Bitcoin om miljoenen, of zelfs miljarden gebruikers te dienen, zou inderdaad een grote uitdaging worden. Maar veel van de feedback die volgde op deze reactie was meer uiteenlopend , waarbij sommigen duidelijk in de war waren over het ontwerp van Bitcoin.

Ray Dillinger, een informaticus en Cypherpunk die een van de eerste bijdragers

273 James A. Donald, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 3 november 2008, online

274 Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 6 november 2008, online

was aan de Cryptography-mailinglijst, wees bijvoorbeeld Bitcoin af vanwege het inflatiepercentage van 35% — hoewel er in het witboek geen inflatieschema werd genoemd. Hij ging er onterecht van uit dat de uitgifte van nieuwe munten zou toenemen naarmate computerhardwareprestatie door de jaren heen zou verbeteren, zoals het geval was geweest bij een systeem zoals RPOW.[275]

Als mogelijke oplossing voor het inflatieprobleem, stelde Dillinger in een latere e-mail voor dat Bitcoin een moeilijkheidaanpassingsalgoritme zou moeten hebben. Hij leek zich er echter niet van bewust dat dit al onderdeel was van Nakamotos ontwerp.[276]

Ondertussen beweerde Donald dat Nakamotos moeilijkheidaanpassingsalgoritme helemaal niet zou werken. Hij leek te geloven dat dit volledig de prikkel zou wegnemen om nieuwe blokken te minen, hoewel hij in zijn e-mail niet uitlegde waarom.[277]

Zowel Dillinger als Donald waren het er echter over eens dat het proof-of-work-consensusmechanisme van Bitcoin niet robuust of snel genoeg was. Ze hielden niet van het idee dat transacties omkeerbaar konden zijn, in het geval dat de blokketen wordt ingehaald door een langere concurrerende ketting, en vonden het wachten op meerdere blokbevestigingen geen degelijke oplossing.

'Hoe weet iemand wanneer een transactie onomkeerbaar is geworden?' vroeg Dillinger, retorisch. 'Is *een paar* blokken drie? Dertig? Honderd?'[278]

Wat het *juiste* nummer ook was, het zou niet werken, voorspelde hij: noch consumenten noch verkopers zouden bereid zijn om *een uur* te wachten tot transacties waren afgerond.

Donald deelde die assumptie: 'We willen dat mensen zeker zijn dat hun transactie geldig is, en dat dit van dezelfde duur is als tijdens een uitgave om het netwerk te overspoelen, niet op het moment dat het nodig is om vertakkingswedstrijden

275 Ray Dillinger, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 6 november 2008, online

276 Ray Dillinger, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 14 november 2008, online

277 James A. Donald, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 9 november 2008, online

278 Ray Dillinger, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 15 november 2008, online

op te lossen.'[279]

John Levine, een andere informaticus die eerder de Cypherpunks-mailinglijst bezocht, maar later overstapte naar de Cryptography-mailinglijst, zette ook vraagtekens bij het consensusmodel van Bitcoin, maar om een andere reden. Levine voorspelde dat het proof-of-work-consensusmodel niet erg veilig zou zijn tegen aanvallers.

'Slechteriken hebben regelmatig controle over zombienetwerken van meer dan 100.000 machines. Mensen die ik ken houden een zwarte lijst bij van computers die spam verspreiden, en zij vertellen me dat er vaak wel een miljoen nieuwe zombies per dag zijn', schreef Levine. 'Dit is dezelfde reden waarom hashcash niet kan werken op het internet van vandaag — de brave mensen hebben aanzienlijk minder rekenkracht dan de slechteriken.'[280]

Echter, niet iedereen op de Cryptography-mailinglijst was bereid Bitcoin af te doen als een foutief ontwerp.

Optimisme

Op 7 november, ongeveer een week nadat Nakamoto zijn witboek openbaar had gemaakt, kwam er ook een opvallend optimistische reactie naar voren op de lijst.

'Bitcoin lijkt een veelbelovend idee te zijn', begint Hal Finney zijn e-mail, en duidt vervolgens nauwkeurig de twee voornaamste innovaties aan in vergelijking met voorgaande elektronische betaalsystemen. 'Ik waardeer het idee dat de beveiliging is gebaseerd op de veronderstelling dat de CPU-kracht van eerlijke deelnemers die van de aanvaller overstijgt', schreef hij. 'Ik denk ook dat er potentieel is in de vorm van een onvervalsbare token waarvan de productiesnelheid voorspelbaar is en niet kan worden beïnvloed door corrupte partijen. Dit zou meer vergelijkbaar zijn met goud dan met fiatvaluta. Nick Szabo schreef al vele jaren geleden over wat hij *bit gold* noemde en dit kan een implementatie van dat concept zijn.'[281]

---

279 James A. Donald, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 9 november 2008, online

280 John Levine, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 3 november 2008, online

281 Hal Finney, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 7 november 2008, online

Net als Donald haalde Finney ook meteen aan dat Bitcoin wellicht baat kon hebben bij een lichtgewicht betalingssysteem boven op het bestaande protocol. Naast verbeterde schaalcapaciteit gaf de doorgewinterde expert op het gebied van elektronisch geld aan dat dit het systeem sterker zou maken en meer privacyfuncties zou kunnen bieden.

'Er zijn ook voorstellen gedaan om lichtgewicht anonieme betalingssystemen te bouwen bovenop zwaargewicht niet-anonieme systemen, zodat Bitcoin zou kunnen worden ingezet om anonimiteit mogelijk te maken, zelfs verder dan de mechanismen die in het witboek worden besproken', schreef hij.[282]

Een paar dagen later, in een afzonderlijke e-mail, merkte Finney op dat een bron van verwarring in de verschillende reacties op de mailinglijst voortkwam uit het feit dat Bitcoin in feite twee verschillende ideeën bundelde in één voorstel. Hij legde uit dat Bitcoin allereerst een poging was om een wereldwijd consistente, maar gedecentraliseerde database te creëren. Op zijn beurt werd deze database dan gebruikt om een elektronisch geldsysteem te realiseren. Waar verschillende deelnemers aan de mailinglijst zich meer op het ene of het andere aspect focusten en benadrukten dat het aspect waarop ze zich focusten enigszins imperfect was opgelost, was het vindingrijke aan Bitcoin dat het beide deed, en dat op een manier waarop ze elkaar aanvulden.

'Het oplossen van het wereldwijde, sterk gedecentraliseerde databaseprobleem is misschien wel het moeilijkste deel', schreef Finney. 'Het gebruik van *proof-of-work* als hulpmiddel voor dit doel is een nieuw idee dat volgens mij zeker verdere evaluatie verdient.'

Zijn eigen e-mail bevatte een deel van deze beoordeling. Terwijl hij nadacht over de veiligheid van het systeem, bedacht hij dat gebruikers het netwerk draaiende konden houden, zelfs als het enkel om het ondersteunen als sociaal nuttig project ging, niet anders dan de soorten internetprojecten waarbij mensen rekenkracht doneren om medisch onderzoek te ondersteunen of radiosignalen te analyseren op zoek naar tekenen van buitenaards leven. 'In dit geval lijkt het me dat simpel altruïsme kan volstaan om het netwerk goed te laten functioneren',

282 Hal Finney, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 7 november 2008, online

concludeerde Finney.[283]

Nakamoto was het hiermee eens.

'Het is erg aantrekkelijk vanuit het libertaire standpunt als we het goed kunnen uitleggen', antwoordde de uitvinder van Bitcoin. 'Ik ben echter beter met code dan met woorden.'[284]

Het pseudoniem

De voornamelijk sceptische reacties op het witboek in de Cryptography-mailinglijst kunnen waarschijnlijk deels worden verklaard doordat de auteur van het witboek, Satoshi Nakamoto, compleet onbekend was.

Satoshi Nakamoto had tot dan toe nog geen actieve rol gespeeld op de Cryptography-mailinglijst, de Cypherpunk-mailinglijst of enige andere relevante mailinglijst, en niemand onder die naam was ooit naar een Cypherpunk-bijeenkomst gekomen. Satoshi Nakamoto had nog geen eerdere digitale geldsystemen voorgesteld, en hij had ook geen andere opmerkelijke artikels over cryptografie of computertechnologie gepubliceerd. Wat dat betreft, was Satoshi Nakamoto een onbekende in Cypherpunk en cryptokringen, en elke keer wanneer een onbekende een nieuw elektronisch geldsysteem aankondigde, had het doorgaans weinig betekenis.

Maar de uitvinder van Bitcoin had mogelijks meer ervaring in het vakgebied dan hij liet blijken. Hoewel de meeste abonnees van de Cryptography-mailinglijst waarschijnlijk aannamen dat ze werden gecontacteerd door een Japanse man, of op zijn minst een man van Japanse afkomst, was *Satoshi Nakamoto* hoogstwaarschijnlijk een pseudoniem. Degene die achter deze schuilnaam zat, was mogelijk wel één of meerdere van de vooraanstaande bijdragers aan de Cryptography-mailinglijst, of de Cypherpunk-lijst daarvoor.

Aan de andere kant, hij, zij, of zij (als groep) hadden net zo nieuw en onervaren kunnen zijn in het domein van elektronisch geld als hun pseudoniem aanduidde.

Wat de waarheid ook is, de entiteit simpelweg bekend als Satoshi Nakamoto

283 Hal Finney, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 13 november 2008, online

284 Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 14 november 2008, online

leek niet bijzonder gehinderd te zijn door de sceptische reacties. Hoewel zijn witboek een zeer beknopt overzicht was van het Bitcoinprotocol, erkende hij dat hij veel functionele details weggelaten had. Daarom beantwoordde hij geduldig de meeste zorgen en verwarring over zijn voorstel en nam hij de tijd om alle delen van het ontwerp die misschien onduidelijk waren opnieuw uit te leggen.

Hoewel hij niet elk detail in het witboek had opgenomen, had hij over de meeste ervan nagedacht. In een van zijn e-mailreacties verduidelijkte Nakamoto dat hij de ontwikkeling van Bitcoin *achterstevoren* had benaderd: hij had zelfs de meeste Bitcoincode geschreven nog voor het opstellen van het witboek.[285]

Inderdaad, Bitcoin was niet zomaar een voorstel, zoals dat bij Bit Gold en b-money het geval was. Satoshi Nakamoto had al twee jaar gespendeerd aan de implementatie van het idee in code. Na iets meer dan twee weken discussies met een handvol respondenten, bood hij aan om de belangrijkste bestanden te sturen naar abonnees van de Cryptography-mailinglijst als zij daarom vroegen. De volledige release, zo beloofde hij, zou spoedig volgen.

Voor lijstbeheerder Perry Metzger — een andere vroege Cypherpunk — was het een goed moment om een pauze in te lassen voor Bitcoin.

'Ik zou graag voorlopig een einde willen maken aan de bitcoin e-cash-discussie — er wordt veel gediscussieerd en dat zou beter kunnen als mensen op dit moment op zichzelf schrijven in plaats van dingen heen en weer te herhalen', schreef Metzger. 'Misschien kunnen we hier later op terugkomen wanneer Satoshi (of iemand anders) iets in detail opstelt en het publiceert.'[286]

285 Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 8 november 2008, online

286 Perry E. Metzger, *ADMIN: end of bitcoin discussion for now*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 17 november 2008, online

Hoofdstuk 16

De release

*'**Wet, taal, geld**: de drie paradigma's van spontaan ontstane instituties. Gelukkig hebben wet en taal zich mogen ontwikkelen. Geld is ontstaan in zijn oorspronkelijke vorm, maar zodra het er in zijn meest primitieve vorm was, werd het bevroren. Overheden zeiden dat het niet verder mocht ontwikkelen. En wat we sinds die ontwikkeling hebben gehad, waren zaken van overheidsuitvindingen, meestal verkeerde, meestal misbruik van geld, en ik ben tot het punt gekomen dat ik me afvraag: heeft monetair beleid ooit enig goed gedaan? Ik denk het niet. Ik denk dat het alleen maar schade heeft aangericht. Dat is waarom ik nu pleit voor wat ik* denationalisering van geld *heb genoemd.'*[287]

In een van zijn laatst opgenomen interviews in 1984 aan de Universiteit van Freiburg bleef de op leeftijd geraakte Friedrich Hayek pleiten voor radicale monetaire hervormingen. De econoom was er nog steeds van overtuigd dat fiatvaluta en het rentebeleid van centrale banken de economie vergiftigden, en dat geld uiteindelijk best kon worden overgelaten aan de vrije markt.

Maar in de acht jaar sinds de publicatie van *Denationalisation of Money*, was de Oostenrijker nog minder hoopvol geworden dat bestaande regeringen bereid zouden zijn om wetten aan te passen die concurrentie tussen valuta mogelijk zou maken. Hij vermoedde dat ze te veel voordeel haalden uit de status quo.

---

287 Friedrich A. Hayek, *F. A. Hayek on Monetary Policy, the Gold Standard, Deficits, Inflation, and John Maynard Keynes*, interview door James U. Blanchard III, opnieuw gepubliceerd door *Libertarianism.org* op 19 april 2015, online

'Ik geloof nog steeds dat mijn oorspronkelijke plan juist is, maar ik vrees dat ik tot de conclusie ben gekomen dat het politiek gezien volledig utopisch is', legde Hayek nuchter uit. 'Overheden zullen het nooit toestaan, en zelfs bankiers begrijpen het idee niet, omdat ze allemaal zijn opgegroeid in een systeem waarin ze zo volledig afhankelijk zijn van centrale banken, overheidsinstellingen, als kredietverstrekkers in uiterste nood.'[288]

En toch koesterde de toen vierentachtigjarige econoom nog steeds de hoop dat geld gerepareerd kon worden. Maar het vereiste een andere aanpak dan het soort burgerbeweging dat hij in zijn boek beschreef. Aangezien overheden de beperkingen die vrijemarktcompetitie voor valuta belemmerden, niet zouden wegnemen, suggereerde hij dat mensen creatief moesten zijn en een manier moesten vinden om deze beperkingen te omzeilen.

In plaats van te proberen overheden te overtuigen hun feitelijke monopolie op geld op te geven, zouden mensen *op een of andere sluwe, indirecte manier iets moeten introduceren dat ze niet kunnen stoppen*.

Toen Satoshi Nakamoto bijna vijfentwintig jaar later, op 8 januari 2009, terugkeerde naar de Cryptography-mailinglijst om een volledig vertrouwensloos en volledig peer-to-peer elektronisch geldsysteem te starten, deed hij exact wat Hayek suggereerde. Hij maakte gebruik van tientallen jaren onderzoek in privacytechnologie, de architectuur van gedecentraliseerde netwerken en digitale valutasystemen. Satoshi Nakamoto introduceerde iets wat regeringen niet kunnen stoppen.

De broncode

Bitcoin v.0.1 is uitgebracht, luidde de titel van Nakamotos e-mail deze keer.[289]

De abonnees van de Cryptography-mailinglijst die de e-mail openden, troffen er een tweezinnige beschrijving van Satoshi Nakamoto aan over het net gelanceerde project:

'Hierbij kondig ik de eerste release van Bitcoin aan, een nieuw elektronisch geldsysteem

288 Hayek, interview.

289 Satoshi Nakamoto, *Bitcoin v0.1 released*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 8 januari 2009, online

dat een peer-to-peer netwerk gebruikt om dubbele uitgaven te voorkomen. Het is volledig gedecentraliseerd zonder server of centrale autoriteit.'

Naast de korte beschrijving, bevatte de e-mail een downloadlink voor de software, een link naar de website van het project — bitcoin.org — en verschillende alinea's met aanvullende informatie, disclaimers ('de software is nog in alfaversie en experimenteel') en basisinstructies om het te gebruiken.

Iets meer dan twee maanden nadat hij zijn witboek aan de Cryptography-mailinglijst had voorgelegd, maakte Satoshi Nakamoto de eerste versie van de Bitcoinsoftware openbaar. Het programma, bekend als Bitcoin versie 0.1, was klaar om gedownload en gebruikt te worden: men kon sleutelparen aanmaken, transacties uitvoeren, en blokken minen. De release van de software onthulde ook belangrijke nieuwe informatie over het project.

Wat meteen opviel — hoewel het geen grote verrassing was — was dat Satoshi Nakamoto Bitcoin had vrijgegeven als vrije en open source-software. Iedereen was vrij om de code te kopiëren, te gebruiken, te delen en te wijzigen. Gepubliceerd onder de MIT-licentie, konden zelfs commerciële projecten Nakamotos werk integreren (dit maakt de MIT-licentie minder restrictief dan Richard Stallmans GPL-licentie, die deze vrijheid enkel toekent aan andere vrije softwareprojecten).

Het was essentieel dat Bitcoin vrije en open source-software was, omdat de code noodzakelijkerwijs controleerbaar moest zijn: om het systeem echt vertrouwensloos te laten functioneren, zouden gebruikers moeten kunnen verifiëren dat het werkt zoals beloofd. Dit was wellicht nog crucialer voor Bitcoin dan voor vele andere softwareprojecten, aangezien de code letterlijk geld vertegenwoordigde. Passend bij de filosofie van Stallman voor vrije software, zouden mensen Satoshi Nakamoto niet moeten vertrouwen om geen malware in te bouwen om munten te stelen of een geheime achterdeur voor het bijdrukken van geld te introduceren.

Meer in het algemeen maakte Nakamotos vrije en open source-code, geschreven in de programmeertaal C++ en jaren later door de eerste voltijdse Bitcoinontwikkelaar beschreven als 'briljant maar slordig', voor het eerst volledig inzichtelijk hoe het elektronische geldsysteem intern werkte.[290]

290 Michael J. Casey, *Bitcoin Foundation's Andresen on Working With Satoshi Nakamoto*, *The Wall Street Journal*, 6 maart 2014, online

Transacties bleken bijvoorbeeld gebruik te maken van *Script*, een nieuwe programmeertaal voor Bitcoin die geïnspireerd was op Forth, een programmeertaal origineel ontworpen in de jaren 1960 om radiotelescopen te bedienen. Met enkele aanpassingen aan de functionaliteit van Forth, kon Script gebruikt worden om eenvoudige slimme contracten op Bitcoin te schrijven. Munten konden zodanig worden opgeslagen dat ze alleen verplaatst konden worden als er aan bepaalde programmeerbare condities werd voldaan (een eenvoudig voorbeeld hiervan was *multisignature*, of *multisig*, waarbij niet één, maar meerdere cryptografische handtekeningen vereist waren om de munten uit te geven).

Het handtekeningsysteem dat ingebed is in Bitcoin was de Elliptic Curve Digital Signature Algorithm (ECDSA), die, zoals de naam al suggereert, wiskundig gegenereerde elliptische curven gebruikte om sleutelparen te berekenen. Het was uitgevonden in 1985, zo'n acht jaar na RSA. De elliptische curve-cryptografie bood hetzelfde beveiligingsniveau als de oplossing van Rivest, Shamir en Adlemen, maar vereiste veel kleinere sleutelgroottes en was in de loop der jaren een gangbaar alternatief geworden.

Tegelijkertijd had Nakamoto een aantal functies toegevoegd om Bitcoin wat gebruiksvriendelijker te maken. Hoewel betalingen technisch gezien nog altijd naar publieke sleutels gedaan werden, konden gebruikers hun publieke sleutel (of de hash van hun publieke sleutel) coderen in een Bitcoin-*adres*. Wanneer ze geld ontvingen, deelden ze doorgaans alleen deze adressen met andere gebruikers.

De broncode van Bitcoin onthulde ook veel van de min of meer willekeurige parameters die Nakamoto had gekozen. Zoals hij al eerder op de Cryptography-mailinglijst had gesuggereerd, zou er gemiddeld elke tien minuten een nieuw blok gevonden moeten worden. Clusters van 2.016 blokken zouden vervolgens worden gebruikt om de moeilijkheidsgraad van minen aan te passen: als de 2.016 blokken in minder dan twee weken werden gevonden, zou de moeilijkheidsgraad van Bitcoin proportioneel worden verhoogd, en als het meer dan twee weken duurde om de 2.016 blokken te vinden, zou de moeilijkheidsgraad van het proof-of-work naar beneden worden bijgesteld.

En om het Bitcoinnetwerk daadwerkelijk op gang te brengen, bevatte de broncode ook de allereerste blok: het *Genesisblok*. Dit blok moest inderdaad ingebed worden in de release zelf; de blokketen had een startpunt nodig. Een interessant detail is echter dat de beloning voor dit Genesisblok in feite waar-

deloos was: de protocolregels stonden niet toe dat deze specifieke munten onder enige voorwaarde uitgegeven konden worden. In Bitcoin kunnen nieuwe munten alleen worden verdiend door competitief te minen, en Nakamoto weigerde een voorsprong van één blok voor zichzelf te accepteren. Als hij munten wilde hebben, moest zelfs hij, de maker van het systeem, ze verdienen — net als alle anderen.

Nakamoto benadrukte nog eens zijn expliciete weigering om enig oneerlijk voordeel te genieten boven andere Bitcoingebruikers. Hij had ook een bewijs toegevoegd dat hij in de weken of maanden voorafgaand aan het openbaar maken van de code niet privé had gemined. Hij had een kop van de voorpagina van de Engelse krant *The Times* van 3 januari in het Genesisblok opgenomen, wat aantoont dat deze blok niet voor die datum kon gecreëerd zijn. Dit betekent op zijn beurt dat elk daaropvolgend blok later gemined moest zijn.[291]

Als kers op de taart leek de specifieke kop ook niet willekeurig voor dit doel gekozen te zijn:

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

De wereld van geld en financiën was een puinhoop geworden. Met Bitcoin stelde Satoshi Nakamoto een alternatief voor.

Eenentwintig miljoen

Het interessantste nieuw onthulde kenmerk was echter het *monetaire beleid* van Bitcoin. Het witboek beschreef hoe Bitcoin een voorspelbaar uitgifteschema kon garanderen, dankzij vaste blokbeloningen en het moeilijkheidsaanpassingsalgoritme. Maar het document gaf nog niet precies aan hoe dit schema eruit zou zien.

Het bleek nu dat de code van Bitcoin zo was geprogrammeerd dat het aantal nieuwe munten die per blok werden toegekend halveerde na elke 210.000 blokken, of ongeveer eens in de vier jaar. In de eerste vier jaar zouden miners 50 nieuwe munten per blok verdienen, maar in de vier jaar daarna zouden ze slechts 25 nieuwe munten per blok verdienen. In de volgende vier jaar zou dat

291 Aangezien Bitcoin uiteindelijk op 8 januari werd uitgebracht, zou dit de maker van het systeem een maximum van zes dagen hebben gegeven om comfortabel munten te genereren zonder enige concurrentie, maar vroege block-timestamps geven aan dat hij dit ook niet heeft gedaan.

12,5 zijn, daarna 6,25 in de vier daaropvolgende jaren, en zo verder. Nakamoto kondigde in zijn e-mail aan:

> *De totale circulatie zal bestaan uit 21.000.000 munten. Ze worden verdeeld onder de netwerknodes wanneer ze blokken maken, waarbij de hoeveelheid elke 4 jaar gehalveerd wordt.*
>
> *In de eerste 4 jaren: 10,500,000 munten*
>
> *In de volgende 4 jaren: 5.250.000 munten.*
>
> *In de volgende 4 jaren : 2.625.000 munten.*
>
> *In de volgende 4 jaren : 1.312.500 munten.*
>
> *Wanneer dit tot zijn einde komt, kan het systeem transactiekosten invoeren, indien nodig.*

Eenentwintig miljoen munten.[292] Bitcoin was ontworpen met een vaste voorraad. De gevolgen hiervan waren waarschijnlijk groter dan veel abonnees van de Cryptography-mailinglijst zich realiseerden.

Slechts enkele jaren eerder was het RPOW-project van Hal Finney mislukt, grotendeels omdat mensen geen economische prikkel hadden (zelfs een negatieve economische prikkel) om RPOW-tokens te bezitten. Dit betekende dat vrijwel niemand bereid was om ze als betaling te accepteren. Doordat er bijna geen plaatsen waren om ze uit te geven, waren de tokens praktisch nutteloos en daardoor waardeloos, wat betekende dat ze niet echt als geld gebruikt konden worden. Net als eCash en hashcash, leed RPOW onder een kip-en-ei-probleem dat het niet had kunnen overwinnen.

Bitcoin moest zichzelf ook opstarten vanaf nul. Toen Nakamoto zijn code voor het eerst vrijgaf, werd bitcoin natuurlijk nergens als betaalmiddel geaccepteerd en hadden deze munten geen monetaire waarde. Maar het was net Hal Finney die besefte dat de stimulansen deze keer enigszins anders zaten.

Op 10 januari, twee dagen na de release van Bitcoin, was Finney de eerste persoon op de Cryptography-mailinglijst die reageerde op de aankondigingsmail.

292 Het is echter belangrijk op te merken dat elke bitcoin tot acht decimalen kan worden opgedeeld, waardoor er in zekere zin 2,1 biljard valutadelen zijn. De kleinste eenheid, 0,00000001 bitcoin, wordt tegenwoordig meestal een *satoshi* genoemd, of kortweg *sat*.

Na Nakamoto te feliciteren met de release en te beloven het te proberen, richtte de veteraan in de wereld van elektronisch geld zijn aandacht snel op de vaste geldvoorraad van Bitcoin.

'Een direct probleem met elke nieuwe munteenheid is hoe deze te waarderen', schreef hij. 'Zelfs als we het praktische probleem negeren dat vrijwel niemand het in het begin zal accepteren, is er nog steeds een uitdaging om een redelijk argument te vinden ten gunste van een specifieke niet-nul waarde voor de munten.'

Maar Finney, die goed onderlegd was in de wereld van statistiek en kansberekening, geloofde dat de vaste voorraad van Bitcoin de oplossing kon bieden. Het stelde mensen in staat om eenvoudige inschattingen te maken over de potentiële toekomstige waarde van de munten.

'Stel je voor dat Bitcoin succesvol is en het dominante betalingssysteem in de wereld wordt. Dan zou de totale waarde van de valuta gelijk moeten zijn aan de totale waarde van alle rijkdom ter wereld. Actuele schattingen van het totale wereldwijde vermogen liggen tussen de 100 en 300 biljoen dollar. Met 20 miljoen munten zou elke munt een waarde hebben van ongeveer 10 miljoen dollar', berekende hij.

'Dus de kans om vandaag de dag munten te genereren met slechts enkele centen aan computertijd kan een zeer goede *gok* zijn, met een mogelijke uitbetaling van iets als 100 miljoen tegen 1! Zelfs als de kans klein is dat Bitcoin in deze mate succesvol wordt, zijn ze echt 100 miljoen tegen één? Iets om over na te denken…'[293]

Het was inderdaad iets om over na te denken. De schattingen van Finney waren natuurlijk ruw, het was slechts wat rekenwerk op een kladblad. Maar zolang de kans dat Bitcoin in de toekomst zou slagen niet nul was, zou het inderdaad rationeel zijn om voor een goedkope prijs wat munten te bemachtigen.

Als anderen dezelfde redenering volgden, zou dat meteen de vraag naar de munten doen toenemen, ruwweg tot het punt waar de markt inschat dat de verhouding tussen risico en beloning het nog steeds waard zou zijn. De potentiële toekomstige waarde van een bitcoin, en de geschatte kans dat deze toekomst

293 Hal Finney, *Bitcoin v0.1 released*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 10 januari 2009, online

werkelijkheid wordt, zou in feite in de huidige marktprijs moeten worden weerspiegeld.

En zodra er een marktprijs voor de munten is vastgesteld — dat wil zeggen, *elke* niet-nul marktprijs — kunnen ze daadwerkelijk ook als een vorm van geld gebruikt beginnen worden, waarschijnlijk eerst in plaatsen zonder enige alternatieven.

In een vervolgmail suggereerde Nakamoto: '[…] zoals beloningspunten, donatietokens, valuta voor een spel of micropayments voor volwassenensites.'[294]

Dit zou de vraag *nog* meer moeten stimuleren. Hierdoor zou bitcoin in feite het klassieke kip-en-ei-probleem, waar eerdere digitale geldprojecten onder te lijden hadden, kunnen overwinnen. Bitcoin zou zelfs een *positieve* feedbacklus kunnen vertonen!

In zekere zin had Finney het regressietheorema van Ludwig von Mises ondersteboven gekeerd: in plaats van de waarde van een valuta te herleiden uit de koopkracht in het *verleden*, stelde de Cypherpunk voor dat een valuta waarde in eerste instantie kan worden afgeleid uit de verwachte koopkracht in de *toekomst*.

'Het zou logisch kunnen zijn om er gewoon wat te bemachtigen in het geval dat het aanslaat', stemde Satoshi Nakamoto toe. 'Als genoeg mensen op dezelfde manier denken, wordt dat een *self-fulfilling prophecy*.'[295]

Hayeks ideaal

Het oplossen van het kip-en-ei-probleem was niet het enige potentiële voordeel van de limiet van eenentwintig miljoen. Het was misschien zelfs niet het grootste voordeel, zeker niet op een grotere tijdschaal. Als de analyse van Friedrich Hayek over de monetaire economie aan het begin van zijn carrière correct was, *zou Bitcoin de economie kunnen helpen te herstellen*.

Bitcoin, als een ongedekte valuta die zonder centrale bank werkt, was een volledig homogene vorm van geld. Iedereen kon zijn eigen munten beheren, en er waren geen reserveverhoudingen om zich zorgen over te maken. En aangezien bitcoin op het internet bestond, kende het geen grenzen. Iedereen

294 Satoshi Nakamoto, *Bitcoin v0.1 released*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 16 januari 2009, online

295 Satoshi Nakamoto, *Bitcoin v0.1 released*, oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, 16 januari 2009, online

met een internetverbinding, waar ook ter wereld, kon de software downloaden en beginnen met het verzenden en ontvangen van transacties naar wie dan ook.

Deze combinatie — een homogeen, grenzeloos geld met een vaste voorraad — is wat Hayek ooit beschreef als *neutraal geld*.

Toen hij hier voor het eerst over schreef, beschouwde Hayek neutraal geld als een onbereikbaar ideaal, een perfecte valuta die eigenlijk niet gerealiseerd kon worden. Belangrijker nog, hij geloofde niet dat er een internationale autoriteit was die te vertrouwen was om zo'n valuta uit te geven. De econoom dacht dat, op een zeer fundamenteel niveau, naties niet op elkaar konden vertrouwen om de vaste voorraad te eren. En hij had waarschijnlijk gelijk. In voldoende extreme omstandigheden (zoals oorlog), zouden degenen die controle over de geldprinter hadden altijd in de verleiding komen om dit privilege te misbruiken, ongeacht eerdere afspraken, conventies of verdragen.

Maar Bitcoin werd niet uitgegeven door dergelijke internationale autoriteit: er was geen geldprinter om controle over te hebben. Satoshi Nakamoto had het systeem zo ontworpen dat er absoluut geen vertrouwde derde partij nodig was. Bitcoin was vanaf het begin niet afhankelijk van monetaire afspraken, conventies of verdragen, dus er waren ook geen afspraken, conventies of verdragen om te verbreken. Althans in theorie, verwezenlijkte Bitcoin wat Hayek onmogelijk achtte.

Dit betekende dat als bitcoin enige kans zou hebben om de wereldwijde valuta te worden, het potentieel — zoals geschetst door Hayek in de jaren 1920 en 1930 — enorm zou zijn.

Om te beginnen zou Bitcoin een einde kunnen maken aan monetair nationalisme. Als de elektronische valuta van Nakamoto op grote schaal werd geaccepteerd in internationale handel, zouden gezamenlijke prijswijzigingen tussen landen eindelijk nauwkeurige signalen aan de markt kunnen geven, wat de optimale toewijzing van middelen over landsgrenzen heen mogelijk zou maken, los van nationaliteiten. Bijgevolg zou Bitcoin ook de internationale handel op een veel directere manier vergemakkelijken, waarbij alleen de koper en verkoper en (de prijzen van) hun respectieve producten worden beïnvloed — niet de prijsniveaus over hun hele landen.

Bovendien kon Bitcoin een einde maken aan valutaoorlogen. Als de hele wereld hetzelfde, neutrale geld zou gebruiken, zouden onderlinge devaluaties en de

economische ellende die daaruit voortkomt, voorgoed tot het verleden behoren.

Bitcoin kon ook een einde maken aan het Cantillon-effect. Vooral als alle eenentwintig miljoen munten in omloop zijn, zou niemand profiteren van nieuw geld in omloop te brengen, wat zou leiden tot een wanverhouding van middelen in hun voordeel. Maar zelfs wanneer er nog nieuwe munten worden gemined, zou dit in feite geen enkel individu, groep of specifieke sector bevoordelen. Iedereen zou vrij zijn om te minen, waardoor (en door het moeilijkheidsaanpassingsalgoritme) vrije concurrentie de winstmarges tot nul moest drijven: het proof-of-work dat het zou kosten om een blok te vinden zou ongeveer gelijk moeten zijn aan de waarde van de blokbeloning.

Maar misschien heeft Bitcoin nog een grotere impact dan dat. Voor het eerst zou het intertemporele prijssysteem zonder belemmeringen kunnen functioneren. Als gevolg hiervan zouden de rentetarieven *eindelijk* de gezamenlijke tijdsvoorkeuren in de maatschappij weergeven. Dit zou producenten informeren in welk productiestadium ze moeten investeren, wat een efficiënte toewijzing van middelen doorheen de tijd vergemakkelijkt. Door zich te verzetten tegen een beleid van kunstmatige rentetarieven, zou Bitcoin een eind kunnen maken aan het centraal beheerde monetaire beleid. Volgens de Oostenrijkse conjunctuurcyclustheorie zou dit de daarmee samenhangende economische op- en neergangen stoppen.

En dankzij de vaste geldhoeveelheid zou tot slot een verandering in productiekosten precies weerspiegeld worden in veranderende prijzen. Als de productiekosten zouden dalen, dan zouden de prijzen hetzelfde doen: dit was het soort deflatie dat Hayek als natuurlijk en gezond beschouwde.

Met ongeveer 32.000 regels code legde Satoshi Nakamoto de basis om de monetaire dogma's van de stabilisatoren, die de dominante Keynesiaanse en Monetaristische monetaire theorieën bijna een eeuw lang hebben beïnvloed, te verdringen.

… *Als* het alom aanvaard zou worden.

Het laatste punt van centralisatie

Op 8 januari 2009, begon Bitcoin zijn reis met slechts één gebruiker: de ontwerper van het digitale valutasysteem zelf. Hoewel het waarschijnlijk is dat honderden

mensen, na de aankondiging van Nakamoto op de Cryptography-mailinglijst, over het project hadden gehoord, wijzen de weinige reacties op zijn e-mail en de eerder sceptische reacties erop, dat in de begindagen slechts een handvol mensen de software daadwerkelijk hadden geprobeerd (met Hal Finney die op 12 januari de allereerste transactie ooit van Nakamoto ontving).

Desondanks was het zaadje geplant. Met een vastgestelde geldvoorraad, semi-anonimiteit, betalingen die resistent zijn tegen censuur, de mogelijkheid tot simpele slimme contracten, en relatief snelle en goedkope wereldwijde transacties als inherent onderdeel van Bitcoin, was het klaar om gebruikt te worden door iedereen die er baat bij dacht te hebben.

Eén ding was duidelijk: als Bitcoin gebruikers zou aantrekken, zouden die uit eigen initiatief komen. Bitcoin was een valuta die men gebruikte als en wanneer men ervoor koos om het te gebruiken, niet omdat iemand hen daartoe dwong. Terwijl het gebruik van fiatgeld bij wet verplicht was — het was het geld dat tenminste voor het betalen van belasting moest worden gebruikt — zou het verzenden en ontvangen van bitcoin volledig vrijwillig zijn.

Uiteindelijk kwamen er inderdaad gebruikers. Ondanks een zeer traag beginjaar, begon Bitcoin in de loop van 2010 best wat aantrekkingskracht te vertonen. Het transactievolume begon langzaam toe te nemen, nieuwe ontwikkelaars ontdekten het project, en er vormde zich een kleine onlinegemeenschap op een internetforum dat volledig gewijd was aan het project voor elektronisch geld. Dat is het moment waarop Satoshi Nakamoto het laatste aanzienlijke punt van centralisatie uit het project verwijderde: zichzelf.

De pseudonieme maker van Bitcoin had aanvankelijk een leidende rol in de voortzetting van de softwareontwikkeling en had een grote invloed op de richting van het vrije en open source-project. Maar toen de digitale valuta in populariteit begon te groeien, begon Nakamoto zich langzaam terug te trekken. Uiteindelijk, tegen het einde van 2010, stopte hij volledig met reageren op berichten en verwijderde hij zijn contactgegevens van de bitcoin.org-website.

Technisch gezien was het verdwijnen van Nakamoto onbelangrijk. De mysterieuze ontwikkelaar had eigenlijk geen controle over Bitcoin: het bestond als een peer-to-peer netwerk dat werd bediend door gebruikers over de hele wereld. Maar in de praktijk had de maker van het project de natuurlijke autoriteit om aanpassingen aan de code door te voeren.

Bijgevolg kon Satoshi Nakamoto de regels van het systeem bepalen, en tijdens zijn periode als hoofdontwikkelaar heeft hij inderdaad enkele wijzigingen in deze regels aangebracht. Hij verwijderde bijvoorbeeld functionaliteit uit Script die hij als potentieel gevaarlijk beschouwde, terwijl hij tegelijkertijd bepaalde beperkingen toevoegde aan het protocol om de systeemvereisten te beperken en een soepele werking te garanderen.[296]

In de begindagen was dit type leiderschap waarschijnlijk noodzakelijk. Bitcoin was een klein project met experimentele software en het was handig om cruciale oplossingen snel en eenzijdig uit te rollen. Maar op lange termijn zou Nakamotos invloed een risico kunnen vormen: als projectleider kon hij het doelwit worden van toezichthouders, afpersers of verschillende vormen van corruptie. Of hij zou zijn verstand kunnen verliezen en Bitcoin in gevaar brengen door enkel zijn eigen gemoedstoestand.

Zonder Nakamoto had niemand een vergelijkbaar natuurlijk gezag over het project. Aan het eind van 2010 werd Bitcoin echt gedecentraliseerd.

Het Bitcoin-project

Vandaag de dag wordt de code van Bitcoin onderhouden en ontwikkeld door een open gemeenschap van vrijwillige programmeurs van over de hele wereld. Of ze nu bewogen zijn door ideologische redenen, geïnteresseerd zijn in de technologie, worden gesponsord door een bedrijf dat een belang heeft in het project, of om een andere reden: ze nemen het op zich om Bitcoin up-to-date te houden en te verbeteren waar ze maar kunnen.

Een deel van dit werk bestaat simpelweg uit het updaten van de software. Iedereen met de juiste vaardigheden kan de bestaande code verbeteren, nieuwe code toevoegen, of het werk van anderen controleren. Volgens de Wet van Linus, zou de kwaliteit van de Bitcoinsoftware moeten verbeteren naarmate meer ontwikkelaars hieraan werken: *met genoeg ogen, zijn alle bugs oppervlakkig*.

Daarnaast kunnen aan Bitcoins protocol ook nieuwe functies worden toegevoegd om zo het systeem enkele van de originele beperkingen op domeinen te

296 Dit omvatte het meest bekend de 1-megabyte limiet voor de blokgrootte, die voorkwam dat de blockchain zo snel zou groeien dat de meeste gewone gebruikers geen Bitcoin-node op hun thuiscomputer zouden kunnen draaien.

laten overwinnen, zoals schaalbaarheid en privacy. Bijvoorbeeld kan Script uitgebreid worden om nieuwe uitgavevoorwaarden te bieden, meer soorten slimme contracten mogelijk te maken, en zelfs volledig nieuwe betalingslagen boven op het basisprotocol mogelijk te maken, vergelijkbaar met wat James A. Donald en Hal Finney suggereerden in hun eerste reacties op Nakamotos ontwerptekst.[297]

Dit betekent niet dat iedereen zomaar elke wijziging kan aanbrengen aan de code van Bitcoin en die naar eigen inzicht over het netwerk kan uitrollen. In een samenwerkingsverband moet de ontwikkelingsgemeenschap over het algemeen akkoord gaan met een wijziging van de originele broncode (nu *Bitcoin Core* genoemd), en dit is nog meer het geval wanneer de wijzigingen effect hebben op regels van het Bitcoinprotocol. Zonder ruime consensus, zal een verandering meestal niet doorgevoerd worden.

Dit terzijde, omdat Bitcoin bestaat uit vrije en open source-software, kan elke ontwikkelaar een kopie (*fork*) van deze broncode maken en wijzigingen aanbrengen in deze nieuwe versie van de software. Ze zijn ook vrij om deze software te gebruiken en te verspreiden onder anderen. Maar geen enkele ontwikkelaar — of ze nu bijdragen aan Bitcoin Core of aan een kopie — heeft de macht om hun software aan gebruikers op te dringen.

Inderdaad, het zijn de gebruikers, niet de ontwikkelaars die uiteindelijk beslissen welke code ze willen gebruiken. Ze kunnen altijd besluiten een verandering niet te accepteren door te weigeren om een nieuwe release te downloaden en te installeren, en in plaats daarvan te blijven werken met de Bitcoinsoftware die ze al gebruikten. Het tegenovergestelde is ook waar: gebruikers kunnen een nieuwe versie van de software (of eender welke *fork*) aanvaarden die een verandering bevat. Bij Bitcoin is niemand de baas… en is iedereen de baas.

Het Bitcoin-ecosysteem heeft in de loop der jaren zeker de introductie van verschillende nieuwe softwareversies gezien. Sommige daarvan zijn volledige herimplementaties van het Bitcoinprotocol, met een geheel nieuwe code. Anderen zijn afsplitsingen van Bitcoin Core met enkele relatief kleine aanpassingen om beter aan persoonlijke voorkeuren te voldoen. Weer anderen zijn gespecialiseerde programma's die zich concentreren op een specifieke taak, zoals het minen. En er zijn zelfs versies van de software die bewust afwijken van de bestaande regels van

297 Op dit moment is het meest bekende voorbeeld van zo'n betalingslaag het Lightning Network.

het Bitcoinprotocol.

Toch heeft dit niet tot chaos geleid. De meeste gebruikers willen geen veranderingen aanbrengen die de waarde van hun munten zouden verminderen, zoals code die inflatie van de valuta introduceert voorbij de limiet van eenentwintig miljoen, of een versie van de software die het niet eens zou kunnen worden met de rest van het netwerk. Integendeel: gebruikers, in hun eigen belang handelend, hebben de neiging alleen waardevolle veranderingen te accepteren: upgrades die het protocol sterker maken, nodes efficiënter, en het netwerk betrouwbaarder.

In de meer dan tien jaar sinds Satoshi Nakamoto vertrok, hebben ontwikkelaars en gebruikers zich op eigen kracht georganiseerd om gezamenlijk tot een zeer betrouwbaar Bitcoinprotocol te komen: nieuwe blokken worden ongeveer elke tien minuten gevonden, splitsingen in de blokketen zijn zeldzaam en kortstondig, en dubbele uitgaven zijn onbestaand. Ondertussen zijn het aantal gebruiksmogelijkheden, het totale transactievolume en de marktwaarde van Bitcoin spectaculair toegenomen.

In een wereld met van bovenaf, centraal beheerde fiatvaluta en al hun problemen, vertegenwoordigt Bitcoin een krachtig voorbeeld van spontane orde.

Erkenningen

Ik had dit boek niet kunnen schrijven zonder de hulp die ik van zoveel mensen heb gekregen.

Allereerst, grote dank aan David Bailey, die me de tijd en kans heeft gegeven om aan dit boek te werken tijdens mijn tijd bij *Bitcoin Magazine*.

Vervolgens wil ik mijn redacteuren bedanken. Pete Rizzo, die geduldig genoeg was om de zeer slordige vroege concepten te lezen en hielp met het structureren van het verhaal, en Joakim Book, die de tekst liet glanzen, een aantal fouten ving die niemand anders zag, en me hielp om alles over de finish te krijgen.

Ik ben ook erg dankbaar voor de steun die ik heb gekregen van andere collega's bij *Bitcoin Magazine*, namelijk Ellen Sullivan en Christian Keroles.

Ik had het grote geluk dat een aantal mensen die in het boek voorkomen beschikbaar waren voor interviews en/of feedback, waaronder (in alfabetische volgorde) Adam Back, David Chaum, Douglas Jackson, Gregory Maxwell, Martin Hellman, Nick Szabo, Richard Stallman, Scott Stornetta, Tom Morrow, Wei Dai en Whitfield Diffie. Hartelijk bedankt!

Speciale dank gaat naar de domeindeskundigen die zo vriendelijk waren om de vroege hoofdstukconcepten na te kijken, met name Adam Gibson, Bryan Bishop, Eduard de Jong, Jan Burgers, Tony Klausing, Vijay Boyapati, en Wolf von Laer.

Om verschillende redenen wil ik ook Austin Hill, Andreas Antonopoulos, Ferdinando Ametrano, Jurjen Bos, LENA, Marcel van der Peijl, Tuur Demeester, en Wouter Habraken bedanken.

In mei 2023 heb ik dit boek *open source* gemaakt door de tekst op Google Docs te publiceren en zo aan iedereen de gelegenheid te geven om het te lezen en

suggesties voor verbeteringen aan te kaarten. Gedurende de volgende maanden hadden daadwerkelijk een aantal mensen bijgedragen, sommigen klein, anderen groot. De deelnemers waren onder meer: 0x3phemeralsoul, Antoine Poinsot, Ben Murdock, Bitcoin Graffiti, Fractal Encrypt, Giacomo Zucco, Haarman Haarman, Info Scholarium, Jake Franklin, Jake Thomas, Jan-Paul Franken, Joao Bordalo, Jonathan Bier, John Doe, Leonhard Weese, Ludovic Lars, Marc Bonenberger, Mengu Gulmen, Muhammad Saqib Arfeen, Nadir Khan, Nick Nell, Pieter Meulenhoff, Richard Hogan, Thomas Farstrike, Will Wohler, en Zionfuo.

Tot slot wil ik mijn familie en vrienden (in het bijzonder Frederique Mol) bedanken voor hun steun gedurende de jaren, evenals iedereen die mij heeft geholpen op mijn Bitcoinreis sinds 2013.

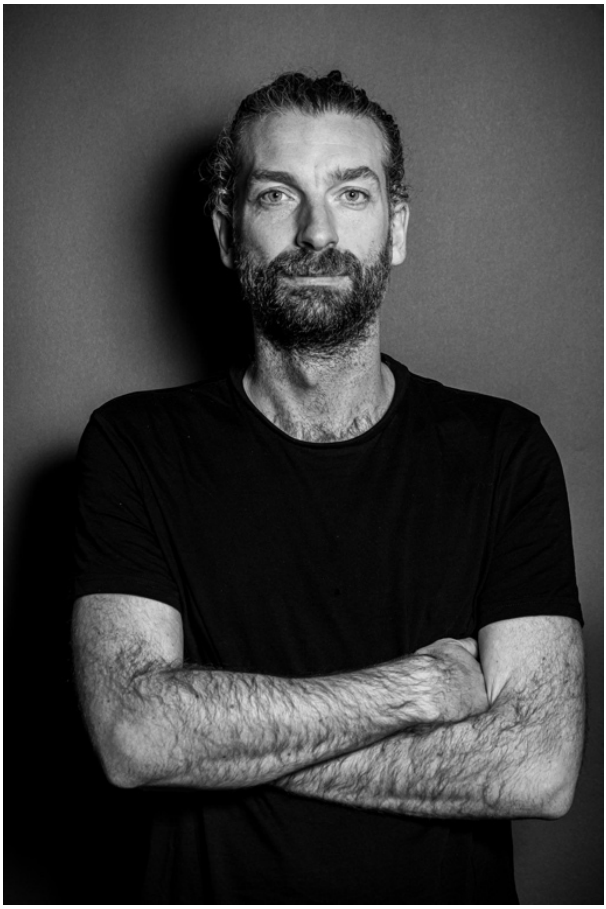
En natuurlijk, bedankt Satoshi Nakamoto, wie je dan ook mag zijn.

Mijn excuses aan iedereen die ik ben vergeten te noemen.

Free Ross.

Over de auteur

Aaron van Wirdum studeerde Journalistiek aan de Hogeschool Utrecht en Politiek en Maatschappij in Historisch Perspectief aan de Universiteit Utrecht, met speciale aandacht voor de invloed van nieuwe technologieën op maatschappelijke structuren door de geschiedenis heen. In 2013 maakte hij voor het eerst kennis met Bitcoin en legde zich sindsdien volledig toe op het schrijven over 's werelds eerste succesvolle elektronische geldsysteem. Jarenlang schreef hij voor Bitcoin Magazine: eerst als journalist, later als technisch redacteur en uiteindelijk als hoofdredacteur van de gedrukte editie.



Figuur 16.1: Aaron van Wirdum

Bibliografie

Alfabetisch

American Banker. *Digicash Sends Signal by Hiring Visa Veteran.* American Banker. May 6, 1997. https://www.americanbanker.com/news/digicash-sends-signal-by-hiring-visa-veteran

Back, Adam. *[ANNOUNCE] hash cash postage implementation.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. March 28, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/03/msg00774.html.

Back, Adam. *cypherpunks digicash bank?* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. October 7, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/10/msg00690.html.

Back, Adam. *digital cc transactions, digital checks vs real digital cash.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. May 2, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/05/msg00104.html.

Back, Adam. *distributed virtual bank.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 27, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/08/msg01289.html.

Back, Adam. *no government regulation of the net (was Re: bulk postage fine).* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 3, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/08/msg00087.html.

Back, Adam. *Re: 'why privacy' revisited.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. March 22, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/03/msg00586.html.

Back, Adam. *Re: bulk postage fine (was Re: non-censorous spam control).* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 3, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/08/msg00070.html.

Back, Adam. *Re: Bypassing the Digicash Patents.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. April 30, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/04/msg00822.html.

Back, Adam. *Re: cypherpunks digicash bank?* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. October 8, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/10/msg00734.html.

Back, Adam. *Re: Remailer problem solution?* March 23, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/03/msg00631.html.

Back, Adam. *The Bitcoin Game #59: Dr. Adam Back.* Interview door Rob Mitchell. The Bitcoin Game, YouTube. October 25, 2018. https://youtu.be/xxYsRjanphA?si=XVdLXPWGUk6oVPXg&t=647%2047:59.

Barnes, Douglas. *Re: cypherpunks digicash bank?* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. October 8, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/10/msg00731.html.

Bayer, Dave, Stuart Haber, and Scott W. Stornetta. *Improving the Efficiency and Reliability of Digital Time-Stamping.* Conference Paper, Sequences II: Methods in Communication, Security, and Computer Science (1993): 329–34. https://www.math.columbia.edu/~bayer/papers/Timestamp_BHS93.pdf.

BitTorrent. *BitTorrent and µTorrent Software Surpass 150 Million User Milestone; Announce New Consumer Electronics Partnerships.* BitTorrent.com. January 9, 2012. Geraadpleegd via https://web.archive.org/web/20140326102305/http://www.bittorrent.com/intl/es/company/about/ces_2012_150m_users

Black Unicorn. *DigiCash Announcement.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. May 10, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/05/msg00616.html.

Blaug, Mark. Economic Theory in Retrospect. 4th edition. Cambridge: Cambridge University Press, 1985.

Brafman, Ori and Rod A. Beckstrom. The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations. New York: Portfolio, 2006.

Brimmer, Andrew F. *Remembering William McChesney Martin Jr.,* Federal Reserve Bank of Minneapolis. September 1, 1998. https://www.minneapolisfed.org/

article/1998/remembering-william-mcchesney-martin-jr

Brunton, Finn. *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Built Cryptocurrency*. Princeton, NJ: Princeton University Press, 2019.

Butler, Eamonn. *Hayek: His Contribution to the Political and Economic Thought of Our Time*. New York: Universe Books, 2010.

Caldwell, Bruce and Hansjoerg Klausinger. *Hayek: A Life, 1899–1950*. Chicago: University of Chicago Press, 2022.

Casey, Michael J. *Bitcoin Foundation's Andresen on Working With Satoshi Nakamoto*. The Wall Street Journal. March 6, 2014. https://www.wsj.com/articles/BL-MBB-17626

Cave, Damien. *The Mojo solution.* Salon. October 9, 2000. https://www.salon.com/2000/10/09/mojo_nation/.

Chaum, David. *Achieving Electronic Privacy.* Scientific American 267, no. 2 (August 1992): 96–101. https://www.jstor.org/stable/24939181.

Chaum, David. *Blind Signatures for Untraceable Payments,* Advances in Cryptology: Proceedings of Crypto 82: 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18.

Chaum, David. *Security Without Identification: Transaction Systems to Make Big Brother Obsolete.* Communications of the ACM 28, no. 10 (October 1985): 1030–1044. https://dl.acm.org/doi/10.1145/4372.4373.

Chaum, David. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,* Communications of the ACM 24, 2 (February 1981): 84–90. https://dl.acm.org/doi/10.1145/358549.358563.

Dai, Wei. *Law vs Technology.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. February 10, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/02/msg00508.html.

Dai, Wei. *PipeNet 1.1 and b-money,* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, November 26, 1998, Beschikbaar op https://cypherpunks.venona.com/date/1998/11/msg00941.html.

Dai, Wei. *Re: alternative b-money creation.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. December 11, 1998. Beschikbaar op https://cypherpunks.venona.com/date/1998/12/msg00448.html.

Dai, Wei. *Work on Security Instead of Friendliness?* GreaterWrong, July 21,

2012, https://www.greaterwrong.com/posts/m8FjhuELdg7iv6boW/work-on-security-instead-of-friendliness.

Dai, Wei. Comment in the discussion thread *AALWA: Ask any LessWronger anything*. LessWrong. 2014. https://www.lesswrong.com/posts/YdfpDyRpNyypivgdu/aalwa-ask-any-lesswronger-anything.

Dai, Wei. Untitled b-money description. 1998. Geraadpleegd via https://web.archive.org/web/20090415130807/https:/www.weidai.com/bmoney.txt.

Dawkins, Richard. *The Selfish Gene*. Oxford: Oxford University Press, 2016.

De Jong, Eduard. *Electronic Money: From Cryptography and Smart Cards to Bitcoin and Beyond,* Fraunhofer SmartCard Workshop 2017 (2017): 1–10.

Diffie, Whitfield and Martin E. Hellman. *Multiuser Cryptographic Techniques*. AFIPS '76: Proceedings of the June 7-10, 1976, national computer conference and exposition (June 1976): 109–112. https://dl.acm.org/doi/10.1145/1499799.1499815.

Diffie, Whitfield and Martin E. Hellman. *New Directions in Cryptography,* IEEE Transactions On Information Theory vol. IT-22, no. 6 (November 1976): 644–654. https://ieeexplore.ieee.org/document/1055638.

DigiCash, *Bank Austria and Den norske Bank to Issue ecash™ the Electronic Cash for the Internet.* DigiCash. April 14, 1997. Geraadpleegd via https://web.archive.org/web/19970605025912/http:/www.digicash.com:80/publish/ec_pres8.html.

DigiCash. *Advance Bank First to Provide DigiCash's ecash™ System in Australia.* DigiCash. October, 1996. Geraadpleegd via https://web.archive.org/web/19961102121407/https:/www.digicash.com/publish/ec_pres6.html.

DigiCash. *DigiCash's Ecash™ to be Issued by Deutsche Bank*. DigiCash. May 7, 1996. Geraadpleegd via https://web.archive.org/web/19961102121355/https:/www.digicash.com/publish/ec_pres5.html.

Dillinger, Ray. *Bitcoin P2P e-cash paper,* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst, November 6, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014822.html.

Dillinger, Ray. *Bitcoin P2P e-cash paper,* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst, November 14, 2008, Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014857.html.

Dillinger, Ray. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 15, 2008. Beschikbaar

op https://www.metzdowd.com/pipermail/cryptography/2008-November/014859.html.

Dimsdale, Nicholas. *British Monetary Policy and the Exchange Rate 1920-1938.* Oxford Economic Papers 33, New Series (Jul. 1981): 307–49. https://www.jstor.org/stable/2662793.

Donald, James A. *Bitcoin P2P e-cash paper,* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 9, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014837.html.

Donald, James A. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 2, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014814.html.

Donald, James A. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 3, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014819.html.

Donald, James A. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 9, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014841.html.

Drexler, K. Eric. Engines of Creation. New York: Doubleday, 1986.

Dwork, Cynthia and Moni Naor, *Pricing via Processing or Combatting Junk Mail,* Advances in Cryptology—Crypto '92 (1992): 139–147. https://dl.acm.org/doi/10.5555/646757.705669.

Economist, The. *Why Don't Rising House Prices Count Towards Inflation?* The Economist. July 29, 2021. https://www.economist.com/the-economist-explains/2021/07/29/why-dont-rising-house-prices-count-towards-inflation

e-gold. *e-gold News.* December 1999, Geraadpleegd via http://www.e-gold.com/news.html

e-gold. *e-gold® Welcomes US Government Review of its Status as a Privately Issued Currency.* January 20, 2006. Geraadpleegd via https://web.archive.org/web/20060322134922if_/https:/www.e-gold.com/letter2.html

e-gold. *Transcript of sentence before the honorable Rosemary M. Collyer United States District Judge.* 114. November 20, 2008. https://legalupdate.e-gold.com/2008/11/transcript-of-sentence-before-the-honorable-rosemary-m-collyer-united-states-district-judge.html.

Energy Exploration & Exploitation. *World Oil Reserves 1948–2001: Annual Statis-*

tics and Analysis. Energy Exploration & Exploitation 19, no. 2 & 3 (2001). https://journals.sagepub.com/doi/pdf/10.1260/0144598011492561

Federal Reserve Economic Data. *Consumer Price Index for All Urban Consumers (CPIAUCSL).* Beschikbaar op https://fred.stlouisfed.org/series/CPIAUCSL

Finney, Hal. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 7, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html.

Finney, Hal. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 13, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014848.html.

Finney, Hal. *Bitcoin v0.1 released.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. January 10, 2009. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html

Finney, Hal. *Chaum on the wrong foot?* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 22, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/08/msg00652.html.

Finney, Hal. *Digital Gold, a bearer instrument?* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 26, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/08/msg00788.html.

Finney, Hal. *POLI: Politics vs Technology.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. January 2, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/01/msg00014.html.

Finney, Hal. *Protecting Privacy with Electronic Cash.* Extropy 10 (Winter/Spring 1993): 8–14. http://fennetic.net/irc/extropy/ext10_1.pdf

Finney, Hal. *Re: Re: re: re: digital cash.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. March 16, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/03/msg00694.html.

Finney, Hal. *Re: Voluntary Governments?* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 4, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/08/msg00239.html.

Finney, Hal. *Reusable Proofs of Work.* RPOW website index page. Beschikbaar op https://web.archive.org/web/20090217090451/http:/rpow.net/index.html.

Finney, Hal. *RPOW FAQs.* RPOW website FAQ page. Geraadpleegd via https://nakamotoinstitute.org/rpow/

Finney, Hal. *RPOW Theory,* RPOW website theory page. Geraadpleegd via https://nakamotoinstitute.org/finney/rpow/theory.html

Finney, Hal. *Why remailers...* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. November 15, 1992. Beschikbaar op https://cypherpunks.venona.com/date/1992/11/msg00108.html.

Finney, Hal. *Re: Physical to digital cash, and back again.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, August 19, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/08/msg00581.html.

Fisher, Irving. The Purchasing Power of Money. New York: The Macmillan Company, 1920.

Forste, Eric Watt. *The Theory of Free Banking (George A. Selgin),* Extropy 15 (2nd–3d Quarter 1995): 51–53. https://archive.org/details/extropy-15/Extropy-15/.

Frauenfelder, Mark. *Homeless Cypherpunks Turn to Usenet.* Wired. February 17, 1997. https://www.wired.com/1997/02/homeless-cypherpunks-turn-to-usenet/

Friedman, Milton and Anna Schwartz, A Monetary History of the United States. Princeton, NJ: Princeton University Press, 1963.

Gladstein, Alex. *Uncovering The Hidden Costs of the Petrodollar.* Bitcoin Magazine. April 28, 2021. https://bitcoinmagazine.com/culture/the-hidden-costs-of-the-petrodollar

GNU Operating System, *What is Free Software?* 1996. https://www.gnu.org/philosophy/free-sw.en.html

GNU Operating System. *The GNU Manifesto.* 1985, https://www.gnu.org/gnu/manifesto.en.html

Graeber, David. Debt: The First 5,000 Years. New York: Melville House, 2011.

Graetz, Michael J. and Olivia Briffault. *A 'Barbarous Relic': The French, Gold, and the Demise of Bretton Woods.* In The Bretton Woods Agreements, edited by Naomi Lamoreaux and Ian Shapiro, 121–142. New Haven: Yale University Press, 2019.

Grant, Mark. *Introduction to Digital Cash.* Extropy 15 (2nd–3d Quarter 1995): 14–16. https://archive.org/details/extropy-15/Extropy-15/

Haber, Stuart and Scott W. Stornetta, *How to Time-Stamp a Digital Document.* Journal of Cryptology 3 (1991): 99–111.

Haber, Stuart and Scott W. Stornetta, *Secure Names for Bit-strings.* CCS '97: Proceedings of the 4th ACM Conference on Computer and Communications Security, (April 1997): 28–35. https://dl.acm.org/doi/10.1145/266420.266430

Hayek, Friedrich A. *Can We Still Avoid Inflation?* in The Austrian Theory of the Trade Cycle and Other Essays, edited by Richard M. Ebeling, 93–110. New York: Center for Libertarian Studies, 1978.

Hayek, Friedrich A. *F. A. Hayek on Monetary Policy, the Gold Standard, Deficits, Inflation, and John Maynard Keynes.* Interview door James U. Blanchard III. Re-uploaded by Libertarianism.org on April 19, 2015. https://youtu.be/EYhEDxFwFRU%2026:27.

Hayek, Friedrich A. *Intertemporal Price Equilibrium and Movements in the Value of Money,* in The Collected Works of F.A. Hayek, Good Money: part I, edited by Stephen Kresge, 186–227. Indianapolis, IN: Liberty Fund, 2009.

Hayek, Friedrich A. *Monetary Nationalism and International Stability,* in The Collected Works of F.A. Hayek, Good Money: part II, edited by Stephen Kresge, 37–105. Indianapolis, IN: Liberty Fund, 2009.

Hayek, Friedrich A. *Monetary Policy in the United States after the Recovery from the Crisis of 1920,* in The Collected Works of F.A. Hayek, Good Money: part I, edited by Stephen Kresge, 71–152. Indianapolis, IN: Liberty Fund, 2009.

Hayek, Friedrich A. *The Gold Problem,* in The Collected Works of F.A. Hayek, Good Money: part I, edited by Stephen Kresge, 169–85. Indianapolis, IN: Liberty Fund, 2009.

Hayek, Friedrich A. *The Use of Knowledge in Society.* American Economic Review XXXV, no. 4 (1945): 519–530. https://www.jstor.org/stable/1809376

Hayek, Friedrich A. Choice in Currency: A Way to Stop Inflation. London: The Institute of Economic Affairs, 1976.

Hayek, Friedrich A. Denationalisation of Money: The Argument Refined. London: The Institute of Economic Affairs, 1990.

Hayek. Friedrich A. Denationalisation of Money. London: The Institute of Economic Affairs, 1976.

Hayek. Friedrich A. Prices and Production. New York: Augustus M. Kelly, Publishers, 1967.

Hettinga, Robert. *Re: Bypassing the Digicash Patents.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, April 29, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/04/msg00811.html.

Hettinga, Robert. *Re: digital cc transactions, digital checks vs real digital cash.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. May 3, 1997. Beschikbaar

op https://cypherpunks.venona.com/date/1997/05/msg00147.html.

Hill, Austin. Draft document from 2005 shared with author, March 30, 2022.

House of Representatives, *Deleting Commercial Pornography Sites From the Internet: The U.S. Financial Industry's Efforts to Combat This Problem.* Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, One-Hundred-Ninth Congress, Second Session. September 21, 2006. https://www.govinfo.gov/content/pkg/CHRG-109hhrg31467/html/CHRG-109hhrg31467.htm.

Hughes, Eric. *A Cypherpunk's Manifesto.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. March 17, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/03/msg00392.html.

Hughes, Eric. *Kid Gloves or Megaphones.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. March 14, 1996. Beschikbaar op https://cypherpunks.venona.com/date/1996/03/msg00932.html.

Hughes, Eric. *No digital coins (was: Chaum on the wrong foot?).* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 24, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/08/msg00690.html.

Keynes, John Maynard. A Tract on Monetary Reform. London: Macmillan and Co, 1923.

Keynes, John Maynard. The General Theory of Employment, Interest and Money (London: Palgrave Macmillan, 1936).

Kresge, Stephen. The Collected Works of F.A. Hayek, Good Money: part I. Indianapolis, IN: Liberty Fund, 2009.

Kutler, Jeffrey. *Credit Suisse, Digicash in E-Commerce Test.* American Banker. June 16, 1998. https://www.americanbanker.com/news/credit-suisse-digicash-in-e-commerce-test

Lamport, Leslie, Robert Shostak, and Marshall Pease. *The Byzantine Generals Problem,* ACM Transactions on Programming Languages and Systems (July 1982): 382–401. https://dl.acm.org/doi/10.1145/357172.357176

Lavoie, Don, Howard Baetjer, and William Tulloh. *High-Tech Hayekians: Some Possible Research Topics in the Economics of Computation.* Market Process 8 (Spring 1990): 119–146.

Law, Laurie, Susan Sabett, and Jerry Solinas. *How To Make a Mint: The Cryptography of Anonymous Electronic Cash.* National Security Agency Office of Informa-

tion Security Research and Technology, Cryptology Division. June 18, 1996. https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm

Levine, John. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 3, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014817.html

Levy, Steven. *E-Money (That's What I Want).* Wired. December 1, 1994. https://www.wired.com/1994/12/emoney/

Levy, Steven. Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age. New York: Viking, 2001.

Levy, Steven. Hackers: Heroes of the Computer Revolution. Sebastopol, CA: O'Reilly, 2010.

Lewis, Peter H. *Attention Internet Shoppers: E-Cash Is Here.* The New York Times. October 19, 1994. https://www.nytimes.com/1994/10/19/business/attention-internet-shoppers-e-cash-is-here.html

Lindenfors, Patrick, Andreas Wartel, and Johan Lind, *'Dunbar's Number' Deconstructed.* Biology Letters. May 5, 2021. https://royalsocietypublishing.org/doi/10.1098/rsbl.2021.0158

Martin, Douglas. *Futurist Known as FM-2030 Is Dead at 69.* The New York Times. July 11, 2000. https://www.nytimes.com/2000/07/11/us/futurist-known-as-fm-2030-is-dead-at-69.html

Mason, Edward S. and Robert E. Asher, The World Bank Since Bretton Woods: The Origins, Policies, Operations and Impact of the International Bank for Reconstruction. Washington, DC: Brookings Institution, 1973.

Maxwell, Gregory. IRC message to author, August 13, 2020.

May Tim. *What backs up digital money?* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. March 27, 1996. Beschikbaar op https://cypherpunks.venona.com/date/1996/03/msg01576.html

May, Tim. *'Stopping Crime' Necessarily Means Invasiveness.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. October 17, 1996. Beschikbaar op https://cypherpunks.venona.com/date/1996/10/msg01269.html

May, Tim. *'Who shall speak for us?'* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. September 29, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/09/msg02189.html

May, Tim. *Crypto Activism and Respectability.* Oorspronkelijk verstuurd naar de

Cypherpunk-mailinglijst. April 21, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/04/msg00400.html.

May, Tim. *Crypto Anarchy, the Government, and the National Information Infrastructure.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. November 29, 1993, Beschikbaar op https://cypherpunks.venona.com/date/1993/11/msg01106.html.

May, Tim. *Cyberspace, Crypto Anarchy, and Pushing Limits.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. April 3, 1994. Geraadpleegd via https://cypherpunks.venona.com/date/1994/04/msg00096.html.

May, Tim. *Degrees of Freedom.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. February 8, 1996. Beschikbaar op https://cypherpunks.venona.com/date/1996/02/msg00637.html.

May, Tim. *DigiCash can use whatever currencies are valued* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. May 4, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/05/msg00243.html.

May, Tim. *Hayek (was: Cato Institute conference on Net-regulation).* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 27, 1996. Geraadpleegd via http://cypherpunks.venona.com/date/1996/08/msg02102.html.

May, Tim. *Libertaria in Cyberspace.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 9, 1993. Geraadpleegd via https://cypherpunks.venona.com/date/1993/08/msg00168.html.

May, Tim. *My Departure, Moderation, and *Ownership of the List.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. February 2, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/02/msg02898.html.

May, Tim. *Opportunities in Cyberspace.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. September 8, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/09/msg00140.html.

May, Tim. *Re: alternative b-money creation.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. December 11, 1998. Beschikbaar op https://cypherpunks.venona.com/date/1998/12/msg00455.html.

May, Tim. *Re: Hettinga's e$yllogism.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. June 28, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/06/msg01637.html.

May, Tim. *Re: More on digital postage.* Oorspronkelijk verstuurd naar de

Cypherpunk-mailinglijst. February 15, 1997. Beschikbaar op https://cypherpunks.venona.com/date/1997/02/msg02295.html.

May, Tim. *Re: Stalling the crypto legislation for 2-3 more years.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. July 23, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/07/msg01245.html.

May, Tim. *Re: The War on Some Money* https://cypherpunks.venona.com/date/1995/12/msg01044.html.

May, Tim. *Scenario for a Ban on Cash Transactions.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. November 24, 1992. Beschikbaar op https://cypherpunks.venona.com/date/1992/11/msg00211.html.

May, Tim. *Software Patents are Freezing Evolution of Products.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. October 7, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/10/msg00685.html.

May, Tim. *The Crypto Anarchist Manifesto* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst, November 22, 1992. Beschikbaar op https://cypherpunks.venona.com/date/1992/11/msg00204.html.

May, Tim. *The Cyphernomicon.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. September 10, 1994. Beschikbaar op https://nakamotoinstitute.org/static/docs/cyphernomicon.txt.

May, Tim. *Untraceable Digital Cash, Information Markets, and BlackNet ('Governmental and Social Implications of Digital Money' panel at CFP '97).* The Computers Freedom & Privacy Conference (1997). Geraadpleegd via https://web.archive.org/web/20130501134401/https:/osaka.law.miami.edu/~froomkin/articles/tcmay.htm.

May, Tim. *Untraceable Payments, Extortion, and Other Bad Things.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. December 21, 1996. Beschikbaar op https://cypherpunks.venona.com/date/1996/12/msg01468.html.

McCloskey, Deirdre N. *How to be Human – Though an Economist.* Ann Arbor: The University of Michigan Press, 2000.

McCullagh, Declan. *Digging Those Digicash Blues.* Wired. June 14, 2001. https://www.wired.com/2001/06/digging-those-digicash-blues/.

Menger, Carl. *Untersuchungen über die Methode der Sozialwissenschaften und der Politischen Oekonomie insbesondere.* Leipzig: Dunker und Humblot, 1883.

Merkle, Ralph C. *A Certified Signature.* Advances in Cryptology—CRYPTO '89:

Proceedings (1989): 218–238. https://link.springer.com/chapter/10.1007/0-387-34805-0_21.

Metzger, Perry E. *ADMIN: end of bitcoin discussion for now.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 17, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014867.html.

Metzger, Perry E. *Re: Virtual Cash.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. May 3, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/05/msg00131.html.

Mor, Federico. *Bank Rescues of 2007-09: Outcomes and Cost.* House of Commons Research Briefing. October 8, 2018. Beschikbaar op https://commonslibrary.parliament.uk/research-briefings/sn05748/.

More, Max. *Hayek's Denationalisation of Money.* Extropy 15 (2nd–3d Quarter 1995): 19–20. https://archive.org/details/extropy-15/Extropy-15/

More, Max. *The Extropian Principles: A Transhumanist Declaration.* maxmore.com, Geraadpleegd via https://web.archive.org/web/20090130143449/https://www.maxmore.com/extprn3.htm

More, Max. *Transhumanism: Towards a Futurist Philosophy.* maxmore.com, Geraadpleegd via https://web.archive.org/web/20051029125153/http://www.maxmore.com/transhum.htm

Nagy, Daniel A. comments in response to *The Mojo Nation Story—Part 2*. Financial Cryptography. October 12, 2005. https://www.financialcryptography.com/mt/archives/000572.html

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008. Beschikbaar op https://bitcoin.org/bitcoin.pdf

Nakamoto, Satoshi and Wei Dai. *Wei Dai/Satoshi Nakamothttps://gwern.net/doc/bitcoin/2008-nakamoto

Nakamoto, Satoshi. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. October 31, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, Satoshi. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 2, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014815.html

Nakamoto, Satoshi. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar

de Cryptografie-mailinglijst. November 6, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html

Nakamoto, Satoshi. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 14, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014853.html

Nakamoto, Satoshi. *Bitcoin P2P e-cash paper.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. November 8, 2008. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html

Nakamoto, Satoshi. *Bitcoin v0.1 released.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. January 8, 2009. Beschikbaar op https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

Nakamoto, Satoshi. *Bitcoin v0.1 released.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. January 16, 2009. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html

Nakamoto, Satoshi. *Bitcoin v0.1 released.* Oorspronkelijk verstuurd naar de Cryptografie-mailinglijst. January 16, 2009. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html

Nash, Hadon. *Digital Gold,* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. August 24, 1993. Beschikbaar op https://cypherpunks.venona.com/date/1993/08/msg00698.html

Next! Magazine. *Hoe DigiCash alles verknalde.* Next! January 1999. Geraadpleegd via https://web.archive.org/web/19990427142412/https:/www.nextmagazine.nl/ecash.htm

Nixon, Richard. *Address to the Nation Outlining a New Economic Policy: 'The Challenge of Peace'.* August 15, 1971. Beschikbaar op The American Presidency Project. https://www.presidency.ucsb.edu/documents/address-the-nation-outlining-new-economic-policy-the-challenge-peace

Officer, Lawrence H. *Exchange Rates Between the United States Dollar and Forty-one Currencies*, MeasuringWorth, 2023. https://www.measuringworth.com/datasets/exchangeglobal/

Patel, Rupal and Jack Meaning. Can't We Just Print More Money? Economics in Ten Simple Questions. The Bank of England. London: Cornerstone Press, 2022.

Pitta, Julie. *Requiem for a Bright Idea,* Forbes. November 1, 1999. https://www.forbes.com/forbes/1999/1101/6411390a.html

Pr0duct Cypher. *Magic Money Digicash System.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. February 4, 1994. Beschikbaar op https://cypherpunks.venona.com/date/1994/02/msg00247.html

Purdy, George B. *A High Security Log-in Procedure.* Communications of the ACM 17, no. 8 (August 1974): 442–445.

Quinn, Michelle. *The Cypherpunks Who Cracked Netscape,* San Francisco Chronicle. September 20, 1995. https://people.eecs.berkeley.edu/~daw/press/iang/ian1.html

Raymond. Eric S. The Cathedral & The Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary. Sebastopol, CA: O'Reilly, 2001.

Regis, Ed. *Meet the Extropians.* Wired. October 1, 1994. https://www.wired.com/1994/10/extropians/

Richardson, Gary and Tim Sablik. *Banking Panics of the Gilded Age: 1863–1913.* Federal Reserve History. December 4, 2015. https://www.federalreservehistory.org/essays/banking-panics-of-the-gilded-age

Rickards, James. *Currency Wars: The Making of the Next Global Crisis*. New York: Portfolio 2012.

Roosevelt, Franklin D. *Relating to the Hoarding, Export, and Earmarking of Gold Coin, Bullion, or Currency and to Transactions in Foreign Exchange.* August 28, 1993. Beschikbaar op The American Presidency Project. https://www.presidency.ucsb.edu/documents/executive-order-6260-relating-the-hoarding-export-and-earmarking-gold-coin-bullion-or.

Salin, Phil. *Costs and Computers.* Release 1.0 (November 25, 1991): 5–18. https://www.yumpu.com/en/document/read/17286753/25-november-1991-cdnoreillycom

Salin, Phil. *The Ecology of Decisions, or 'An Inquiry into the Nature and Causes of the Wealth of Kitchens'.* Market Process 8 (Spring 1990): 91–114.

Schulze, Hendrik and Klaus Mochalski. *Internet Study 2008/2009.* Ipoque. 2009. https://sites.cs.ucsb.edu/~almeroth/classes/W10.290F/papers/ipoque-internet-study-08-09.pdf

Selgin, George. *The New Deal and Recovery, Part 15: The Keynesian Myth.* Cato Institute. March 16, 2022. https://www.cato.org/blog/new-deal-recovery-part-15-keynesian-myth

Stallman, Richard. *Free Software Is Even More Important Now.* gnu.org, https://

www.gnu.org/philosophy/free-software-even-more-important.en.html

Stallman, Richard. *Free Unix!* September 27, 1983, https://www.gnu.org/gnu/initial-announcement.en.html

Stallman, Richard. *Richard Stallman: High School Misfit, Symbol of Free Software, MacArthur-Certified Genius.* Interview door Michael Gross, mgross.com, 1999. https://www.mgross.com/writing/books/my-generation/bonus-chapters/richard-stallman-high-school-misfit-symbol-of-free-software-macarthur-certified-genius/

Stallman, Richard. *RMS Berättar.* Linköping University, http://www.lysator.liu.se/history/garb/txt/87-2-rms.txt

Stallman, Richard. *Talking to the Mailman.* Interview door Rob Lucas, New Left Review, Sept–Oct 2018. https://newleftreview.org/issues/ii113/articles/richard-stallman-talking-to-the-mailman

Stornetta, Scott. *The Missing Link between Satoshi & Bitcoin: Cypherpunk Scott Stornetta.* Interview door Naomi Brockwell. NBTV, with Naomi Brockwell. YouTube, September 6, 2018, https://youtu.be/fYr-keVOQ18,%2057:08

Szabo, Nick. (@NickSzabo4), *Some of the most important books I've read.* X. January 31, 2016. https://twitter.com/NickSzabo4/status/693682157525401601

Szabo, Nick. *Bit Gold Markets.* Unenumerated. December 27, 2008. https://unenumerated.blogspot.com/2008/04/bit-gold-markets.html

Szabo, Nick. *Bit Gold.* Unenumerated. December 27, 2008. https://unenumerated.blogspot.com/2005/12/bit-gold.html

Szabo, Nick. *Bit Gold: Towards Trust-Independent Digital Money.* 1999. Geraadpleegd via https://web.archive.org/web/20140406003811/http:/szabo.best.vwh.net/bitgold.html

Szabo, Nick. *Nick Szabo on Cypherpunks, Money and Bitcoin.* Interview door Peter McCormack, What Bitcoin Did, November 1, 2019, https://www.whatbitcoindid.com/podcast/nick-szabo-on-cypherpunks-money-and-bitcoin%201:39:37

Szabo, Nick. *Nick Szabo—The Quiet Master of Cryptocurrency | Co-Hosted by Naval Ravikant.* Interview door Tim Ferriss, The Tim Ferriss Show. YouTube. August 12, 2017. https://youtu.be/3FA3UjA0igY%202:34:27

Szabo, Nick. *Re: Crypto + Economics + AI = Digital Money Economies.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. September 19, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/09/msg01303.html

Szabo, Nick. *Re: Crypto + Economics + AI = Digital Money Economies.* Oorspronkelijk verstuurd naar de Cypherpunk-mailinglijst. September 19, 1995. Beschikbaar op https://cypherpunks.venona.com/date/1995/09/msg01303.html

Szabo, Nick. *Secure Property Titles with Owner Authority.* Satoshi Nakamoto Institute (1998). https://nakamotoinstitute.org/secure-property-titles/

Szabo, Nick. *Shelling Out: The Origins of Money.* Satoshi Nakamoto Institute (2002). https://nakamotoinstitute.org/shelling-out/

Szabo, Nick. *Smart Contracts: Building Blocks for Digital Free Markets.* Extropy 16 (1st Quarter of 1996): 50–64. https://archive.org/details/extropy-16.

Szabo, Nick. *Trusted Third Parties are Security Holes.* Satoshi Nakamoto Institute (2001), https://nakamotoinstitute.org/trusted-third-parties/

Szabo, Nick. *Why Cryptocurrency? Governments Abuse Their Power—Nick Szabo Interview Part 1.* Interview door Zulu Republic. Zulu Republic, YouTube. October 25, 2018. https://youtu.be/LZw4LNLYUgc?si=_FilNeaFnWxpvv9U%201:02.

Szabo, Nick. Personal correspondence, email to author, July 10, 2018.

US Department of Justice. *Digital Currency Business e-gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges.* July 21, 2008. https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html.

US Department of the Treasury. *Troubled Asset Relief Program (TARP)* Beschikbaar op https://home.treasury.gov/data/troubled-asset-relief-program.

von Mises, Ludwig. *Economic Calculation in the Socialist Commonwealth*. Auburn, AL: Ludwig von Mises Institute, 2012.

von Mises, Ludwig. *Human Action: A Treatise on Economics, The Scholar's Edition* (Auburn, AL: Ludwig von Mises Institute, 1998).

von Mises, Ludwig. *The Historical Setting of the Austrian School of Economics*. New Rochelle, NY: Arlington House, 1969.

von Mises, Ludwig. *The Theory of Money and Credit*, translated by J.E. Batson. New Haven, CT: Yale University Press, 1953.

Wang, Liang. *BitTorrent Mainline DHT Measurement.* MLDHT. 2013. Beschikbaar op https://www.cl.cam.ac.uk/~lw525/MLDHT/

Wapshott, Nicholas. Keynes *Hayek: The Clash That Defined Modern Economics*. New York: Norton, 2011.

Watercutter, Angela. *Why Free Software Is More Important Now Than Ever Before.* Wired. September 20, 2013. https://www.wired.com/2013/09/why-free-software-

is-more-important-now-than-ever-before/

Weinstock, Nicole. *Member Profile: Hal Finney.* Cryonics 40, issue 2 (2nd Quarter 2019): 3–9. https://cryonicsarchive.org/docs/cryonics-magazine-2019-02.pdf

White, Lawrence H. *Thoughts on the Economics of 'Digital Currency'.* Extropy 15 (2nd–3d Quarter 1995): 16–19. https://archive.org/details/extropy-15/Extropy-15/.

White, Lawrence H. *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and e-gold.* Cato Journal 34, no. 2 (2014): 281–301. https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/2014/5/cato-journal-v34n2-5.pdf

Wilcox-O'Hearn, Bryce. *Experiences Deploying A Large-Scale Emergent Network.* Peer-to-Peer Systems (2002): 104–110. https://dl.acm.org/doi/10.5555/646334.687811

Wong, Andrea. *The Untold Story Behind Saudi Arabia's 41-Year U.S. Debt Secret.* Bloomberg. May 31, 2016. https://www.bloomberg.com/news/features/2016-05-30/the-untold-story-behind-saudi-arabia-s-41-year-u-s-debt-secret#xj4y7vzkg.

Andere geraadpleegde werken

Ammous, Saifedean. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Hoboken, NJ.: Wiley, 2018.

Assange, Julian. *Cypherpunks: Freedom and the Future of the Internet.* OR Books, 2012.

Back, Adam. *Adam Back Reflects on the Cypherpunk Movement, Inventing Hashcash, Satoshi & Bitcoin.* Interview door Cedric Youngelman. The Bitcoin Matrix 114, YouTube. July 11, 2022. https://youtu.be/uCavLyzQMbk 1:06:35.

Back, Adam. *Hashcash — A Denial of Service Counter-Measure.* cypherspace.org. August 1, 2002. Beschikbaar op https://archive.li/W7QWn.

Back, Adam. *Hashcash information and documentation.* http://www.hashcash.org/.

Back, Adam. *who is this annoying Adam Back guy?,* Bitcoin Forum, June 4, 2013, https://bitcointalk.org/index.php?topic=225463.0

Back, Adam. *Why Dr Adam Back So Legendary.* Interview door Trace Mayer. Bit-

coin Knowledge Podcast, YouTube. September 7, 2015. https://youtu.be/0VboMe_2fnc

Backhouse, Roger E. *Austrian Economics and the Mainstream: View From the Boundary.* The Quarterly Journal of Austrian Economics 3, no. 2 (Summer 2000): 31–43.

Barta, Silas and Robert B. Murphy. *Understanding Bitcoin: The Liberty Lover's Guide to the Mechanics and Economics of Crypto-Currencies*. 2017.

Birch, David and Neil McEvoy. *Downloadsamoney.* Demos Quarterly 8 (1996): 85–94.

Board of Governors of the Federal Reserve System. *Arthur F. Burns.* Federal Reserve Bank of St. Louis. https://www.federalreservehistory.org/people/arthur-f-burns.

Brands, Stefan. *An Efficient Off-line Electronic Cash System Based On The Representation Problem.* Computer Science/Department of Algorithmics and Architecture, Report CS-R9323 (1993). https://ir.cwi.nl/pub/5303

Chaum, David and Adam Back. *Why Bitcoin Now: David Chaum and Adam Back Reflect on the Crypto Wars.* Interview door Laura Shin. Unchained Podcast 186, YouTube. August 18, 2020. https://youtu.be/ZVZxRMAeIdo

Chaum, David and Stefan Brands. *'Minting' Electronic Cash.* IEEE Spectrum. January 4 1999. https://spectrum.ieee.org/minting-electronic-cash

Chaum, David, Amos Fiat, and Moni Naor. *Untraceable Electronic Cash.* Crypto 1988: Advances in Cryptology (1988), 319–27.

Chaum, David. *The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability.* Journal of Cryptology 1 (1988): 65–75. https://link.springer.com/article/10.1007/BF00206326

Coulouris, George, Jean Dolllimore, and Tim Kindberg. *Low-Value electronic transactions: the Millicent protocol.* Distributed Systems, ed. 3 (2001): 303–306. https://www.cdk5.net/security/Ed3/Millicent.pdf

De Jong, Eduard, Nathaniel Tkacz, and Pablo Velasco. *'Live As Friends and Count as Enemies': On Digital Cash and the Media of Payment.* Moneylab Reader (2015): 258–267. https://www.academia.edu/31349137/_You_Will_Live_as_Friends_and_Count_as_Enemies_On_Digital_Cash_and_the_Media_of_Payment

Diffie, Whitfield. *Interview with Whitfield Diffie on the Development of Public Key Cryptography.* Interview door Franco Furger. January 16, 2002. https://www.itas.

kit.edu/pub/m/2002/wedi02a.htm

Drexler, K. Eric. *Molecular engineering: An approach to the Development of General Capabilities for Molecular Manipulation.* Proceedings of the National Academy of Sciences 78, no. 9 (September 1981): 5275–5278.

Ebeling, Richard M. *The Austrian Theory of the Trade Cycle*. Auburn, AL.:Ludwig von Mises Institute, 1996.

Epstein, Jim. *Cypherpunks Write Code Series.* ReasonTV, YouTube. October 7-28, 2020. https://www.youtube.com/playlist?list=PLBuns9Evn1w-T2RwqMhUnTZbTTe-M-g42

Epstein, Jim. *How Will Bitcoin Lead to More Freedom?*, Reason. October 10, 2020. https://reason.com/2020/10/16/how-will-bitcoin-lead-to-more-freedom/

Finney, Hal. *Bitcoin and me (Hal Finney).* Bitcoin Forum. March 19, 2013. https://bitcointalk.org/index.php?topic=155054.0

Finney, Hal. *Hal Finney interview.* Interview door Scott Stilphen. Atari Compendium, https://www.ataricompendium.com/archives/interviews/hal_finney/interview_hal_finney.html

George Edward Durell Foundation. *Money and Banking: The American Experience*. George Mason University Press, 1995.

Gibson, William. *Neuromancer*. New York: Ace, 1984.

Greenberg, Andy. *Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To a Paralyzed Crypto Genius.* Forbes. March 25, 2014. https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/?sh=38f8f8854a37

Greenberg, Andy. *This Machine Kills Secrets: How WikiLeakers, Hacktivists and Cypherpunks Aim to Free the World's Information*. London: Virgin Books, 2012.

Grigg, Ian. *A Quick History of Cryptocurrencies BBTC — Before Bitcoin.* Bitcoin Magazine. April 16, 2014. https://bitcoinmagazine.com/business/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630

Hayek, Friedrich A. *A Free-Market Monetary System.* Lecture delivered at the Gold and Monetary Conference, New Orleans. November 10, 1977. Republished by the Mises Institute, https://mises.org/library/free-market-monetary-system

Hayek, Friedrich A. *Choice in Currency: A Way to Stop Inflation*. London: The Institute of Economic Affairs, 1976.

Hayek, Friedrich A. *A Tiger by the Tail: The Keynesian Legacy of Inflation*, edited

by Sudha R. Shenoy. The Institute of Economic Affairs and the Ludwig von Mises Institute, 2009.

Hellman, Dorothie and Martin Hellman. *A New Map for Relationships: Creating True Love at Home & Peace on the Planet*. New Map Publishing, 2016.

Jackson, Douglas. *The Story of egold.* Interview door Dustin. Did You Know Crypto 72. February 9, 2020. https://didyouknowcrypto.com/ep72/

Kawamoto, Dawn. *Compaq to license digital cash technology.* CNET. January 2, 2002. https://www.cnet.com/tech/tech-industry/compaq-to-license-digital-cash-technology/

Koblitz, Neal. *Elliptic Curve Cryptosystems,* Mathematics of Computation 48, no. 177 (January 1987): 203–9. https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf

Kreling, Tom. *Douglas Jackson bedacht de eerste digitale valuta en werd veroordeeld voor witwassen.* de Volkskrant. January 13, 2018. https://www.volkskrant.nl/economie/douglas-jackson-bedacht-de-eerste-digitale-valuta-en-werd-veroordeeld-voor-witwassen~b6ea3bcd/

Lopp, Jameson. *Bitcoin and the Rise of the Cypherpunks.* CoinDesk. April 9, 2016. https://www.coindesk.com/markets/2016/04/09/bitcoin-and-the-rise-of-the-cypherpunks/

Lynch, Daniel C. and Leslie Lundquist. *Digital Money: The New Era of Internet Commerce*. Hoboken, NJ.: Wiley, 1996.

Massias, H., X. Serret Avila, and J.-J. Quisquater. *Design of a Secure Timestamping Service With Minimal Trust Requirement.* 20th Symposium in Information Theory in the Benelux. May 1999. Beschikbaar op Satoshi Nakamoto Institute: https://nakamotoinstitute.org/static/docs/secure-timestamping-service.pdf

Maxwell, Gregory. *SF Bitcoin Devs Seminar: Greg Maxwell.* SF Bitcoin Developers, YouTube. April 29, 2015. https://youtu.be/Gs9lJTRZCDc 1:23:12.

Merkle, Ralph C. *A Digital Signature Based on a Conventional Encryption Function* Crypto 1987: Advances in Cryptology (1987): 369–378. https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf

Miller, Victor S. *Use of Elliptic Curves in Cryptography.* Crypto 1985: Advances in Cryptology (1985): 417–26. https://dl.acm.org/doi/10.5555/646751.704566

Möller, Niels, *Ncash — An Experimental Digital Cash System* (1998). https://www.lysator.liu.se/~nisse/NCash/

More, Max and Natasha Vita-More. *Max More & Natasha Vita-More on the History of Transhumanism w/ Like Robert Mason.* Interview door Luke Robert Mason. Luke Robert Mason, YouTube. May 28, 2020. https://youtu.be/ffEDNLRq6y8 1:23:58.

More, Max. *Max More — Transhumanism and the Singularity.* Science, Technology & the Future. YouTube. January 4, 2012. https://youtu.be/1xIQgBXw9-o 20:43.

Narayanan, Arvind and Jeremy Clark. *Bitcoin's Academic Pedigree: The concept of cryptocurrencies is built from forgotten ideas in research literature.* Queue 15, no. 4 (July–August 2017): 20–49. https://dl.acm.org/doi/10.1145/3134434.3136559

Okamoto, Tatsuaki and Kazuo Ohta. *Universal Electronic Cash.* Crypto 1991: Advances in Cryptology (1991): 324–337. https://dl.acm.org/doi/abs/10.5555/646756.705374

Orwell, George. *Nineteen Eighty-Four*. London: Penguin Books, 2003.

Pein, Corey. *Everybody Freeze!* The Baffler. March 2016. https://thebaffler.com/salvos/everybody-freeze-pein

Phillips, A. W. *The Relationship Between Unemployment and the rate of Change of Money Wage Rates in the United Kingdom, 1861–1957.* Economica 25: 283–99. https://www.jstor.org/stable/2550759

Popper, Nathaniel. *Digital Gold: The Untold Story of Bitcoin*. New York: Penguin Books, 2016.

Pritzker, Yan, *Inventing Bitcoin: The Technology Behind the First Truly Scarce and Decentralized Money Explained*. 2019.

Rivest, Ronald, Adi Shamir, and Leonard Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM 21, no. 2 (1978): 120–126. https://web.williams.edu/Mathematics/lg5/302/RSA.pdf

Rothbard, Murray N. *The End of Socialism and the Calculation Debate Revisited.* The Review of Austrian Economics 5, no. 2 (1991): 51–76.

Rothbard, Murray N. *The Mystery of Banking*. Auburn, AL.:Ludwig von Mises Institute, 2008.

Rothbard, Murray N. *What Has Government Done to Our Money?* Auburn, AL.: Ludwig von Mises Institute, 2010.

Salerno, Joseph T. *Hayek on the Business Cycle.* Mises Daily. October 8, 2008, https://mises.org/library/hayek-business-cycle

Schneier, Bruce. *Applied Cryptography*, Second Edition: Protocols, Algorithms, and Source Code in C. London: John Wiley & Sons, Inc. 1996.

Selgin, George A. *The Theory of Free Banking: Money Supply Under Competitive Note*. Issue. Totowa, NJ.: Rowman & Littlefield Publishers, 1988.

Skidelsky, Robert. *Keynes: The Return of the Master*. London: PublicAffairs, 2010.

Stephenson, Neal. *Snow Crash.* New York: Bantham Books, 1993.

Szabo, Nick, Adam Back and David Chaum. *The Godfathers of Bitcoin: Nick Szabo, Adam Back and David Chaum*. Interview door John Riggins. Bitcoin in Asia 29, YouTube. November 16, 2020, https://youtu.be/D5LpgX-pkUM 43:33.

Szabo, Nick. *Bitcoin, what took ye so long?* Unenumerated. May 28, 2011. https://unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html

UK Parliament. *Small Change: Britain and the Gold Standard.* UK Parliament. https://www.parliament.uk/business/publications/research/olympic-britain/the-economy/small-change/

US Office of the Historian. *Nixon and the End of the Bretton Woods System, 1971–1973.* https://history.state.gov/milestones/1969-1976/nixon-shock

Vigna, Paul and Casey, Michael J. *Cryptocurrency: The Future of Money?* London: Vintage, 2016.

Vinge, Vernor. *A Fire Upon the Deep*. New York: Tor Books, 1992.

Vinge, Vernor. *True Names: and the Opening of the Cyberspace Frontier*. London: Penguin Books, 2016.

von Böhm-Bawerk, Eugen. *Capital and Interest: A Critical History of Economic Theory*. Translated by William Smart. London: Macmillan and Co., 1890.

Wayner, Peter. *Digital Cash: Commerce on the Net*. London: Academic Press Limited, 1996.

White, Lawrence H., *Banking without a Central Bank: Scotland before 1844 as a 'Free Banking' system.* In Unregulated Banking: Chaos or Order? Edited by F. Capie and G.E. Wood, 37–71. London: Palgrave Macmillan, 1991.

Algemeen

Extropy magazines 1–17 (1988-1996).

eCash news archieven op Chaum.com, https://chaum.com/ecash/

Cypherpunks mailing list archieven, 1992–2000. Beschikbaar op https://cypherpunks.venona.com/

Cryptography mailing list archieven, October 2008–January 2009. Beschikbaar op https://www.metzdowd.com/pipermail/cryptography/