# 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 ondersteund 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 tijdenseen wereldwijde oliecrisis.

In 1973 riepen olieproducerende Arabische landen, verenigd in de Organisatie van de Olie-Exporterende Landen (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 de nieuwbenoemde Amerikaanse minister van Financiën, William Simon, in 1973 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 drukmiddel: 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 - 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]

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 Economische Beleidsadviesraad. 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 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 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 vrije markteconomen 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 van laatste toevlucht 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 vrije markteconomie.

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 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) doorheen de Amerikaanse financiële sector begonnen te verspreiden als een epidemie 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 het 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 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 leningverstrekker in absolute 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 doorheen de vermogensmarkten via 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 economen, bekend als de “Nieuwe 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…

## Hoofdstuk 15:

## Het witboek

**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 witboek, getiteld “Elektronisch Geld Zonder een Vertrouwde Derde Partij.” 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 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.*
* *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.”

### De block chain

Het systeem dat Satoshi Nakamoto in zijn whitepaper 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 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-geld, 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 Hash-bomen (Merkle Trees) 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 Hash-boom, zodat de Hash-wortel opgenomen kon worden in de volgende Hash-boom. Dit resulteerde in een wiskundig verifieerbare chronologische volgorde van Hash-bomen en dus ook een chronologische volgorde van documenten opgenomen in de Hash-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 Hash-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 “blokhash” 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.

### Delven

Omdat een Bitcoinblok alleen als geldig zou worden beschouwd als het geen conflicterende transacties bevat, bood de “block chain” 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 block chains 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 block chain, 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 van op welke block chain 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 het Bitcoin-witboek. 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 blokhash 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” (delven) zou noemen. De mensen die aan het delven zijn (of de “delvers”) zouden willekeurig veel verschillende nonces in een gewenst blok moeten proberen op te nemen, totdat één van hen een geldige blokhash zou genereren. Een geldig blok — dat door niemand zou kunnen worden aangepast nadat het geproduceerd was, omdat dat de blokhash ook zou veranderen — zou dan over het netwerk worden verzonden, waarbij elke gebruiker hun eigendomsregister zou bijwerken met de transacties in dit blok.

Delvers zouden ondertussen hun delfinspanningen aanpassen om de nieuwe blokhash op te nemen in een mogelijk volgend blok, dat op zijn beurt zijn eigen geldige blokhash 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 Bitcoindelvers een cryptografische ketting van blokhashes 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 delven. 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 block chain langer wordt dan het alternatief, zouden Bitcoingebruikers en delvers 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 overkomen, 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 delven, hadden ze een aansporing nodig.

Delvers zouden dus beloond worden met bitcoineenheden als ze een geldige blok delven, 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 delven (waardoor het netwerk kon overeenkomen over de staat van het grootboek), 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 dat 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 gedolven. 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 blokhash 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 gedolven, 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/dat 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 block chain 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 delven met de conflicterende transactie, en doorgaan met het delven van deze alternatieve block chain 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 gedolven 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 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 blokhashes hoefden op te slaan. En ten tweede, door gebruik te maken van hashbewijzen, konden gebruikers controleren met behulp van deze blokhashes dat transacties naar hen waren opgenomen in de block chain — 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 delver te zijn, deze delvers 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 block chain.

“Ik denk dat we ons moeten bezighouden met het minimaliseren van de 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.” /footnote{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 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 block chain 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 zou zijn, 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 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.”/footnote{281}

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”, 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 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 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]

## 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 was in zijn meest primitieve vorm, werd het bevroren. Overheden zeiden dat het niet verder mocht ontwikkelen. En wat we sinds die ontwikkeling hebben gehad, waren zaken van overheidsuitvindingen, meestal verkeerd, 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 het beste kon worden overgelaten aan de vrije markt.

Echter, 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 om concurrentie tussen valuta’s mogelijk te maken. Hij vermoedde dat ze te veel voordeel haalden uit de status quo.

“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 noodfinanciers.”[^288]

De toen vierentachtigjarige econoom koesterde nog steeds de hoop dat geld gerepareerd kon worden. Dit vereiste echter 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 vertrouwenloos 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 Codebasis

*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 nieuw uitgebrachte project:

“Hierbij kondig ik de eerste release van Bitcoin aan, een nieuw elektronisch geldsysteem 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, de 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 voor hoe 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 Bitcoin-software 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 delven.

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 gratis 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 beter toegankelijk dan Richard Stallmans GPL-licentie, die deze vrijheid enkel toekent aan andere gratis softwareprojecten.)

Het was essentieel dat Bitcoin een gratis en open source-software was, omdat de code noodzakelijkerwijs controleerbaar moest zijn: om het systeem echt vertrouwenloos 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 gratis software, zouden mensen Satoshi Nakamoto niet hoeven te vertrouwen op het niet inbouwen van malware om munten te stelen of een geheime achterdeur voor het bijdrukken van geld.

Meer in het algemeen maakte Nakamotos gratis en open source-code, geschreven in de programmeertaal C++ en jaren later door de eerste fulltime Bitcoinontwikkelaar beschreven als “briljant maar slordig”/footnote{290}, voor het eerst volledig inzichtelijk hoe het elektronische grootboeksysteem intern werkte.

Transacties bleken bijvoorbeeld gebruik te maken van “Script”, een nieuwe programmeertaal voor Bitcoin die geïnspireerd was door Forth. Forth is origineel ontworpen in de jaren 1960 om radiotelescopen te bedienen. Met enkele aanpassingen aan de functionaliteit van Forth, kon Script gebruikt worden om eenvoudige smart contracts op Bitcoin te schrijven. Munten konden zodanig worden opgeslagen dat ze alleen verplaatst konden worden als er aan bepaalde programmeerbare condities werd voldaan. (Een simpel 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 algemeen toegepast alternatief geworden.

Tegelijkertijd had Nakamoto een aantal functies toegevoegd om Bitcoin wat gebruiksvriendelijker te maken. Hoewel betalingen technisch gezien nog altijd gedaan werden naar publieke sleutels, 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 codebasis 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 moeten worden gevonden. Clusters van 2.016 blokken zouden vervolgens worden gebruikt om de moeilijkheidsgraad van delven 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 codebasis ook de allereerste blok: het “Genesisblok”. Dit blok moest inderdaad ingebed worden in de release zelf; de block chain had een startpunt nodig. Een interessant detail is echter dat de beloning voor dit Genesisblok in feite waardeloos 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 delven, 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 ieder ander.

Nakamoto benadrukte nog eens zijn expliciete weigering om enig oneerlijk voordeel te genieten boven andere Bitcoingebruikers. Hij had ook een bewijs inbegrepen dat hij in de weken of maanden voorafgaand aan het openbaar maken van de code niet privé had gedelfd. 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 gedelfd moet zijn geweest na dat moment./footnote{291}

Als kers op de taart leek de specifieke kop voor dit doel ook niet willekeurig 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 had beschreven hoe Bitcoin een voorspelbaar uitgifteschema kon ondersteunen, dankzij vaste blokbeloningen en het moeilijkheidsaanpassingsalgoritme. Maar er was op dit punt in het document nog niet precies aangegeven hoe dit schema eruit zou zien.

Het bleek nu dat de code van Bitcoin zo was geprogrammeerd dat het aantal nieuwe munten dat per blok werd toegekend halveerde na elke 210.000 gedolven blokken, of ongeveer eens in de vier jaar. In de eerste vier jaar zouden delvers 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 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 ondersteunen indien nodig.*

Eenentwintig miljoen munten. /footnote{291} 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.

Echter, het was net Hal Finney die besefte dat de stimulansen deze keer enigszins anders gepositioneerd waren.

Op 10 januari, twee dagen na de release van Bitcoin, was Finney de eerste persoon op de Cryptography-mailinglijst die reageerde op de aankondigingsmail. 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 waarschijnlijkheid, geloofde dat de vaste voorraad van Bitcoin de oplossing zou kunnen bieden. Het stelde mensen in staat om basale inschattingen te maken over de potentiële toekomstige waarde van de munten.

“Stel je voor dat Bitcoin succesvol is en het dominante betalingssysteem wordt in de wereld. 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…”/footnote{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 zouden volgen, 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 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 beginnen te worden gebruikt, waarschijnlijk beginnend in plaatsen zonder enige alternatieven.

In een vervolgmail suggereerde Nakamoto: “[…] zoals beloningspunten, donatietokens, valuta voor een spel of micropayments voor volwassenensites.”/footnote{294}

Dit zou de vraag *nog* meer moeten stimuleren. Hierdoor zou bitcoin in feite het klassieke kip-en-ei-probleem kunnen overwinnen waar eerdere digitale geldprojecten onder te lijden hadden. Bitcoin zou zelfs baat kunnen hebben bij een *positieve* feedbacklus!

Op een zekere manier had Finney Ludwig von Mises zijn regressietheorema 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’s 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*.”/footnote{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 een centrale bank werkt, was een volledig homogene vorm van geld. Iedereen kon zijn eigen munten beheersen, en er waren geen reserveverhoudingen om zich zorgen over te maken. En aangezien bitcoin op het internet bestond, kende het geen grenzen. Iedereen 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 hebben altijd in de verleiding komen om dit privilege te misbruiken, ongeacht eerdere afspraken, conventies of verdragen.

Maar Bitcoin werd niet uitgegeven door een 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 niet afhankelijk van monetaire afspraken, conventies of verdragen vanaf het begin, dus er waren ook geen afspraken, conventies of verdragen om te falen. 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 zou worden geaccepteerd in de internationale handel, zouden samengevoegde 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 kan 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 tot het verleden behoren.

Bitcoin kan 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 gedelfd, zou dit in feite geen enkel individu, groep of specifieke sector bevoordelen. Iedereen zou vrij zijn om te delven, daardoor (en door het moeilijkheidsaanpassingsalgoritme) zou open concurrentie de winstmarges tot nul moeten drijven: het proof of work dat het zou kosten om een blok te delven zou ongeveer gelijk moeten komen aan de waarde van de blokbeloning.

Maar misschien heeft Bitcoin nog een grotere impact dan dat. Voor het eerst ooit zou het intertemporele prijssysteem vlekkeloos kunnen worden uitgevoerd. Als gevolg hiervan zouden de rentetarieven *eindelijk* de gezamenlijke tijdsvoorkeuren in de maatschappij weergeven. Dit zou producenten informeren in welk productiestadium zij zouden moeten investeren, wat een efficiënte toewijzing van middelen op termijn vergemakkelijkt. Door zich te verzetten tegen een kunstmatig rentebeleid, 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 tot slot, dankzij de vaste geldhoeveelheid zou 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.

In ongeveer 32.000 regels code heeft Satoshi Nakamoto het potentieel ingebed om de stabiliserende monetaire dogma’s, 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 minimaal honderden mensen over het project hadden gehoord, na de aankondiging van Nakamoto in de Cryptography -mailinglijst, wijzen de gebrekkige betrokkenheid bij 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 valutavoorraad, semi-anonimiteit, betalingen die resistent zijn tegen censuur, basale smart contract-capaciteiten, 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 eerste jaar, begon Bitcoin in de loop van 2010 best wat aantrekkingskracht te krijgen. Het volume van de transacties begon langzaam toe te nemen, nieuwe ontwikkelaars ontdekten het project, en er vormde zich een kleine onlinegemeenschap op een internetforum dat 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 gratis 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 inspraak om codeveranderingen voor te leggen.

Bijgevolg kon Satoshi Nakamoto de regels van het systeem bepalen, en tijdens zijn periode als hoofdontwikkelaar heeft hij inderdaad enkele wijzigingen aangebracht in deze regels. Hij verwijderde bijvoorbeeld functionaliteit uit Script die hij als potentieel gevaarlijk beschouwde, terwijl hij tegelijkertijd bepaalde beperkingen toevoegde aan het protocol om de vereisten tot middelen te beperken en een soepele werking te garanderen./footnote{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. Aan de andere kant, 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 laten overwinnen, zoals schaalbaarheid en privacy. Bijvoorbeeld kan Script uitgebreid worden om nieuwe uitgavevoorwaarden te bieden, meer soorten smart contracts mogelijk te maken, en zelfs volledig nieuwe betalingslagen boven op het basisprotocol mogelijk te maken, vergelijkbaar met wat Joris A. Donald en Hal Finney suggereerden in hun eerste reacties op Nakamotos whitepaper./footnote{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 codebasis (nu “Bitcoin Core” genoemd), en dit is nog meer het geval wanneer de wijzigingen effect hebben op de regels van het Bitcoinprotocol. Zonder ruime consensus, zal een verandering meestal niet doorgevoerd worden.

Dit terzijde, omdat Bitcoin bestaat uit gratis en open source-software, kan elke ontwikkelaar een fork (kopie) van deze codebasis 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. Echter, geen enkele ontwikkelaar — of ze nu bijdragen aan Bitcoin Core of aan een fork — heeft de macht om hun software op te dringen aan gebruikers.

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 delven. En er zijn zelfs versies van de software die bewust afwijken van de bestaande regels van 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, handelend in hun eigen belang, 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 block chain zijn zeldzaam en kortstondig, en dubbele uitgaven zijn onbestaande. Ondertussen zijn het aantal gebruiksmogelijkheden, het totale transactievolume en de marktwaarde van Bitcoin spectaculair toegenomen.

In een wereld met van bovenaf centraal beheerde fiatvaluta’s en al hun problemen, vertegenwoordigt Bitcoin een krachtige uitdrukking 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 Hogeschool Utrecht, waar hij zich specifiek richtte op de historische impact van nieuwe technologieën op maatschappelijke structuren. Hij stuitte op Bitcoin in 2013, en sindsdien schrijft hij over ’s werelds eerste succesvolle elektronische geldproject. Voor het grootste deel van deze jaren deed hij dit voor *Bitcoin Magazine*: eerst als journalist, daarna als technisch redacteur, en uiteindelijk als hoofdredacteur van de gedrukte editie. *Het Genesis Boek* is zijn eerste boek.

# Bibliografie

# Eindnota’s