## 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.