## 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]